Präventive Telekommunikationsüberwachung

Inauguraldissertation
zur Erlangung der Doktorwürde
an der Rechtswissenschaftlichen Fakultät
der Albert-Ludwigs-Universität Freiburg im Breisgau

vorgelegt von
Heike Schäfer

aus Ludwigsburg/Württemberg
2007

Dekan: Herr Professor Dr. Walter Perron

Erstgutachter: Herr Professor Dr. Thomas Würtenberger

Zweitgutachter: Herr Professor Dr. Dietrich Murswiek

Dissertationsort: Freiburg

Datum mündliche Prüfung: 20.05.2008

Erscheinungsjahr: 2008

Vorwort

Diese Arbeit lag der Rechtswissenschaftlichen Fakultät der Albert-Ludwigs-Universität Freiburg i.Br. im Wintersemester 2007/2008 als Dissertation vor.

Das Thema dieser Dissertation, die präventive Telekommunikationsüberwachung, ist weiterhin im Fluss. Aufgrund der grundlegenden rechtlichen Neuregelungen und einer sich immer weiter ausdifferenzierenden Rechtsprechung des Bundesverfassungsgerichts war es im Herbst 2007 erforderlich, eine endgültige Zäsur zu ziehen. Gesetzgebung, Rechtsprechung und Literatur sind bis Dezember 2007 berücksichtigt. Aufgrund der besonderen Bedeutung für das Thema dieser Arbeit sind das zum 01.01.2008 in Kraft getretene „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen“ und der Beschluss der Bundesverfassungsgerichts zur Vorratsdatenspeicherung vom 11.03.2008, AZ: 1 BvR 256/08 eingearbeitet.

Mein besonderer Dank gilt Herrn Professor Dr. Thomas Würtenberger, der mit seiner fachlichen Unterstützung und der Anregung zum bearbeiteten Themengebiet diese Arbeit erst ermöglicht hat. An dieser Stelle danke ich auch Herrn Professor Dr. Dietrich Murswiek für die freundliche und zügige Erstellung des Zweitgutachtens. Ebenfalls danke ich Herrn PD Ralf P. Schenke für seine wertvollen Hinweise bei der Ausarbeitung der einzelnen Kapitel.

Nicht zuletzt geht mein Dank an meine Familie – insbesondere an meinen Mann Ulf – für die unermüdliche Unterstützung während der Erstellung dieser Arbeit.

Bietigheim-Bissingen, im Juli 2008 Heike Schäfer

Inhaltsverzeichnis

Kapitel 1: Rechtfertigung der Themenstellung

I. Gesetzgeberische Überlegungen für eine präventiv-polizeiliche Telekommunikationsüberwachung

Die Überwachung der Telekommunikation durch staatliche Maßnahmen ist vermutlich so alt wie der Fernmeldeverkehr selbst.[1] Zum Zweck der Strafverfolgung und zur Abwehr von Gefahren durch den Staat wird sie grundsätzlich als legitim angesehen.[2]

Überlegungen, eine präventiv-polizeiliche Telekommunikationsüberwachung in der Bundesrepublik Deutschland einzuführen, gab es schon seit längerem.[3] Bereits bei den Beratungen über den Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG) wurde das Thema erörtert.[4] Der Gesetzesentwurf des Bundesrats im Jahr 1990 sah dazu in Art. 9 eine Änderung des Fernmeldeanlagengesetzes (FAG) vor.[5] Nach den neu zu schaffenden §§ 12 a und 12 b FAG sollte eine Aufzeichnung des Fernmeldeverkehrs angeordnet werden dürfen, wenn diese zur Abwehr einer gegenwärtigen Gefahr für Leben, Leib oder Freiheit einer Person erforderlich ist.[6] In der Begründung des Gesetzesentwurfs wurde ausgeführt:

> *„Nach den Erfahrungen der Polizei hat es sich bei der Abwehr gegenwärtiger Gefahren für Leib, Leben oder Freiheit einer Person als wesentlicher Mangel erwiesen, dass eine Telephonüberwachung im präventiven Bereich nicht möglich ist.“*[7]

---

1 Bereits im 1928 wurde die Norm des § 12 FAG erlassen (vgl. RGBl. I, S. 8 ff.), nach der der Richter und bei Gefahr in Verzug auch die Staatsanwaltschaft in strafgerichtlichen Untersuchungen Auskunft über den Fernmeldeverkehr verlangen konnten, wenn die Mitteilungen an den Beschuldigten gerichtet waren oder wenn Tatsachen vorlagen, aus denen zu schließen war, dass die Mitteilungen von dem Beschuldigten herrührten oder für ihn bestimmt waren und dass die Auskunft für die Untersuchung Bedeutung hatte, vgl. *Hansen-Oest*, in: Schmidt/Königshofen/Zwach, § 85 TKG, Rn. 37. Zu § 12 FAG und sein Außer-Krafttreten im Jahr 2001 durch die Regelungen der §§ 100 g und 100 h StPO vgl. die Ausführungen in Kapitel 2 unter I.

2 Vgl. *Kubicek*, DuD 1995, 656 (658); *Hermes*, in: Dreier (Hrsg.), Art. 10 GG, Rn. 67; *Hofmann*, in: Schmidt-Bleibtreu/Klein, Art. 10 GG, Rn. 28 ff.; *Loewer*, in: v.Münch/Kunig (Hrsg.), Art. 10 GG, Rn. 39 ff.

3 Vgl. *R.P. Schenke*, AöR 125 (2000), 1 (3); *W.-R. Schenke*, JZ 2001, 997 ff.

4 Vgl. *Weitemeier/Große*, Kriminalistik 1997, 335.

5 Vgl. BT-Drucksache 11/7663, S. 48; BT-Drucks. 12/989, S. 49.

6 Vgl. BT-Drucks. 11/7663, S. 17; BT-Drucks. 12/989, S. 17. Vgl. auch *W.-R. Schenke*, JZ 2001, 997 ff.; *Weitemeier/Große*, Kriminalistik 1997, 335.

7 BT-Drucks. 11/7663, S. 48; BT-Drucks. 12/989, S. 49.

In dem später erlassenen OrgKG[8] wurde die vorgeschlagene Telefonüberwachung zur Gefahrenabwehr allerdings nicht mehr berücksichtigt.[9] Nach Ansicht von *W.-R. Schenke*[10] beruhte dies darauf, dass gegenüber einer derartigen, der Gefahrenabwehr dienenden Regelung im Hinblick auf die Gesetzgebungskompetenz des Bundes erhebliche Bedenken bestanden.[11]

Zum anderen wurde der Bund in der Stellungnahme des Bundesrates vom 04.09.1997 zum Entwurf des Begleitgesetzes zum Telekommunikationsgesetz[12] aufgefordert, telekommunikative Auskunftsersuchen im Bereich der allgemeinen Gefahrenabwehr zu ermöglichen sowie die Regelungen über die Pflicht der Netzbetreiber zur Ermöglichung und technischen Unterstützung von Überwachungsmaßnahmen zukunftsoffen für landesrechtliche Regelungen auf dem Gebiet der Gefahrenabwehr zu gestalten.[13] Dies wurde aber von der Bundesregierung ohne nähere Begründung abgelehnt.[14]

Das Bedürfnis für präventiv-polizeiliche Telekommunikationsüberwachungen bestand jedoch offensichtlich[15] und so wurden diese in der Praxis auch durchgeführt. Sie fanden unter Berufung auf einen übergesetzlichen Notstand bzw. auf die §§ 32 und 34 StGB statt,[16] wobei die Übermittlung von Kommunikationsdaten in Notfällen von den Telekommunikationsdiensteanbietern verlangt wurde, die diesen Forderungen wohl auch nachkamen.[17]

---

8 Gesetz zu Bekämpfung der organisierten Kriminalität vom 04.05.1998, BGBl. I, S. 845.

9 Vgl. *Weitemeier/Große,* Kriminalistik 1997, 335; *R.P. Schenke,* AöR 125 (2000), 1 (3).

10 Vgl. *W.-R. Schenke,* JZ 2001, 997.

11 Zur Gesetzeskompetenz für eine präventiv-polizeiliche Telekommunikationsüberwachung vgl. das Kapitel „Der Zugriff auf die Telekommunikationsdaten" unter IV. 1.

12 Zum Begleitgesetz zum Telekommunikationsgesetz vom 17.12.1997 (BGBl. I, 3108) siehe *Bizer*, DuD 1998, 42 ff.

13 Vgl. BT-Drucks. 13/8453, S. 2, 5; siehe auch *R.P. Schenke*, AöR 125 (2000), 1 (3).

14 Zur ablehnenden Stellungsnahme der Bundesregierung vgl. BT-Drucks. 13/8453, S. 11, 13.

15 Vgl. dazu *Weitemeier/Große*, Kriminalistik 1997, 335 (336), die anhand konkreter Fallkonstellationen, wie Kidnapping oder Banküberfällen, das Bedürfnis für eine präventive Telekommunikationsüberwachung aufzeigen, da in diesen Fällen der Schutz des Opfers im Vordergrund stehe und sich eine Ermächtigungsgrundlage für eine Kommunikationsüberwachung nur aus dem Gefahrenabwehrrecht ergeben könne. Siehe auch *R.P. Schenke*, AöR 125 (2000), 1 (3).

16 Vgl. dazu das Kapitel „Entwicklung und bisherige gesetzliche Grundlagen der Telekommunikationsüberwachung in der Bundesrepublik Deutschland" unter IV.

17 Dies kommt in der Gesetzesbegründung des Landes Bayern zur präventiven Telekommunikationsüberwachung zum Ausdruck, LT- Drucks. 15/2096, S. 60. Auch im Bericht der thüringer Landesregierung über die präventiv-polizeiliche Telekommunikationsüberwachung aus dem Jahr 2003 wird erwähnt, dass durch die thüringer Polizeibehörden Daten von den Telekommunikationsunternehmen unter Berufung auf § 34 StGB abgefordert wurden, obwohl diese Verfahrensweise seit In-Kraft-Treten von § 34 a ThPAG nicht mehr zulässig war, LT-Drucks. Th. 4/249, S. 3.

Die Notwendigkeit das Instrumentarium staatlicher Maßnahmen den tatsächlichen Gefahren- und Bedrohungslagen anzupassen um diesen dadurch effektiv begegnen zu können, ist zu Beginn des 21. Jahrhunderts insbesondere durch die Anschläge auf das World Trade Center in New York und das Verteidigungsministerium in Washington D.C. am 11. September 2001, die Anschläge auf Madrider Vorortzüge im März 2004 und die Anschläge vom 07. und 21.07.2005 auf Londoner Busse und U-Bahnen deutlich hervorgetreten. So haben nicht nur die Vereinigten Staaten von Amerika[18], sondern auch die Europäische Union[19] und die Bundesrepublik Deutschland mit einem energischen Ausbau des Sicherheitsrechts auf die Herausforderungen dieses „neuen Terrorismus“[20] reagiert.

1. Rechtsänderungen in der Bundesrepublik Deutschland

Ergebnis dieser Reaktionen auf Bundesebene waren die beiden sog. *Sicherheitspakete*. Während das *erste Sicherheitspaket*[21] lediglich eine Streichung des Religionsprivilegs im Vereinsgesetz[22], ferner eine Anhebung von Tabak- und Versicherungssteuer[23] zur Finanzierung von Behördenaufstockungen enthielt, wurde das *zweite Sicherheitspaket*[24] von den beteiligten

---

18 Folge der Terroranschläge in den USA war der Erlass des Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (US Patriot Act); http://www.epic.org/privacy/terrorism/hr3162.pdf. Frei übersetzt etwa: „Gesetz zur Einigung und Stärkung Amerikas durch Bereitstellung angemessener Mittel zur Verhinderung von Terrorismus“. Durch den US Patriot Act wurde u.a. die Befugnis zur Kommunikationsüberwachung und zum Datenaustausch erweitert. Diese Ausweitung erfolgte sowohl für Zwecke der Strafverfolgung, als auch aus Gründen der Spionageabwehr zur Überwachung des Auslands oder ausländischer Agenten, vgl. *Pallasky*, DuD 2002, 221 ff., der die Änderungen des Überwachungsrechts durch den US Patriot Act ausführlich darstellt.

19 Reaktionen innerhalb der Europäischen Union waren insbesondere auf der Strafverfolgungsebene zu verzeichnen, vgl. *v.Bubnoff*, NJW 2002, 2672 ff. So durch die Rahmenbeschlüsse zur Terrorismusbekämpfung, ABl. EG 2002, Nr. L 164, S. 3 ff., zum Europäischen Haftbefehl ABl. EG 2002, Nr. L 190, S. 1 ff. und zum Einfrieren von Straftaterträgnissen, ABl. EG 2001, Nr. L 182, S. 1, den Beschluss über die Errichtung von Eurojust als Europäische Justizbehörde, ABl. EG 2002, Nr. L 63, S. 1, die Verordnung des Rates über spezifische Maßnahmen zur Terrorismusbekämpfung, ABl. EG 2001, Nr. L 344, S. 70 sowie durch die Ratsempfehlung über die Zusammenarbeit bei der Finanzierungsbekämpfung des Terrorismus, ABl. EG 2001, Nr. L 344, S. 90.

20 Zum „Neuen“ am gegenwärtigen Terrorismus vgl. *Lutz*, in: H.J. Koch (Hrsg.), S. 9 (18 ff.). Bislang mangelt es in den einschlägigen Übereinkommen sowohl auf UN- wie auf gesamteuropäischer Ebene an einer einheitlichen Terrorismusdefinition. Allgemein lässt sich sagen, dass Terrorismus auf eine Destabilisierung unserer Zivilisation und auf eine Verunsicherung der Bevölkerung abzielt. Er gefährdet geordnete politische, wirtschaftliche und soziale Strukturen und deren rechtsstaatliche Grundlagen. Terrorspezifische Elemente sind die Einschüchterung, die Druckausübung und die Destabilisierung, vgl. *v.Bubnoff*, NJW 2002, 2672.

21 Vgl. *Jahn*, ZRP 2002, 109 ff. mit weiteren Ausführungen.

22 Art. 1 des Ersten Gesetzes zur Änderung des Vereinsgesetzes vom 4.12.2001, BGBl. I, S. 3319.

23 Art. 1 und Art. 2 des Gesetzes zur Finanzierung der Terrorbekämpfung vom 10.12.2001, BGBl. I, 3436.

24 Das Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz) vom 09.01.2002, BGBl. I, S. 361, beinhaltet grob gesehen drei Schwerpunkte: Geheimdienst – Datenbeschaffung über alle Bürger – Ausländer; vgl. dazu *v.Bubnoff*, NJW 2002, 2672 (2676); *Rublack*, DuD 2002, 202 ff.

Politikern als „umfassendstes Sicherheitsgesetz in der Geschichte der Bundesrepublik Deutschland“ und „epochales Gesetzeswerk“ charakterisiert.[25]

Schon allein seines Umfangs wegen nimmt es eine herausragende Stellung ein, ordnet es doch nicht weniger als rund zweihundert Gesetzesänderungen bzw. –ergänzungen an, vor allem in den Bereichen Nachrichtendienstrecht, Bundespolizeirecht, Vereinsrecht, Ausländerrecht, Passrecht sowie dem Recht der Sicherheitsüberprüfung.[26]

Die Aufgaben und Befugnisse der Nachrichtendienste[27], namentlich des Bundesamtes für Verfassungsschutz (BfV), des Militärischen Abschirmdienstes (MAD) und des Bundesnachrichtendienstes (BND) wurden wesentlich erweitert.[28] So erstreckt sich der Beobachtungsauftrag des Bundesamtes für Verfassungsschutz sowie des Militärischen Abschirmdienstes nun auf Bestrebungen, die gegen den Gedanken der Völkerverständigung, insbesondere gegen das friedliche Zusammenleben der Völker gerichtet sind.[29]

Das BfV hat zudem umfangreiche Auskunftsbefugnisse u.a. gegenüber Banken, Post-, Telekommunikations-, Flug- und Teledienste- sowie Luftfahrtunternehmen erhalten.[30] Im Einzelnen sind dies Auskünfte:

---

25 So die Äußerungen des Abgeordneten *Dieter Wiefelspütz* sowie des Bundesministers des Inneren *Otto Schily* in der 209. Sitzung des 14. Bundestages vom 14.12.2001, abgedruckt in: Bundestagsplenarprotokoll 14/209, S. 20748 und 20761.

26 Zu den verfassungsrechtlichen Problemen des Terrorismusbekämpfungsgesetzes vgl. *Baldus*, ZRP 2002, 400 ff.

27 Zum Begriff vgl. *Roewer*, § 1 PKKG, Rn. 10.

28 Siehe dazu *König*, 2005, S. 243 ff.

29 § 3 Abs. 1 Nr. 4 BVerfSchG und § 1 Abs. 1, Satz 2 MADG, eingefügt durch Art. 1 und 2 des Terrorismusbekämpfungsgesetzes. Diese Neuregelung hat ausländerextremistische Organisationen im Blick, vgl. *Baldus*, ZRP 2002, 400. Richten sich diese Gruppierungen gegen die Bundesrepublik Deutschland und ihre Institutionen, so konnten sie schon nach bisherigem Recht nachrichtendienstlich beobachtet werden, da der Tatbestand „Bestrebungen gegen die freiheitlich-demokratische Grundordnung“ gegeben war (§ 3 Abs. 1 Nr. 1 BVerfSchG). Die Nachrichtendienste konnten auch dann tätig werden, wenn diese Gruppen vom Gebiet der Bundesrepublik aus mit gewaltsamen Mitteln gegen ausländische Staaten zu agieren beabsichtigten, denn das Bundesverfassungsschutzgesetz erlaubte schon nach seiner alten Fassung Kräfte zu observieren, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitung auswärtige Belange der Bundesrepublik Deutschland gefährdeten (§ 3 Abs. 1 Nr. 3 BVerfSchG). Eine Befugnislücke bestand aber, wenn diese Organisationen entweder nicht gegen die Bundesrepublik Deutschland vorgingen oder ihnen Gewaltanwendungen sowie entsprechende Vorbereitungshandlungen nicht nachgewiesen werden konnten, vgl. *Baldus*, ZRP 2002, 400. Diese Lücke soll durch die Neuregelung geschlossen werden. Der Gesetzgeber zielt dabei vor allem auf Gruppierungen ab, die einen „Nährboden für Entstehung extremistischer Auffassungen“ bilden sowie „Hass schüren“ und die „auch vor terroristischer Gewaltanwendung nicht zurückschrecken“; so die Formulierung in der Gesetzesbegründung BT-Dr. 14/7386, S. 84 und 91.

30 § 8 a BVerfSchG.

- über Konten, Kontobewegungen, Kontoinhaber und sonstige Berechtigte, Geldbewegungen und –anlagen und am Zahlungsverkehr Beteiligte,
- über die Umstände des Postverkehrs,
- über Namen, Anschriften und Daten über Transportleistungen und „sonstige Umstände des Flugverkehrs“ sowie
- über Telekommunikationsverkehrsdaten und Teledienstenutzungsdaten.

Dem MAD und dem BND wurden entsprechende telekommunikations- und teledienstbezogene Auskunftsbefugnisse eingeräumt.[31] Zudem dürfen die Geheimdienste unter Einsatz eines IMSI-Catchers den Standort eines Mobiltelefons bzw. einer Person ermitteln.[32]

Mit Gesetz vom 05.01.2007 wurde die Befugnisse des BfV, des MAD und BND abermals neu gefasst und erweitert.[33] Die dem BfV zustehenden Befugnisse zu besonderen Auskunftsverlangen gegenüber Luftfahrtunternehmen, Kreditinstituten sowie Telekommunikations- und Postunternehmen sind nunmehr eigenständig in § 8 a BVerfSchG geregelt und § 2 a BNDG stellt jetzt dem BND die gesamte Bandbreite der Eingriffsbefugnisse des § 8 a BVerfSchG zur Verfügung. Auch dem MAD wurden mit § 4 a MAD entsprechende umfassende Befugnisse erteilt.[34]

Zudem wurde durch das Gemeinsame-Dateien-Gesetz[35] eine Anti-Terror-Datei eingeführt[36], an der neben dem Bundeskriminalamt die Nachrichtendienste sowie das Zollkriminalamt und die Polizeibehörden des Bundes und der Länder beteiligt sind. In die Anti-Terror-Datei sind

---

31 § 4 a MADG; § 2 a BNDG. Dazu kritisch *Rublack*, DuD 2002, 202 (203), die es als Systembruch ansieht, dass die neuen kommunikationsbezogenen Auskunftsbefugnisse außerhalb des G-10-Gesetzes angesiedelt wurden. Da nach der Rechtsprechung des BVerfG auch die näheren Umstände der Kommunikation dem Fernmeldegeheimnis unterliegen, sollten ihrer Ansicht nach alle Eingriffsbefugnisse der Geheimdienste in Bezug auf Art. 10 GG daher innerhalb des G-10-Gesetzes und nicht in Spezialgesetzen geregelt sein, um ein einheitliches System der materiellen Voraussetzungen, des Anordnungsverfahrens, der Datenverarbeitungsbefugnisse und ihrer Kontrollen Gewähr zu leisten.

32 § 9 Abs. 4 BVerfSchG; § 5 MADG iVm § 9 Abs. 4 BVerfSchG eingeführt durch Art. 1 und 2 des Terrorismusbekämpfungsgesetzes. Für den BND ergibt sich der Einsatz des IMSI-Catchers aus § 3, Satz 2 BNDG iVm § 9 BVerfSchG.

33 Vgl. Terrorismusbekämpfungsergänzungsgesetz vom 05.01.2007, BGBl. I, S. 2.

34 Vgl. dazu *Roggan/Bergemann*, NJW 2007, 876 (879); *B. Huber*, NJW 2007, 881 (882).

35 Gesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder vom 22.12.2006, BGBl. I, S. 3409.

36 Vgl. Anti-Terror-Datei-Gesetz als Artikel 1 des Gemeinsame-Dateien-Gesetzes.

erhobene Daten einzustellen, für die nach sicherheitsbehördlichen Erkenntnissen tatsächliche Anhaltspunkte für einen Bezug zu einem terroristischen Hintergrund gegeben sind.[37]

Am 18.04.2007 wurde vom Bundeskabinett ein Gesetzesentwurf vorgelegt, mit dem u.a. die Richtlinie 2006/24/EG[38] umgesetzt werden soll, welche die Mitgliedsstaaten zum Erlass von Rechtsvorschriften verpflichtet, die die (Vorrats-)Speicherung betriebsbedingter Kommunikationsdaten für einen Zeitraum von mindesten sechs Monaten bis maximal zwei Jahre vorsehen.[39] Vorgesehen ist die Speicherung von Verkehrs- und Standortdaten, da diese Daten ein wertvolles Mittel bei der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten und insbesondere der Organisierten Kriminalität darstellen.[40] Eine exakte Beschreibung der Daten, die zu speichern sind, ergibt sich aus Art. 5 der Richtlinie: Dies sind insbesondere Name, Anschrift, Rufnummer, Benutzerkennung, Datum, Uhrzeit und Dauer der Kommunikation. Die Daten sind für mindestens sechs Monate und nicht mehr als zwei Jahre ab dem Zeitpunkt der Kommunikation zu speichern.[41]

---

37 Vgl. § 2 ATDG und ausführlich zu den einzelnen Tatbestandsvoraussetzungen *Roggan/Bergemann*, NJW 2007, 876 (878). Der Zugriff auf die Datei ist als automatisches Abrufverfahren ausgestaltet, § 5 ATDG. Mit den Art. 2 und 4 des Gemeinsame-Dateien-Gesetzes wurde weiter die Möglichkeit zur Errichtung sogenannter Projektdateien geschaffen. Die Projektdateien sollen eine befristete Zusammenarbeit zwischen BfV, MAD, BND und den Polizeibehörden des Bundes und der Länder, dem Zollkriminalamt sowie der Landesämter für Verfassungsschutz ermöglichen. Hierzu kritisch *Roggan/Bergemann*, NJW 2007, 876 (878 f.), die u.a. darauf hinweisen, dass eine tatbestandliche Eingrenzung, in welchen Fällen ein entsprechendes Projekt vorliegt, nicht existiert.

38 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der RL 2002/58/EG vom 15.03.2006, ABl. EG Nr. L 105, S. 54.

39 Vgl. Regierungsentwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, BT-Drucks. 16/5846, S. 17 . Siehe dazu die kritischen Würdigungen von *Leutheusser-Schnarrenberger*, ZRP 2007, 9 ff.; siehe auch *Gola/Klug*, NJW 2005, 2434 (2439); *Ulmer/Schrief*, DuD 2004, 591 (592). Die Pläne zur Vorratsdatenspeicherung von Telekommunikationsdaten gehen auf die Schlussfolgerungen des Rates für Justiz und Inneres vom 20.09.2001 zurück. Kurz nach den Terroranschlägen vom 11.09.2001 hat der Rat für Justiz und Inneres die Europäische Kommission zur Erarbeitung eines Vorschlages aufgefordert, der die Sicherheitsbehörden befähigen soll, unter Nutzung der elektronischen Telekommunikation begangene Straftaten besser aufzuklären und zu verfolgen, vgl. Schlussfolgerung Nr. 4 des Rates für Justiz und Inneres vom 20.09.2001, Ratsdok. 12156/01. Von einer Speicherung von Telekommunikationsdaten auf "Vorrat" ist auf Ratsebene erstmals in der Erklärung zum Kampf gegen den Terrorismus die Rede gewesen. In dieser Erklärung, als Reaktion auf die Terroranschläge von Madrid, beauftragte der Europäische Rat den Rat der EU, Vorschläge für Rechtsvorschriften zu beraten, welche die Aufbewahrung von Verkehrsdaten durch die Anbieter von Telekommunikationsdiensten regeln, vgl. Entwurf einer Erklärung zum Kampf gegen den Terrorismus vom 25.03.2004, Ratsdok.. 7764/04, S. 4. Siehe zur Entwicklung auch *Hartung*, in: Wilms/Masing/Jochum (Hrsg.), § 96 TKG, Rn. 19 ff.

40 Vgl. die Erwägungsgründe der Richtlinie.

41 Art. 6 der Richtlinie.

Mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung und andere verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG wurde den europäischen Vorgaben zum 01.01.2008 nachgekommen.[42] Durch die neugeschaffenen §§ 113 a und 113 b im Telekommunikationsgesetz wurde die Vorratsdatenspeicherung festgeschrieben.[43] Danach haben öffentlich zugängliche Telekommunikationsdienste Verkehrsdaten sechs Monate im Inland oder in einem anderen Mitgliedstaat der Europäischen Union zu speichern. Die aufgrund § 113 a TKG gespeicherten Daten dürfen gemäß § 113 b TKG zur Verfolgung von Straftaten, zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit oder zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und das militärischen Abschirmdienstes auf Verlangen an die zuständigen Behörden übermittelt werden, soweit dies in den jeweiligen gesetzlichen Bestimmungen unter Bezugnahme auf § 113 a TKG vorgesehen und die Übermittlung im Einzelfall angeordnet ist.[44]

2. Rechtsänderungen in den Bundesländern

Der Ausbau des Sicherheitsrechts erfolgte auch auf Länderebene. So erhielten die Landesverfassungsschutzbehörden die Befugnis zur präventiven Wohnraumüberwachung.[45] Doch nicht nur auf der Ebene des (Landes-) Verfassungsschutzes, sondern auch auf der Ebene der „einfachen Gefahrenabwehr“ haben die Anschläge vom 11. September Spuren hinterlassen.

---

42 Vgl. BGBl. 2007, S. 3198.

43 § 113 a TKG enthält in seinem Abs. 2 die Speicherpflicht der Anbieter von öffentlich zugänglichen Telefondiensten für die dort genannten Daten. § 113 b TKG regelt die Verwendung der nach § 113 a TKG gespeicherten Daten, BGBl. I, 2007, S. 3198 (3207 f.). § 113 b TKG enthält jedoch keine eigenständige Abrufbefugnis; diese muss durch das jeweils geltende Fachrecht geregelt werden, vgl. BVerfG, Beschluss vom 11.03.2008 – 1 BvR 256/08 – Rn. 10.

44 Mit Beschluss vom 11.03.2008 – 1 BvR 256/08 hat das BVerfG im Wege einer einstweiligen Anordnung bestimmt, dass Verkehrsdaten zwar gemäß § 113 a TKG gespeichert werden dürfen, eine Weitergabe der Daten an eine Strafverfolgungsbehörde aber nur erfolgen darf, wenn die Voraussetzungen des § 100 a Abs. 1 und 2 StPO vorliegen. Das BVerfG hat die Folgen, die eintreten würden, wenn die einstweilige Anordnung nicht erginge, die Verfassungsbeschwerde aber später in der Hauptsache Erfolg hätte, gegen die Nachteile abgewogen, die entstünden, wenn die begehrte einstweilige Anordnung erlassen würde, der Verfassungsbeschwerde aber der Erfolg zu versagen wäre, vgl. BVerfG, Beschluss vom 11.03.2008 – 1 BvR 256/08, Rn. 139. In der Datenspeicherung allein hat das BVerfG noch keine so schwerwiegende Nachteile gesehen, dass es die Aussetzung der Datenbevorratung als geboten angesehen hätte, da sich die Einschränkungen von Freiheit und Privatheit der betroffenen Personen erst mit dem Abruf der Daten konkretisieren (vgl. Rn. 149). In dem Verkehrsdatenabruf selbst hat das BVerfG jedoch einen so schwerwiegenden und nicht mehr rückgängig zu machenden Eingriff in das Grundrecht des Art. 10 Abs. 1 GG gesehen, dass eine Übermittlung nur in den Fällen zulässig ist, in denen die Voraussetzungen des § 100 a Abs. 1 und Abs. 2 StPO vorliegen (vgl. Rn. 156, 164 ff.). Denn unter diesen Voraussetzungen hat der Gesetzgeber auch gewichtige Eingriffe in Art. 10 GG als gerechtfertigt erachtet (vgl. Rn. 167 ff.).

45 Siehe dazu die Regelungen in Art. 6 a BayVSG; § 7 ThürVSG; § 8 HbgVerfSchG; § 7 NWVerfSchG.

Die Polizeigesetze der Länder Thüringen, Niedersachsen, Bayern, Rheinland-Pfalz und Hessen führten eine präventive Telekommunikationsüberwachung ein und erweiterten damit das polizeiliche Instrumentarium.[46] Vier dieser fünf Landesgesetzgeber sehen eine gesetzliche Regelung der Telekommunikationsüberwachung in ihren Polizeigesetzen als notwendig an, um mit dieser Fortschreibung des Polizei- und Sicherheitsrechts den neuen Erscheinungsformen der schweren und grenzüberschreitenden Kriminalität, insbesondere der Organisierten Kriminalität[47] sowie der „Ausbreitung des Extremismus“ und dem internationalen Terrorismus Rechnung zu tragen.[48]

II. Themenabgrenzung und Gegenstand der Untersuchung

Thema dieser Arbeit ist die durch Landesgesetz eingeführte Überwachung der Telekommunikation zu Zwecken der Gefahrenabwehr. Herangezogen für die Untersuchung werden die Polizeigesetze der Länder Thüringen[49], Niedersachsen[50], Bayern[51], Rheinland-Pfalz[52] und Hessen[53].

---

46 Ebenfalls wurde durch das Gesetz zur Erhöhung der öffentlichen Sicherheit in Hamburg vom 16.06.2005, HmbGVBl. Nr. 21, S. 233, die präventive Telekommunikationsüberwachung durch die §§ 10 a – d in das Gesetz über die Datenverarbeitung der Polizei (HmbPolDVG) aufgenommen. Regelungen zur präventiven Telekommunikationsüberwachung finden sich seit dem Jahr 2006 auch in § 33 b BbgPolG und § 34 a SOG M-V. Das schleswig-holsteinische Landesverwaltungsgesetz wurde durch das Gesetz zur Anpassung der gefahrenabwehrrechtlichen und verwaltungsverfahrensrechtlichen Bestimmungen des Landesverwaltungsgesetz vom 13.04.2007, GVBl. 2007, S. 234, geändert und mit § 185 a die Ermächtigung der Polizei zur präventiven Telekommunikationsüberwachung eingeführt.

47 Zum Begriff vgl. BVerfGE 109, 279 (338 f.): „In der öffentlichen Diskussion wird meist der Begriffsbestimmung der gemeinsamen Arbeitsgruppe der Innenminister- und der Justizministerkonferenz gefolgt. Danach versteht man unter >> Organisierter Kriminalität << die vom Gewinn- oder Machtstreben bestimmte planmäßige Begehung von Straftaten, die einzeln oder in ihrer Gesamtheit von erheblicher Bedeutung sind, wenn mehr als zwei Beteiligte auf längere oder unbestimmte Dauer arbeitsteilig unter Anwendung von Gewalt oder anderer zur Einschüchterung geeigneter Mittel oder unter Einflussnahme auf Politik, Medien, öffentliche Verwaltung, Justiz oder Wirtschaft zusammenwirken.“

48 LT-Drucks. Th. 3/2128, S. 1; LT-Drucks. Nds. 15/240, S. 8; LT-Drucks. Bayern 15/2096, S. 2; LT-Drucks. RhPf. 14/2287, S. 30.

49 Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei vom 04.06.1992, GVBl. 1992, S. 199, zuletzt geändert durch Artikel 1 des Thüringer Gesetzes zur Änderung des Polizei- und Sicherheitenrechts vom 27.06.2002, GVBl. 2002, S. 247. Die präventive Telekommunikationsüberwachung in § 34 a ThPAG wurde durch Artikel 1 des Thüringer Gesetzes zur Änderung des Polizei- und Sicherheitenrechts vom 27.06.2002, GVBl. 2002, S. 247 eingeführt.

50 Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung in der Fassung der Bekanntmachung vom 19.01.2005, Nds.GVBl.2005, S. 9, zuletzt geändert durch Art. 2 des Gesetzes zur Neuregelung des Justizvollzugs in Niedersachsen, GVBl. 2007, S. 720. Die präventive Telekommunikationsüberwachung in §§ 33 a – c Nds.SOG wurde durch Art. 1 des Gesetzes zur Änderung des Niedersächsischen Gefahrenabwehrgesetzes vom 11.12.2003, Nds.GVBl. 2003, S. 414 eingeführt. Mit Urteil vom 27.07.2005 hat das BVerfG § 33 a Abs. 1 Nr. 2 und Nr. 3 Nds.SOG für mit dem Grundgesetz unvereinbar und nichtig erklärt, vgl. BVerfGE 113, 349 ff. Durch Art. 2 des Gesetzes zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung vom 25.11.2007, Nds.GVBl. 2007, S. 654, wurden neben weiteren Änderungen die Regelungen des § 33 a Abs. 1 Nr. 2 und 3 Nds.SOG gestrichen. Soweit das

Die Untersuchung orientiert sich primär am Bayerischen Polizeiaufgabengesetz, wobei Abweichungen in den anderen Landespolizeigesetzen kurz dargestellt werden.[54]

Zunächst wird in einem Rückblick die Situation dargestellt, die bis zum Erlass der polizeigesetzlichen Regelungen bestanden hat. Untersucht wird dabei, ob den Landespolizeibehörden bereits aufgrund bestehender Regelungen die präventive Telekommunikationsüberwachung möglich war bzw. ob ihnen die Telekommunikationsdaten anderer Behörden zur Verfügung stehen. Eingegangen wird dabei insbesondere auf die Problematik des Datenaustausches sowohl zwischen den Verfassungsschutz- und den Gefahrenabwehrbehörden als auch zwischen den Strafverfolgungs- und Gefahrenabwehrbehörden. Herausgearbeitet wird, inwiefern das Zitiergebot des Art. 19 Abs. 1, Satz 2 GG einer Datenweitergabe entgegensteht und welche weiteren verfassungsrechtlichen Anforderungen an die Übermittlungsvoraussetzungen zu stellen sind.

Es folgt die Erläuterung, welche Informationen unter den Begriff der Telekommunikationsdaten fallen und die Darstellung, wie der Zugriff auf diese Daten durch Landespolizeibehörden unter Inanspruchnahme von Telekommunikationsdienstleistungsunternehmen erfolgt und welche Voraussetzungen die Landesgesetze erfüllen müssen, damit den Polizeibehörden der Datenzugriff offen steht. In diesem Zusammenhang wird besonderes Augenmerk auf die Frage der Gesetzgebungskompetenz der Länder für die Verpflichtung der Telekommunikationsunternehmen zur Überwachungsermöglichung und Auskunftserteilung gerichtet.

Nds.SOG in seiner Ausgestaltung, die es durch das Gesetz vom 19. 01.2005, GVBl. 2005, S. 9, erhalten hat, gemeint ist, erfolgt der Zusatz Nds.SOG 2005.

51 Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei (Polizeiaufgabengesetz) in der Fassung der Bekanntmachung vom 14.09.1990, GVBl. 1990, S. 397, zuletzt geändert durch § 2 des Gesetzes vom 08.07.2008, GVBl. 2008, S. 365. Die präventive Telekommunikationsüberwachung in Art. 34 a – c PAG wurde durch § 1 des Gesetzes zur Änderung des Polizeiaufgabengesetzes und des Parlamentarischen Kontrollgremium-Gesetzes vom 24.12.2005, GVBl. 2005, S. 641 eingeführt.

52 Polizei- und Ordnungsbehördengesetz in der Fassung vom 10.11.1993, GVBl. 1993, S. 595, zuletzt geändert durch Art. 1 des sechsten Landesgesetzes zur Änderung des Polizei- und Ordnungsbehördengesetzes vom 25.07.2005, GVBl. 2005, S. 320. Die präventive Telekommunikationsüberwachung in § 31 POG wurde durch das Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes und anderer Gesetze vom 02.03.2004, GVBL. 2004, 202 eingeführt.

53 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung vom 26.06.1990, GVBl. I, S. 197, 534, in der Fassung vom 14.01.2005, GVBl. I, S.14. Die präventive Telekommunikationsüberwachung in § 15 a HSOG wurde durch die Neufassung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung vom 14.01.2005, GVBl. I, S.14 eingeführt.

54 Das Bayerische Polizeiaufgabengesetz wurde gewählt, da es die ausführlichsten Regelungen zur Telekommunikationsüberwachung enthält, die Telekommunikationsüberwachung sowohl für die eigentliche Gefahrenabwehr als auch zur Verhinderung von Straftaten vorsieht sowie den Einsatz des IMSI-Catchers regelt. Damit deckt es nahezu alle Regelungsbereiche ab, die auch in den anderen Polizeigesetzen bei der präventiven Telekommunikationsüberwachung zu finden sind.

Erörtert wird weiter die Problematik der “länderübergreifenden Sachverhalte“, also des (möglichen) Zugriffs der Landespolizeibehörden auf Telekommunikationsdaten und –verbindungen außerhalb des jeweiligen Bundeslandes. Bezug genommen wird dabei auf die Möglichkeit einer „Auslandstelekommunikationsüberwachung“ und die verfassungsrechtlichen Voraussetzungen, die bei einer bundesweiten Geltung von Landesgesetzen zu beachten sind. Erörtert wird insbesondere die verfassungsrechtliche Zulässigkeit einer „Bundesländergrenzen überschreitenden Kommunikationsüberwachung“ im Hinblick auf den Grundsatz bundesfreundlichen Verhaltens.

Danach werden die neuen Regelungen an den Vorgaben des Grundgesetzes und der EMRK gemessen. Herausgearbeitet wird dabei, welche Anforderungen an die Eingriffsvoraussetzungen zu stellen sind, um eine präventive Telekommunikationsüberwachung (verfassungsrechtlich) rechtfertigen zu können. Darüber hinaus erfolgt ein kurzer Vergleich mit den Regelungen der StPO zur repressiven Telekommunikationsüberwachung und mit den Normen zur Standortbestimmung in den Polizeigesetzen; auch werden rechtspolitische Aspekte angesprochen, die sich vor allem im Hinblick auf Gemengelagen ergeben. Änderungsvorschläge zu den neuen gesetzlichen Regelungen werden herausgearbeitet und zur Diskussion gestellt.

Es schließt sich die Darstellung an, welche (verfassungsrechtlichen) Voraussetzungen bei der Weitergabe der Telekommunikationsdaten zu erfüllen, insbesondere welche Anforderungen bei Zweckänderungen zu stellen sind. Differenziert wird dabei zwischen der Weitergabe an andere Gefahrenabwehrbehörden und Behörden der Strafverfolgung. In diesem Zusammenhang wird untersucht, ob die landesgesetzlichen Regelungen diesen Vorgaben entsprechen.

Schließlich werden die Schlussfolgerungen der Untersuchung dargestellt und die Kritikpunkte an den landesgesetzlichen Regelungen zur präventiven Telekommunikationsüberwachung hervorgehoben.

Kapitel 2: Entwicklung und bisherige gesetzliche Grundlagen der Telekommunikationsüberwachung in der Bundesrepublik Deutschland

I. Repressive Telekommunikationsüberwachung

Die Überwachung und Aufzeichnung der Telekommunikation ist vor allem aus dem repressiven Bereich bekannt. Sie dient als Ermittlungsmaßnahme zur Aufklärung begangener Straftaten und hat die Strafverfolgung und Strafrechtspflege zum Zweck.

Strafprozessuale telekommunikative Auskunftsersuchen wurden bis Ende 2001 auf § 12 FAG[55] gestützt.[56] Nach § 12 FAG konnte der Richter und bei Gefahr in Verzug auch die Staatsanwaltschaft in strafgerichtlichen Untersuchungen Auskunft über den Fernmeldeverkehr verlangen, wenn die Mitteilungen an den Beschuldigten gerichtet waren oder wenn Tatsachen vorlagen, aus denen zu schließen war, dass die Mitteilungen vom Beschuldigten herrührten oder für ihn bestimmt waren und dass die Auskunft für die Untersuchung Bedeutung hatte.[57]

Mit der Einführung elektromechanischer Vermittlungstechnik verlor die Vorschrift an Bedeutung, da bei dieser Technik keine entsprechenden Daten anfielen.[58]
Durch die Digitalisierung des Telefonnetzes erlangte § 12 FAG eine neue Bedeutung.[59] Die elektromechanische Vermittlungstechnik wurde durch digitale Technik ersetzt. Diese ist geeignet, alle Fernmeldedienste zu integrieren, also neben der Sprache auch Daten, Texte und

---

55 Fernmeldeanlagengesetz vom 14.01.1928, RGBl. I, S. 8 ff.

56 Einen guten Überblick über die technische Entwicklung der Telekommunikationsüberwachung enthält das Urteil des BGH vom 12.03.2003 in NJW 2003, 1787 (1790).

57 Siehe zum Auskunftsanspruch nach § 12 FAG *Hansen-Oest*, in: Schmidt/Königshofen/Zwach, 85 TKG, Rn. 37 und *Bär*, CR 1993, 634 (637). Die Norm bezog sich vornehmlich auf Daten handvermittelter Gespräche, bei denen Teilnehmer und Gesprächsdauer manuell auf so genannten Gesprächsblättern festgehalten wurden, deren Herausgabe dann von den Strafverfolgungsbehörden nach § 12 FAG verlangt werden konnte, vgl. *R.P. Schenke*, AöR 125 (2000), 1 (5).

58 Vgl. *R.P. Schenke*, AöR 125 (2000), 1 (5); *Stenger*, CR 1990, 786 (793); *Welp*, NStZ 1994, 209 (210). Diese Fernmeldetechnik übermittelte die Sprache als analoge Sequenz von Stromschwankungen, die der Tonhöhe und Lautstärke des gesprochenen Wortes entsprach. Die notwendigen Schaltungen für eine Verbindung wurden durch elektromagnetische Stellgeräte bewirkt, die den Schalter in die den gewählten Ziffern entsprechenden Positionen brachten. Nach Ende der Verbindungen gingen die Schalter in ihre Ausgangsposition zurück. Die Verbindungsdaten blieben also nur bis zum Ende des Gesprächs erhalten. Danach waren beim Netzbetreiber in der Regel keine Informationen mehr vorhanden, die für ein Strafverfahren beansprucht werden konnten. Lediglich ein Summenzähler erfasste, ohne Identifizierung einzelner Verbindungen, die für den Anschluss angefallenen Entgelteinheiten, vgl. *Welp*, NStZ 1994, 209 (210).

59 Vgl. *R.P. Schenke*, AöR 125 (2000), 1 (5); *Königshofen*, Archiv PT 1994, 39 (48); *Kubicek* DuD 1995, 656 (658); *Bär* CR 1993, 634 (637).

Bilder in einem Netz zu übertragen. Die dazu eingesetzten EDV-Geräte erzeugen im digitalen Netz einen Datensatz, der neben den Nummern der verbundenen Anschlüsse auch das Datum, die Uhrzeit und die Dauer der Verbindung sowie die Art des in Anspruch genommenen Fernmeldedienstes enthält.[60] Entsprechendes gilt für den Mobilfunk, bei dem die gespeicherten Verbindungsdaten zusätzlich auch den Standort der vermittelnden Funkzelle umfassen.[61] Die Bundesrepublik Deutschland besitzt aufgrund der weitgehend abgeschlossenen Umstellung der Fernmeldenetze auf das ISDN-System mittlerweile eine der weltweit modernsten Infrastrukturen auf dem Gebiet der Telekommunikation.[62]

Die Möglichkeiten, die sich durch die moderne Übertragungstechnik den Strafverfolgungsbehörden bei der Telekommunikationsüberwachung bieten, waren vom damaligen Gesetzgeber bei den Eingriffen in das Fernmeldegeheimnis durch § 12 FAG nicht berücksichtigt worden.[63] Wegen der geringen Voraussetzungen die § 12 FAG vorsah und der daraus resultierenden Kritik[64], sollte eine entsprechende Befugnis in die StPO eingefügt werden.[65] § 12 FAG sollte zum 31.12.1997 außer Kraft treten[66] und es war eine Neuregelung in § 99 a StPO im Entwurf zum TKG-Begleitgesetz geplant.[67] Der Entwurf fand jedoch vor allem wegen mangelnder Berücksichtigung von Zeugnisverweigerungsrechten keine Zustimmung.[68] So wurde die Fortgeltung des § 12 FAG bis zum 31.12.1999[69] und im Dezember 1999 wiederum bis zum 31.12.2001 beschlossen.[70] Durch das Gesetz zur Änderung der StPO vom 20.12.2001[71] wurde die Telekommunikationsauskunft neu geregelt und mit den §§ 100 g und 100 h in die StPO eingestellt.[72]

---

60 Vgl. *R.P. Schenke*, AöR 125 (2000), 1 (5); *Kubicek*, DuD 1995, 656 (658); *Walz*, CR 1990, 138 (140); *Welp*, NStZ 1994, 209 (210); *Palm/Roy*, NJW 1996, 1791 (1796); *Kubicek/Bach*, CR 1991, 489 (490); *Klesczewski*, StV 1993, 382 f.

61 Vgl. *Welp*, NStZ 1994, 209 (210); *R.P. Schenke*, AöR 125 (2000), 1 (5); *Kubicek/Bach*, CR 1991, 489 (491).

62 Vgl. *Klesczewski*, JZ 1997, 719.

63 Vgl. *Hansen-Oest*, in: Schmidt/Königshofen/Zwach, § 85 TKG, Rn. 37.

64 Vgl. *Königshofen*, Archiv PT 1994, 39 (48); *Ehmer*, in: BeckTKG-Komm, § 88 TKG, Rn. 19.

65 Vgl. *Hansen-Oest*, in: Schmidt/Königshofen/Zwach, § 85 TKG, Rn. 37; *Ehmer*, in: BeckTKG-Komm, § 88 TKG, Rn. 19.

66 § 28 FAG, eingeführt durch Art. 5 Nr. 20 PTNeuOG, BGBl. I 1994, S. 2325. Vgl. auch *Loewer*, in: v.Münch/Kunig (Hrsg.), Art. 10 GG, Rn. 41.

67 Vgl. BT-Drucks. 13/8016, S. 9.

68 Vgl. BT-Drucks. 13/8016, S. 38 ff; Vgl. auch *Loewer*, in: v.Münch/Kunig (Hrsg.), Art. 10 GG, Rn. 41.

69 Begleitgesetz zum Telekommunikationsgesetz vom 17.12.1997, BGBl. I, S. 3108.

70 Vgl. *Hansen-Oest*, in: Schmidt/Königshofen/Zwach, § 85 TKG, Rn. 37.

71 BGBl. I, S. 3879.

72 Ausführlich dazu *Welp*, GA 2002, 535 ff. Diese Regelungen waren bis zum 31.12.2004 befristet, vgl. Art. 2 des Gesetzes zur Änderung der StPO vom 20.12.2001, BGBl. I, S. 3879. Die Befristung wurde jedoch Ende 2004 verlängert bis zum 01.01.2008, vgl. Gesetz vom 09.12.2004, BGBl. I, S. 3231. Durch das Ge-

Die repressive Telekommunikationsüberwachung ist damit insgesamt in der StPO geregelt. Eingeführt wurde mit dem neuen § 100 i StPO[73] zudem der Einsatz des IMSI-Catchers.

II. Präventive Telekommunikationsüberwachung

1. Die Überwachung nach dem G-10-Gesetz

Die präventive Telekommunikationsüberwachung war bislang nur aus dem Verfassungs(schutz)recht bekannt.

Die Überwachung des Fernmeldeverkehrs zu präventiven Zwecken ist mit dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G-10-Gesetz) vom 13.08.1968[74] für die Verfassungsschutzbehörden und Nachrichtendienste eingeführt worden. Das G-10-Gesetz ist als Art. 1 des Gesetzes zur Neuregelung von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses vom 26.06.2001 neu verkündet worden[75] und hat seitdem zahlreiche Änderungen erfahren.[76]

Die deutschen Nachrichtendienste – das Bundesamt für Verfassungsschutz, der Bundesnachrichtendienst und der Militärische Abschirmdienst – sind besondere Sicherheitsbehörden des Bundes. Diese Dienste nehmen präventiv-polizeiliche Aufgaben wahr, da ihnen der Staatsschutz und damit die Wahrung des Kernbereichs innerer und äußerer Sicherheit obliegt.[77]

Die Sicherheitsbehörden des Bundes sind nach dem G-10-Gesetz zur Telekommunikationsüberwachung und Auskunftsanordnung[78] zur Abwehr von drohenden Gefahren für die frei-

---

setz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, BGBl. I, 2007, S. 3198, wurden die §§ 100 g und 100 h StPO neu gefasst und geltend nunmehr unbefristet.

73 Gesetz vom 06.08.2002, BGBl. I, S. 3018.

74 BGBl. I, S. 949.

75 BGBl. I, S. 1254, berichtigt S. 2298.

76 So sind beispielsweise Änderungen durch das Terrorismusbekämpfungsgesetz, das 34. Strafrechtsänderungsgesetz und das Gesetz zur Umsetzung des Ratsbeschlusses zur Terrorismusbekämpfung vorgenommen worden. Zuletzt wurde das G-10-Gesetz geändert durch Art. 5 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie der Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007, BGBl. I, S. 3198.

77 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 93; *König*, 2005, S. 27.

78 Die Befugnis zur Auskunftsanordnung ergibt sich zudem aus § 8 a Abs. 2 BVerfSchG, soweit dies zur Aufklärung von Bestrebungen oder Tätigkeiten erforderlich ist und tatsächliche Anhaltspunkte für schwerwiegende Gefahren für die nach § 3 Abs. 1 BVerfSchG genannten Schutzgüter vorliegen. Vgl. dazu auch die Verweisungsvorschriften in § 4 a MADG und § 2 a BNDG.

heitliche demokratische Grundordnung, den Bestand und die Sicherheit des Bundes oder eines Landes einschließlich der Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantikvertrages berechtigt.[79] Beschränkungen des Fernmeldeverkehrs sind möglich in Einzelfällen und zur strategischen Überwachung.

Eine Einzelfallbeschränkung kommt in Betracht, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand die in § 3 Abs. 1 G-10-Gesetz aufgeführten Straftaten plant, begeht oder begangen hat. Es sind dies Straftaten des Friedens- oder Hochverrats, der Gefährdung des demokratischen Rechtsstaats, des Landesverrats und der Gefährdung der äußeren Sicherheit, gegen die Landesverteidigung, gegen die Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantikvertrages sowie weiterer Straftaten nach dem Strafgesetzbuch, soweit diese sich gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes richten sowie Straftaten nach § 95 Abs. 1 Nr. 7 des Aufenthaltsgesetzes.

Strategische Beschränkungen, zu denen nur der Bundesnachrichtendienst berechtigt ist, sind möglich für internationale Telekommunikationsbeziehungen, soweit eine gebündelte Übertragung erfolgt. [80] Sie sind zulässig zur Sammlung von Informationen über Sachverhalte, deren Kenntnis notwendig ist, um die Gefahr eines bewaffneten Angriffs auf die Bundesrepublik Deutschland, der Begehung internationaler terroristischer Anschläge mit unmittelbarem Bezug zur Bundesrepublik Deutschland, der internationalen Verbreitung von Kriegswaffen sowie des unerlaubten Außenwirtschaftsverkehrs, der unbefugten Verbringung von Betäubungsmitteln in nicht geringer Menge in die Bundesrepublik, der Beeinträchtigung der Geldwertstabilität im Eurowährungsraum durch im Ausland begangene Geldfälschungen oder der international organisierten Geldwäsche in Fällen von erheblicher Bedeutung rechtzeitig zu erkennen und ihnen zu begegnen.

---

79 § 1 Abs. 1 G-10-Gesetz.

80 § 5 Abs. 1 G-10-Gesetz. Umfasst sind von der Überwachung nach § 5 Abs. 1 G-10-Gesetz leitungsgebundene und der nichtleitungsgebundene Fernmeldeverkehr, also auch Kommunikation via Satellit und Richtfunk, vgl. *B. Huber*, NJW 2001, 3296. Schon nach § 3 Abs. 2 G-10-Gesetz a.F. war dem BND aufgegeben, aus einer Vielzahl von Telekommunikationen die relevanten durch Suchbegriffe herauszufiltern. Das setzt eine gebündelte Übertragung voraus. Kabel, die zu einem einzelnen, individuellen Anschluss führen, dürfen nicht Gegenstand der strategischen Fernmeldekontrolle sein; so die Gesetzesbegründung BT-Drucks. 14/5655, S. 17 und 18.

Dem Bundesamt für Verfassungsschutz obliegen nach § 3 Abs. 1 BVerfSchG vor allem die Sammlung und Auswertung von Informationen über Bestrebungen, die gegen die freiheitliche demokratische Grundordnung bzw. gegen den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind, über geheimdienstliche Tätigkeiten für eine fremde Macht in der Bundesrepublik, Bestrebungen, die durch Anwendung von Gewalt auswärtige Belange der Bundesrepublik gefährden sowie Bestrebungen, die gegen den Gedanken der Völkerverständigung gerichtet sind.[81]

Der Aufgabenbereich des Militärischen Abschirmdienstes umfasst die Sammlung und Auswertung von Informationen über verfassungsfeindliche Bestrebungen und Spionagetätigkeit[82] sowie über Bestrebungen, die gegen den Gedanken der Völkerverständigung gerichtet sind. Im Unterschied zum Bundesamt für Verfassungsschutz ist der Aufgabenbereich des Militärischen Abschirmdienstes immer nur dann eröffnet, wenn der Geschäftsbereich des Bundesministeriums für Verteidigung berührt ist.[83]

Im Gegensatz zum Bundesamt für Verfassungsschutz und zum Militärischen Abschirmdienst handelt es sich beim Bundesnachrichtendienst um einen Auslandsnachrichtendienst.[84] Er sammelt Informationen zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, und wertet diese aus.[85]

Neben der Überwachung der Telekommunikation können die Sicherheitsbehörden des Bundes auch Auskunft über Telekommunikationsverbindungsdaten und Teledienstenutzungsdaten von den Telekommunikationsunternehmen verlangen.[86]

---

81 § 3 Abs. 1 BVerfSchG. Die Bundespolizei nimmt gemäß § 10 Abs. 1 BPolG für das Bundesamt für Verfassungsschutz auf dessen Anforderung Aufgaben nach § 3 Abs. 1 BVerfSchG auf dem Gebiet der Funktechnik und funkbetrieblichen Auswertung wahr. Da dies nur gilt, soweit der Funkverkehr nicht dem Fernmeldegeheimnis unterliegt, wird diese Vorschrift nicht weiter untersucht.

82 Vgl. auch *Dau*, DÖV 1991, 661 (663 ff.).

83 Das ist der Fall, wenn sich die Bestrebungen oder Tätigkeiten gegen Personen, Dienststellen oder Einrichtungen im Geschäftsbereich des Bundesministers der Verteidigung richten und der vermutete Täterkreis dessen Geschäftsbereich angehört, § 1 MADG.

84 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 99.

85 § 1 Abs. 2 BNDG.

86 § 8 a Abs. 2 BVerfSchG; § 4 a MADG; § 2 a BNDG.

2. § 23 a Zollfahndungsdienstgesetz (§§ 39 – 41 Außenwirtschaftsgesetz)[87]

Nach § 23 a ZFdG[88] ist das Zollkriminalamt berechtigt, zur Verhütung von Straftaten nach dem Kriegswaffenkontrollgesetz dem Brief-, Post- oder Fernmeldegeheimnis unterliegende Sendungen zu öffnen und einzusehen sowie den Fernmeldeverkehr zu überwachen und aufzuzeichnen. Gleiches gilt, wenn eine erhebliche Gefahr für die öffentliche Sicherheit und Ordnung vorliegt, wenn ohne Genehmigung oder Entscheidung nach der Verordnung (EG) Nr. 1334/2000 oder nach den §§ 5 c oder 5 d der Außenwirtschaftverordnung die Ausfuhr bestimmter Güter vorbereitet wird.

Die Überwachungsbefugnis bezieht sich ausdrücklich nur auf Straftaten nach dem Kriegswaffenkontrollgesetz und die Gefahrenabwehr wegen der Ausfuhr bestimmter Güter; eine allgemeine Überwachung zu Gefahrenabwehrzwecken ist dagegen nicht vorgesehen.

3. § 8 c Abs. 1, Abs. 2 Nr. 2 VEME PolG

§ 8 c Abs. 1, Abs. 2 Nr. 2 VEME PolG[89] und die ihm entsprechenden Normierungen in den Landespolizeigesetzen sehen als besonderes Mittel der Datenerhebung den verdeckten Einsatz technischer Mittel zur Anfertigung von Lichtbildern und Bildaufzeichnungen sowie zum Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes auf Tonträger vor.
Vereinzelt wurde die Ansicht vertreten, dass von diesen Normen auch die Überwachung der Telekommunikation umfasst ist. So ging *Globig*[90] ohne Begründung davon aus, dass § 15 HSOG, der den Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen oder –aufzeichnungen sowie zum Abhören oder Aufzeichnen des gesprochenen Wortes regelt, auch die Anordnung von Telefonabhörmaßnahmen zu präventiven Zwecken unter vergleichbaren

---

87 Nach den §§ 39 – 41 AWG war das Zollkriminalinstitut berechtigt, zur Verhütung von Straftaten nach dem Außenwirtschaftsgesetz oder dem Kriegswaffenkontrollgesetz dem Brief-, Post- und Fernmeldegeheimnis unterliegende Sendungen zu öffnen und einzusehen sowie den Fernmeldeverkehr zu überwachen und aufzuzeichnen. Da das BVerfG durch Beschluss vom 03.03.2004 (BVerfGE 110, 33 ff.)die §§ 39 - 41 AWG für unvereinbar mit dem Grundgesetz erklärt hat, sind die §§ 23 a ff. ZFdG als „Nachfolgeregelung“ in das Zollfahndungsdienstgesetz eingefügt worden.

88 Zollfahndungsdienstgesetz in der Fassung vom 16.08.2002 geändert durch das Gesetz zu Neuregelung der präventiven Telekommunikations- und Postüberwachung durch das Zollkriminalamt und zur Änderung der Investitionszulagengesetze 2005 und 1999 vom 21.12.2004, BGBl. I, S. 3603, geändert durch Art. 26 des Gesetzes zur Umbenennung des Bundesgrenzschutzes in Bundespolizei vom 21. Juni 2005, BGBl. I, S. 1825; zuletzt geändert durch Art. 4 des Zweiten Gesetzes zur Änderung des Finanzverwaltungsgesetzes und anderer Gesetze vom 13.12.2007, BGBl. I, S. 2897.

89 Musterentwurf eines einheitlichen Polizeigesetzes (Stand 25.11.1977) mit Änderungen des Vorentwurfs zur Änderung des ME PolG (Stand 12.3.1986), abgedruckt als Anhang in *W.-R. Schenke*, 2007, S. 395 ff.

90 *Globig*, ZRP 1991, 81 (84); siehe auch *ders.*, ZRP 1991, 289 (290).

Voraussetzungen, wie dies § 100 a StPO für den repressiven Bereich vorsieht, erlaubt. Auch *Sproß*[91] nahm wohl an, dass durch die Datenerhebung des nicht öffentlich gesprochenen Wortes in oder aus Wohnungen neben dem G-10-Gesetz und den §§ 100 a und b StPO eine weitere Rechtsgrundlage für die Überwachung des Fernmeldeverkehrs geschaffen wurde.

Eine Überwachung der Telekommunikation[92] ist entgegen diesen Auffassungen von § 8 c Abs. 1, Abs. 2 Nr. 2 VEME PolG und den dieser Vorschrift entsprechenden Ermächtigungsnormen nicht umfasst[93]:

Entscheidend für die Anwendbarkeit der oben erwähnten Ermächtigungsgrundlagen auf eine präventiv-polizeiliche Telefonüberwachung ist zunächst, ob sich die zur Telefonüberwachung benutzten Geräte als „technische Mittel zum Abhören und Aufzeichnen des gesprochenen Wortes“ einstufen lassen.[94]

Dagegen spricht schon der Wortlaut der einschlägigen Vorschriften. Die Eingrenzung auf das gesprochene Wort stellt klar, dass das originär geäußerte menschliche Wort, nicht aber eine Wiedergabe oder Umgestaltung desselben gemeint ist. Damit scheidet eine Abhörung oder Aufzeichnung bereits konservierter Äußerungen aus.[95]

Allein nach der Wortlautauslegung lassen sich technische Mittel zum Abhören und Aufzeichnen des gesprochenen Wortes als Vorrichtungen jeglicher Art verstehen, welche geeignet sind, das geäußerte Wort unmittelbar durch technische Verstärkung oder Übertragung über seinen natürlichen Schallbereich hinaus akustisch wahrnehmbar und mittels eines Datenträgers reproduzierbar zu machen.[96] Auch daran zeigt sich, dass die Telekommunikationsüberwachung nicht unter den beschriebenen Tatbestand fallen kann. Denn zum einen sind die geäußerten Worte infolge der Funktionsweise eines Telefons vor ihrer Aufzeichnung elektro-

---

91 *Sproß*, NVwZ 1992, 642 (644).

92 Diese Ausführungen haben lediglich Bedeutung für die Aufzeichnung und Überwachung der Telekommunikation. Keinesfalls lassen sich aus den erwähnten Ermächtigungsgrundlagen solche zur Auskunftserteilung über Verbindungsdaten ableiten.

93 So im Ergebnis auch *Kowalczyk*, 1990, S. 161.

94 Vgl. *Mann/Müller*, ZRP 1995, 180 (181). Nach *Würtenberger/Heckmann*, 2005, Rn. 620, wäre zwar eine präventiv-polizeiliche Überwachung des Fernmeldeverkehrs durch eine Fangschaltung oder telekommunikative Standortbestimmung nach dem Wortlaut des § 23 PolG BW gedeckt. Da § 4 PolG BW aber Art. 10 GG nicht als einschränkbares Grundrecht nenne, würde eine präventiv-polizeiliche Telekommunikationsüberwachung in Konflikt mit dem Zitiergebot des Art. 19 Abs. 1, Satz 2 GG geraten.

95 Vgl. *Mann/Müller*, ZRP 1995, 180 (181).

96 Vgl. *Mann/Müller*, ZRP 1995, 180 (181).

nisch verstärkt und in elektrische Impulse umgesetzt worden, so dass es sich im Zeitpunkt der Aufzeichnung nicht mehr um gesprochene Worte in ihrem normalen Klangbereich, sondern um in elektrische Impulse kodierte Informationen handelt.[97] Zum anderen liegt keine unmittelbare Aufzeichnung vor, da die Informationen nicht mehr in einer räumlich-gegenständlichen Beziehung zum Teilnehmer steht.[98] In dieser Überwindung einer unter Umständen erheblichen räumlichen Distanz liegt auch der Unterschied zu den sonstigen, als technische Mittel im Sinn der polizeilichen Vorschriften anerkannten Instrumenten, wie Richtmikrophonen, Stethoskopen oder Minispionen, deren Einsatz nur in relativer räumlicher Nähe zu der abgehörten Person möglich ist.[99]

Hinzu tritt, dass die wenigsten Polizeigesetze Art. 10 GG als einzuschränkendes Grundrecht zitieren.[100] Das Zitiergebot des Art. 19 Abs. 1, Satz 2 GG macht dies zur unumgänglichen Voraussetzung.[101] Und selbst bei den Polizeigesetzen, die eine Einschränkung des Art. 10 GG vorsehen, bedarf es jedenfalls wegen der Schwere des Grundrechtseingriffs einer speziellen Ermächtigungsgrundlage[102], so dass der Rückgriff auf die allgemeine polizeiliche Generalklausel verwehrt ist.[103]

III. Die Verwertung „fremder" Telekommunikationsdaten

1. Die Verwertung repressiver Telekommunikationsdaten

Nie erloschen war die Diskussion um die Verwertung von Abhörerkenntnissen aus einer Telefonüberwachung gemäß § 100 a StPO zu präventiven Zwecken.[104] Nach richtiger Ansicht

---

97 Vgl. *Mann/Müller*, ZRP 1995, 180 (181). Siehe dazu auch dieses Kapitel unter I.

98 Vgl. *Mann/Müller*, ZRP 1995, 180 (181).

99 Vgl. *Mann/Müller*, ZRP 1995, 180 (181). Siehe für § 22 PolG BW *Belz/Mußmann*, § 22 PolG BW, Rn. 7.

100 Jetzt jedenfalls § 11 ThPAG; Art. 74 PAG; § 8 Nr. 3 POG. In Niedersachsen und Hessen war Art. 10 GG schon vor der Einführung der präventiven Telekommunikationsüberwachung als einzuschränkendes Grundrecht in § 10 Nr. 3 NGefAG und § 10 HSOG enthalten.

101 Zur Gegenmeinung im Rahmen der Diskussion, ob repressive Kommunikationsdaten für präventive Zwecke verwendet werden dürfen, vgl. *Würz*, 1993, Rn. 348 und *Jarras*, in: Jarras/Pieroth, Art. 19 GG, Rn. 4 aE.

102 Vgl. *W.-R. Schenke*, 2007, Rn. 197 a; siehe *ders.*, JZ 2001, 997 (1002) für die Verwendung repressiv gewonnener Telekommunikationsdaten für präventive Zwecke.

103 So im Ergebnis auch *Mann/Müller*, ZRP 1995, 180 (183).

104 Vgl. *R.P. Schenke*, in: FG für Hilger, S. 211 ff.; *W.-R. Schenke*, in: FG für Hilger, S. 236 ff.; *Würtenberger*, in: FG für Hilger, S. 274; *Walden*, 1996, S. 333 ff. Zum Streitstand vor Inkrafttreten des Strafverfahrensänderungsgesetzes 1999 vgl. *Globig*, ZRP 1991, 81 ff., 289 ff.; *Hassemer*, ZRP 1991, 121 (123 f.); *Riegel*, ZRP 1991, 286 ff.

ist dies jedenfalls in den Ländern unzulässig, deren Polizeigesetze Art. 10 GG nicht als einzuschränkendes Grundrecht zitieren.

Eine Verwertung von Daten aus einer strafprozessualer Telefonüberwachung zu präventivpolizeilichen Zwecken stellt einen erneuten Eingriff in das durch Art. 10 GG geschützte Fernmeldegeheimnis dar.[105] Denn zum Schutzbereich des Fernmeldegeheimnisses zählt nicht nur der Schutz vor dem erstmaligen Eindringen in die Privatsphäre. Vielmehr erstreckt sich der Grundrechtsschutz auch auf den Informations- und Datenverarbeitungsprozess, der sich der Kenntnisnahme von Kommunikationsvorgängen anschließt.[106]

Kann die Polizei nach § 10 a Abs. 3 VEME PolG und den entsprechenden landesgesetzlichen Regelungen personenbezogene Daten, die sie im Rahmen von Strafermittlungsverfahren über Personen gewonnen hat, die verdächtig sind eine Straftat begangen zu haben, in Dateien speichern, verändern und nutzen soweit dies zur vorbeugenden Bekämpfung von Straftaten erforderlich ist, so können darunter – jedenfalls dem Wortlaut nach – auch Telekommunikationsdaten fallen. Bedeutet aber die Datenweitergabe einen weiteren Eingriff in Art. 10 GG, so muss der Gesetzgeber aufgrund des Zitiergebots in Art. 19 Abs. 1, Satz 2 GG eine eindeutige Aussage über seine Absicht, Art. 10 GG durch § 10 a Abs. 3 ME PolG bzw. die entsprechenden Regelungen in den Landespolizeigesetzen einzuschränken, treffen.[107]

Die Gegenmeinung[108], die das Zitiergebot für entbehrlich ansieht, weil es bei der Konkretisierung vorbehaltlos gewährleisteter Grundrechte nicht gelte, übersieht, dass Art. 10 Abs. 2, Satz 1 GG einen Gesetzesvorbehalt enthält und deswegen auch keine nur durch kollidierendes Verfassungsrecht zu ziehenden Schranken in Betracht kommen.

---

105 Zur endgültigen Klarstellung siehe BVerfGE 100, 313 ff.; so schon früher *Würtenberger/Heckmann/Riggert*, 1993, Rn. 418; aA *Globig*, ZRP 1991, 81 (83 f.), der in der Verwendung der durch abgehörte Gespräche erlangten Informationen zu anderen als repressiven Zwecken nur dann einen erneuten und weiteren Grundrechtseingriff sehen will, wenn diese andere Verwendung nach Gewicht und Bedeutung gegenüber den betroffenen Rechtsgütern der abgehörten Personen als eigenständiger Eingriff zu werten sei. Dies sei aber jedenfalls bei dem Zweck „Straftatenverhütung“ im Vergleich zum Zweck „Straftatenahndung“ nicht der Fall.

106 Vgl. BVerfGE 100, 313 (359); E 113, 349 (384); EGMR NJW 2007, 1433 (1434).

107 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 651; *Schild*, ZRP 1991, 311; *Riegel*, RDV 1990, 232; *Belz/Mußmann*, PolG BW,§ 38, Rn. 8; *Kowalczyk*, 1990, S. 231. Deutlich dazu auch BVerfGE 113, 349 (366 f.), welches das bereits vorhandene Zitat des Art. 10 GG im Nds.SOG 2005 vor dem Hintergrund der Einführung der Telekommunikationsüberwachung als nicht genügend ansieht. Die Benennung des eingeschränkten Grundrechts im fortgeltenden Gesetz war für das BVerfG nicht ausreichend, da eine erweiterte Eingriffsgrundlage geschaffen worden war.

108 Vgl. *Würz*, 1993, Rn. 348 und *Jarras*, in: Jarras/Pieroth, Art. 19 GG, Rn. 4.

Soweit angeführt wird, dass einer Datenweitergabe weder Art. 10 GG noch §§ 100 a und b StPO entgegenstehen, da es zu lebensfremden Ergebnissen führen würde, wenn die Polizei „sehenden Auges“ erst die Rechtsgutverletzung abwarten müsste, um dann repressiv einschreiten zu können[109], kann dem dadurch begegnet werden, dass bei der Gefährdung höchstrangiger Rechtsgüter wie dem Leben und der Gesundheit von Menschen eine Ausnahme in Betracht kommt. Die staatlichen Schutzpflichten aus Art. 2 Abs. 2 GG sind insofern bei der verfassungskonformen Auslegung des Polizeirechts zu berücksichtigen.[110]

Das Strafverfahrensänderungsgesetz 1999[111] hat an dieser Rechtslage nichts geändert. Zwar ist in § 477 Abs. 2 StPO nun geregelt, dass auch Informationen, die aus einer Überwachung nach § 100 a StPO stammen, übermittelt werden dürfen[112] und in Art. 12 a StVÄG 1999 die Einschränkung von Art. 10 GG ausdrücklich vorgesehen. Doch ist dadurch dem Zitiergebot nur insoweit genüge getan, als § 477 Abs. 2, Satz 3 StPO die repressiv gewonnenen Daten einer Umwidmung für präventive Zwecke zugänglich machen.[113] Geregelt ist damit nur, dass Informationen an Polizeibehörden unter bestimmten Voraussetzungen weitergegeben werden dürfen. Ob diese Daten tatsächlich genutzt werden dürfen und wie diese Nutzung erfolgt, ist jedoch dem Landesgesetzgeber vorbehalten.[114] So sieht § 481 Abs. 1, Satz 1 StPO ausdrücklich vor, dass die Polizeibehörden personenbezogene Informationen aus Strafverfahren (nur) nach Maßgabe der Polizeigesetze verwenden dürfen. Auch zeigt sich dies an § 39 Abs. 3 Nds.SOG, der eine spezielle Regelung zur Verwendung repressiver Daten vorsieht.[115]

---

109 Vgl. *Wolf/Stephan*, PolG BW, § 38 Rn. 3; *Würz*, 1993; Rn. 347 f.

110 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 654 die davon ausgehen, dass an der Beachtung des Zitiergebots nicht scheitern kann, dass die Polizei z.B. einen geplanten terroristischen Anschlag verhindert, von dem sie auf Grund einer strafprozessual angeordneten Telefonüberwachung Kenntnis erlangt hat; siehe auch *Walden*, 1996, S. 338 und 344. AA wohl *W.-R. Schenke*, 2007, Rn. 197 b, der die Polizei trotz Kenntnis der drohenden Gefahr zur Tatenlosigkeit verurteilt sieht.

111 Gesetz vom 02.08.2000, BGBl. I, S. 1253.

112 Die in § 477 Abs. 2, Satz 3 Nr. 1 StPO geregelte Übermittlung ist grundsätzlich nur zur Abwehr erheblicher Gefahren zulässig. § 477 Abs. 2 StPO wurde durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007, BGBl. I, S. 3198, neugefasst.

113 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 652; *Würtenberger*, in: FG für Hilger, S. 263 f.

114 Sog. Modell der „doppelten Tür“, vgl. *Würtenberger/Heckmann*, 2005, Rn. 645; *R.P. Schenke*, in: FG für Hilger, S. 214; *W.-R. Schenke*, JZ 2001, 997 (999); ausführlich zur Problematik der Gesetzgebungskompetenz *Würtenberger*, in: FG für Hilger, S. 264 ff. Zur Gegenansicht vgl. *Meyer-Goßner*, StPO, § 481, Rn. 1 und *Pfeiffer*, StPO, § 481, Rn. 1, die davon ausgehen, dass § 481 Abs. 1 StPO die Voraussetzungen regelt unter denen die Polizeibehörden die Daten nutzen dürfen.

115 § 39 Abs. 3 Nds.SOG regelt speziell die Verarbeitung von repressiven Daten zur Vorsorge für die Strafverfolgung und die Verhütung von Straftaten. Die Verwendung dieser Daten zur Abwehr einer konkreten Gefahr richtet sich nach § 39 Abs. 1 Nds.SOG.

Demnach können § 10 a Abs. 3 VEME PolG und die entsprechenden landesgesetzlichen Normen verfassungskonform nur dahingehend ausgelegt werden, dass sie die präventivpolizeiliche Verwertung von Erkenntnissen aus einer Telefonüberwachung nicht erfassen, wenn sie Art. 10 GG nicht als einzuschränkendes Grundrecht zitieren.[116]

2. Die Nachrichtenübermittlung durch die Nachrichtendienste

Die Dateien der Strafverfolgungsbehörden sind nicht die einzige Übermittlungsquelle, derer sich die Landespolizeibehörden bedienen können. Auch die Verfassungsschutzgesetze beinhalten Regelungen zur Datenübermittlung. Dies war nicht immer so. Zwar stammt das BVerfSchG bereits aus dem Jahr 1950[117], dessen § 4 eine Datenweitergabe, allerdings ohne eine Zweckbindung und sonstige Verfahrensanforderungen, vorsah. Das MAD-Gesetz[118] wie auch das BND-Gesetz[119] wurden jedoch erst im Jahr 1990 erlassen. Die Aufgaben des Bundesnachrichtendienstes waren bis zu diesem Zeitpunkt in einer Dienstanweisung[120] festgelegt. Für den Militärischen Abschirmdienst wurde davon ausgegangen, dass seine Sammlungsbefugnis und seine Befugnis zur Anwendung nachrichtendienstlicher Mittel denen des Bundesamtes für Verfassungsschutz entsprachen.[121] Hintergrund für den Erlass der Gesetze war das Volkszählungsurteil des BVerfG vom 12. Dezember 1983, das für Einschränkungen des Rechts auf informationelle Selbstbestimmung eine verfassungsgemäße gesetzliche Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen musste, verlangte.[122] Gleichzeitig wurde auch das BVerfSchG neu gefasst[123] und in seinen dritten Abschnitt umfangreiche Übermittlungsvorschriften aufgenommen.[124]

---

116 So für § 38 PolG BW *Würtenberger/Heckmann*, 2005, Rn. 651; *W.-R. Schenke*, 2007, Rn. 209; *R.P. Schenke*, in: FG für Hilger, S. 221 f. Darüber hinaus sind an die Übermittlung und Verwendung der Daten noch weitere (verfassungsrechtliche) Anforderungen zustellen, vgl. *R.P. Schenke*, in: FG für Hilger, S. 218 f.; *W.-R. Schenke*, JZ 2001, 997 (1002 ff.), die ausdrücklich auf die Anforderungen des BVerfG aus dem BND-Urteil verweisen (BVerfGE 100, 393 ff.).

117 Gesetz über die Zusammenarbeit der Bundes und der Länder in Angelegenheiten des Verfassungsschutzes vom 27.09.1950, BGBl. I, S. 682.

118 Gesetz über den Militärischen Abschirmdienst vom 20.12.1990, BGBl. I, S. 2977.

119 Gesetz über den Bundesnachrichtendienst vom 20.12.1990, BGBl. I, S. 2979.

120 Vgl. *Roewer*, § 1 PKKG, Rn. 16, der die Aufgaben des BND gemäß § 1 Dienstanweisung-BND wiedergibt.

121 Vgl. *Roewer*, § 1 PKKG, Rn. 34.

122 BVerfGE 65, 1ff. Vgl. dazu auch den Entwurf des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes, BT-Drucks. 11/4306, S. 1, dessen Artikel die Änderungen des BVerfschG und das MADG wie auch das BNDG enthalten. Der Gesetzesentwurf stellt ausdrücklich fest, dass mit diesem Artikelgesetz dem Volkszählungsurteil Rechnung getragen werden soll.

123 Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz vom 20.12.1990 (BGBl. I, 2954).

124 §§ 17 ff. BVerfSchG.

Schwerpunkt und Hauptaufgabe der Sicherheitsbehörden ist die Unterrichtung untereinander und die Informationsweitergabe an alle sonstigen Behörden.[125] Durch das Trennungsgebot[126] sind den Verfassungsschutzbehörden Informationsgewinnungen mit Hilfe polizeitypischen Zwangs ebenso verwehrt, wie Maßnahmen der Gefahrenabwehr oder Strafverfolgung aufgrund der ihnen zur Verfügung stehenden Erkenntnisse.[127] Diese obliegen allein den Gefahrenabwehr- bzw. Strafverfolgungsbehörden. Da die Nachrichtendienste damit eigenständig weder Maßnahmen zur Gefahrenabwehr noch zu Zwecken der Strafverfolgung ergreifen dürfen, sind sie darauf angewiesen, ihre Erkenntnisse den zuständigen Stellen zugänglich zu machen, um diesen die Reaktion auf drohende Gefahren und begangene Straftaten zu ermöglichen. So sehen das G-10-Gesetz, das BVerfSchG, das MAD-G und das BND-G auch Regelungen für die Datenübermittlung durch und an die Nachrichtendienste vor.[128]

a) Die Übermittlung von Daten nach dem G-10-Gesetz

Unter welchen Voraussetzungen aus der Individualüberwachung erlangte personenbezogene Daten an andere Stellen übermittelt werden dürfen, regelt § 4 Abs. 4 G-10-Gesetz. Danach ist eine Weitergabe u.a. zulässig, zur Verhinderung oder Aufklärung von Straftaten, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine der in § 3 Abs. 1 G-10-Gesetz genannten Straftaten plant oder begeht bzw. wenn bestimmte Tatsachen den Verdacht begründen, dass jemand eine sonstige in § 7 Abs. 4, Satz 1 G-10-Gesetz genannte Straftat plant oder begeht, soweit die Weitergabe zur Erfüllung der Aufgaben des Empfängers erforderlich ist.

---

125 Vgl. *Nehm*, NJW 2004, 3289 (3293); *Gusy*, NVwZ 1983, 322 (323); *Schwagerl*, 1985, S. 205; ausführlich zur informationellen Zusammenarbeit *König*, 2005, S. 256 ff.

126 Dazu ausführlich *König*, 2005, 151 ff.; *Nehm*, NJW 2004, 3289 ff.; *Gusy*, GA 1999, 319 (324 ff.); *ders.* Die Verwaltung 24 (1991), S. 467 ff. Historischer Ausgangspunkt des Trennungsgebots ist der sog. „Polizei-Brief" vom 14.04.1949, abgedruckt bei *Haedge*, 1998, S. 70, mit dem die Westalliierten der Bundesregierung erhebliche Vollmachten auf dem Gebiet der Polizei zugestanden. So wird in Nr. 2 des Polizeibriefs der Bundesregierung gestattet, „eine Stelle zur Sammlung und Verbreitung von Auskünften über umstürzlerische, gegen die Bundesregierung gerichtete Tätigkeiten einzurichten. Diese Stelle soll keine Polizeibefugnisse haben".

127 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 102. *Gusy*, Die Verwaltung 1991, 467 (478).

128 Siehe zur Zusammenarbeit zwischen Polizei und Verfassungsschutz auch *Riegel*, DVBl. 1988, 121, die Erwiderung von *Borgs-Maciejewski*, DVBl. 1998, 388 und die Stellungnahme hierzu von *Riegel*, DVBl. 1998, 391. Zu den neueren Entwicklungen bei der Datenübermittlung zwischen Polizei und Geheimdiensten, insbesondere zur „Anti-Terror-Datei" als Teil des Gemeinsame-Dateien-Gesetzes (BGBl. I 2006, 3409) vgl. *Roggan/Bergemann*, NJW 2007, 876.

Daten aus einer strategischen Überwachung dürfen nach § 7 Abs. 4, Satz 1; Abs. 5, Satz 1 G-10-Gesetz zur Verhinderung der dort genannten Straftaten an die mit polizeilichen Aufgaben betrauten Behörden übermittelt werden, soweit die Übermittlung zur Erfüllung der Aufgaben des Empfängers erforderlich ist.

b) Die Übermittlung von Daten nach dem BVerfSchG

Nach § 19 Abs. 1 BVerfSchG darf das Bundesamt für Verfassungsschutz personenbezogene Daten an inländische Behörden übermitteln, wenn dies zur Erfüllung seiner Aufgaben erforderlich ist oder der Empfänger die Daten zum Schutz der freiheitlichen demokratischen Grundordnung oder sonst für Zwecke der öffentlichen Sicherheit benötigt. Öffentliche Sicherheit bedeutet dabei staatlichen Rechtsgüterschutz und umfasst die Summe der Normen, die zum Schutz des Staates, seiner Einrichtungen und seiner Rechtsordnung aufgestellt sind.[129] Dabei kann aber nicht jeder Zweck der öffentlichen Sicherheit genügen. Schon früh wurde gefordert, dass eine Übermittlung von Daten aus dem Bereich des Verfassungsschutzes an andere Stellen als Nachrichtendienste nur dann erfolgen darf, wenn dies zur Erfüllung von Aufgaben der Verfassungsschutzbehörden notwendig ist.[130]

An Strafverfolgungs- und Sicherheitsbehörden werden Informationen einschließlich personenbezogener Daten übermittelt, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Übermittlung zu Verhinderung oder zur Verfolgung von Staatsschutzdelikten erforderlich ist.[131]

Das Verhältnis der §§ 19 Abs. 1 und 20 Abs. 1 BVerfSchG zueinander ist nicht abschließend geklärt.[132] Soweit jedoch der Anwendungsbereich des § 20 Abs. 1 BVerfSchG nicht eröffnet ist, kann auf § 19 BVerfSchG zurückgegriffen werden.[133] Dann könnten auch Telekommunikationsdaten unter den Voraussetzungen des § 19 BVerfSchG übermittelt werden. Für die

---

129 Vgl. BT-Drucks. 11/4306, S. 63.

130 So der Bundesbeauftragte in seinem ersten Tätigkeitsbericht für den Datenschutz, BT-Drucks. 8/2460, S. 24.

131 § 20 Abs. 1, Satz 1 BVerfSchG

132 Vgl. dazu *König*, 2005, S. 271 f.

133 Vgl. *Lisken/Denninger*, in: Lisken/Denninger (Hrsg.), Kap. C, Rn. 123, die § 19 Abs. 1 BVerfSchG als Globalermächtigung zur Übermittlung von Präventivdaten an die Polizei ansehen. Auch *Droste*, 2007, S. 518 ff. geht davon aus, dass § 20 BVerfSchG keine Spezialnorm ist, die die Befugnis zur Datenübermittlung abschließend regelt. Vielmehr stehe es im Ermessen des BfV, ob es Erkenntnisse, die nicht unter § 20 BVerfSchG fallen, an Straf- und Sicherheitsbehörden gemäß § 19 BVerfSchG übermittelt. *König*, 2005, S. 272, geht von einem Nebeneinander beider Vorschriften aus.

Verarbeitung der nach § 8 a Abs. 2, Satz 1 Nr. 3 - 5 BVerfSchG erhobenen Telekommunikationsdaten gilt jedoch § 4 G-10-Gesetz entsprechend, so dass eine Übermittlung nur unter den Voraussetzungen des § 4 Abs. 4 G-10-Gesetz zulässig ist.[134]

Diese Übermittlungsvorschriften des BVerfSchG gelten auch für den Militärischen Abschirmdienst und den Bundesnachrichtendienst.[135] In beiden Gesetzen ist durch den Verweis auf § 8 a BVerfSchG ebenfalls der Verweis auf die Verarbeitungsvorschrift des § 4 G-10-Gesetz enthalten.[136]

c) Zusätzliche Anforderungen an die Telekommunikationsdatenübermittlung

Durch das Trennungsgebot ist den Verfassungsschutzämtern und Nachrichtendiensten die Informationsgewinnung mit Hilfe polizeitypischen Zwangs verwehrt. Vielmehr dürfen sie sich bei ihrer Informationsbeschaffung allein nicht-imperativer Methoden unter Einsatz nachrichtendienstlicher Mittel bedienen.[137] Das sind zumeist heimliche Ermittlungsmethoden, wie der Einsatz von V-Leuten, Verdeckten Ermittlern und technischen Instrumenten zur visuellen und auditiven Überwachung.[138] Die mit Hilfe dieser Mittel erhobenen Daten können nach den §§ 19 und 20 BVerfSchG an Polizeibehörden unter den dort genannten Voraussetzungen weitergegeben werden, da die Polizeigesetze der Länder identische Mittel zur Datenerhebung vorsehen und ihre Gesetze die dadurch betroffenen Grundrechte zitieren.[139]

---

134 So die Regelung in § 8 a Abs. 5, Satz 7 BVerfSchG. Schon vor Erlass der §§ 17 ff. BVerfSchG wurde gefordert, dass Informationen durch die Verfassungsschutzbehörden nicht für jeden beliebigen Sicherheitszweck übermittelt werden dürfen. Nach Ansicht des Bundesbeauftragten für den Datenschutz sollte eine Übermittlung von Daten aus dem Bereich des Verfassungsschutzes an andere Behörden nur erfolgen, wenn dies zur Erfüllung von Aufgaben notwendig ist, die den Verfassungsschutzbehörden zugewiesen sind. Als Beispiel nannte er die Strafverfolgung von Staatsschutzdelikten. Für die Verfolgung anderer Straftaten, wie Eigentums- und Steuervergehen, dürften gesicherte Erkenntnisse nicht übermittelt werden, denn das widerspräche der grundsätzlichen Aufgaben- und Befugnistrennung der staatlichen Stellen untereinander, die durch die allgemeine Pflicht zur Amtshilfe nicht aufgehoben werden kann, vgl. Erster Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 19 Abs. 2 Satz 2 BDSG BT-Drucks. 8/2460, S. 24.

135 § 11 Abs. 1 und 2 MADG; § 9 Abs. 2 und 3 BNDG. Der BND darf darüber hinaus nach § 9 Abs. 1 BNDG personenbezogene Daten an inländische öffentliche Stellen übermitteln, wenn dies zur Erfüllung seiner Aufgaben erforderlich ist oder wenn der Empfänger die Daten für Zwecke der öffentlichen Sicherheit benötigt.

136 § 4 a MADG; § 2 a BNDG.

137 Vgl. *Nehm*, NJW 2004, 3289; *Roggan*, 2003, S. 17; *Gusy*, Die Verwaltung 1991, 467 (483 ff.).

138 § 8 Abs. 2 BVerfSchG; § 6 Abs. 1 LVSG BW. Vgl. *Nehm*, NJW 2004, 3289 (3293); *Kniesel/Tegtmeyer/Vahle*, 1986, Rn. 149.

139 Siehe für Baden-Württemberg die Regelungen in §§ 22 und 23 PolG BW. Zu Grundrechtseingriffen aufgrund Datenerhebung durch die Nachrichtendienste vgl. *Gusy*, NVwZ 1983, 322 (323).

Bleibt zu klären, ob dies auch gilt, wenn es sich um Daten handelt, die durch Eingriffe in das Fernmeldegeheimnis erlangt wurden.[140] Bedeutet die Weitergabe von Telekommunikationsdaten durch Verfassungsschutzbehörden einen weiteren Eingriff in Art. 10 GG, so sind die gleichen Maßstäbe anzusetzen, wie bei einer Weitergabe repressiver Telekommunikationsdaten an Gefahrenabwehrbehörden. Werden die Daten durch die Verfassungsschutzbehörden an Landespolizeibehörden weitergegeben, da diese für Zwecke der öffentlichen Sicherheit benötigt werden,[141] so ist dies nur zulässig, wenn das jeweilige Polizeigesetz Art. 10 GG als einzuschränkendes Grundrecht nennt.[142] Eine andere Beurteilung kann allenfalls dann geboten sein, wenn diese Daten von den Nachrichtendiensten weitergegeben werden zur Erfüllung nachrichtendienstlicher Aufgaben.[143] Denn eine solche Weitergabe hält sich im Rahmen des Grundsatzes der Zweckbindung. Sind die Speicherung und die Verwendung erlangter Daten grundsätzlich an den Zweck gebunden, den das zur Kenntnisnahme ermächtigende Gesetz festgelegt hat,[144] so steht eine Weitergabe mit diesem Erfordernis dann im Einklang, wenn sie gerade der Zweckerfüllung dient.[145] Eine den verfassungsrechtlichen Anforderungen an das Fernmeldegeheimnis entsprechende gesetzliche Grundlage für eine Datenweitergabe wird mit der Begründung gefordert, dass durch die Weitergabe regelmäßig nicht nur weitere (staatliche) Stellen oder Personen über die Kommunikation informiert werden, sondern die Daten in einen anderen Verwendungszusammenhang überführt werden, der für die Betroffenen mit zusätzlichen, unter Umständen schweren Folgen verbunden ist, als im ursprünglichen Verwendungszusammenhang.[146] Dies ist gerade nicht zu befürchten, wenn die Weitergabe der Erfüllung des Erhebungszwecks dient.

Sollen jedoch geheimdienstliche Informationen für präventiv-polizeiliche Zwecke nutzbar gemacht werden, so müssen Datenverarbeitungsvorschriften bzw. Datenerhebungsvorschrif-

---

140 §§ 3 Abs. 1, 5 Abs. 1 iVm § 1 Abs. 1 G-10-Gesetz; § 8 a Abs. 1, Abs. 2 Nr. 4 BVerfSchG; § 4 a MADG; § 2 a BNDG.

141 § 19 Abs. 1, Satz 1 BVerfSchG.

142 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 651; *König*, 2005, S. 211 f. für die Weitergabe repressiver Telekommunikationsdaten.

143 §§ 19 Abs. 1 und 20 Abs. 1 BVerfSchG. Dazu *König*, 2005, S. 282 f., der darauf abstellt, dass sich die Zulässigkeit von Datenübermittlungen zwischen Polizeien und Nachrichtendiensten, jedenfalls soweit es um Datenübermittlungen zur Erfüllung nachrichtendienstlicher Aufgaben geht, nach den jeweiligen einschlägigen nachrichtendienstrechtlichen Vorschriften des Bundes oder eines Landes richtet, da diese insoweit spezieller sind.

144 Vgl. BVerfGE 100, 313 (360).

145 Grundsätzlich kann die Polizei Daten nur zu dem Zweck übermitteln, zu dem sie diese Informationen erlangt und gespeichert hat, vgl. *Petri*, in: Lisken/Denninger (Hrsg.), Kap. H, Rn. 418; *Schenke*, 2007, Rn. 207.

146 Vgl. BVerfGE 100, 313 (360).

ten eingeführt werden, die den verfassungsrechtlichen Voraussetzungen für die Weitergabe, Entgegennahme und Verarbeitung grundrechtlich geschützter Daten entsprechen.[147] Da sich der „Übermittlungseingriff“ nach dem Vorschriften der übermittelnden Stelle richtet[148], die Speicherung als weiterer Grundrechtseingriff aber nach den Normen der entgegennehmenden/speichernden Stelle[149], müssen die Landespolizeigesetze die Bestimmung getroffen haben, mit ihren Regelungen zur Datenverarbeitung das Grundrecht des Art. 10 GG zu beschränken.[150]

3. Die Datenübermittlung durch das Zollkriminalamt

Nach § 23 d Abs. 1 ZFdG dürfen die vom Zollkriminalamt erlangten personenbezogenen Daten zur Verhütung von Straftaten an die mit polizeilichen Aufgaben betrauten Behörden übermittelt werden. Bei dieser Übermittlung findet eine Unterscheidung danach statt, ob tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine bestimmte Straftat begeht oder begehen will (Nr. 1) oder ob bestimmte Tatsachen diesen Verdacht begründen (Nr.2).

In den Fällen des § 23 d Abs. 1 Nr. 1 ZFdG geht der Gesetzgeber davon aus, dass bei diesen Straftaten das Vorliegen tatsächlicher Anhaltspunkte[151] für einen Verdacht genügt, um den Verhältnismäßigkeitsgrundsatz nicht zu verletzen.[152] Es handelt sich dabei um Straftaten, bei denen die Strafandrohung von mindestens fünf Jahren Freiheitsstrafe die Bedeutung der Rechtsgutsverletzung zum Ausdruck bringt. Ferner ist mit § 129 a StGB, auch in Verbindung

---

147 Vgl. *Lisken/Denninger*, in: Lisken/Denninger (Hrsg.), Kap. C, Rn. 124. Sehen bspw. die Landespolizeigesetze eine präventive Telekommunikationsüberwachung vor, dürfte damit gewährleistet sein, dass Art. 10 GG als einzuschränkendes Grundrecht zitiert wird.

148 Vgl. *Belz/Mußmann*, § 41 PolG BW, Rn. 2.

149 Vgl. *Belz/Mußmann*, Vorbemerkung § 37 PolG BW, Rn. 2.

150 Ausnahmen sind nach *König*, 2005, S. 212, zuzulassen, soweit dies zur Abwehr von Gefahren für höchstrangige Rechtsgüter geschieht.

151 Mit dem Wahrscheinlichkeitsgrad „tatsächliche Anhaltspunkte“ wird verdeutlicht, dass eine hinreichende Wahrscheinlichkeit bestehen muss, mit Hilfe der einzusetzenden Maßnahme verfahrensrelevante Informationen zu gewinnen, vgl. *Petri*, in: Lisken/Denninger (Hrsg.), Kap. H, Rn. 248 unter Hinweis auf BT-Drucks. 15/4533, S. 12 und BVerfGE 109, 279 (356 f.), welche sich auf die tatsächlichen Anhaltspunkte im Rahmen des § 100 c Abs. 1 Nr. 3 StPO beziehen. Für das Vorliegen „tatsächlicher Anhaltspunkte“ genügt es, wenn es nach der gefahrenabwehrbehördlichen oder polizeilichen Erfahrung als möglich erscheint, dass ein bestimmter Sachverhalt vorliegen könnte, der ein Tätigwerden erfordert und hierfür bestimmte Indizien sprechen, vgl. *Meixner/Fredrich*, § 13 HSOG, Rn. 9. Bei Einschränkungen des Brief-, Post- und Fernmeldegeheimnisses hat nach *Meixner/Fredrich*, § 40 HSOG, Rn. 11 unter Hinweis auf BVerfGE 100, 313 (395) eine einengende Auslegung des Begriffs „tatsächliche Anhaltspunkte“ sicherzustellen, dass nicht im Wesentlichen Vermutungen, sondern konkrete und im gewissen Umfang verdichtete Umstände als Tatsachenbasis für den Verdacht vorliegen.

152 Vgl. BT-Drucks. 15/3931, S. 17.

mit § 129 b StGB, der besonderen Gefährlichkeit des organisierten Terrorismus Rechnung getragen.[153] Die Übermittlung bei geplanten Straftaten nach dem AWG oder dem KrWaffG steht in enger Beziehung zum Erhebungszweck.[154]

Für die in § 23 d Abs. 1 Nr. 2 ZFdG genannten Straftaten soll die hohe Übermittlungsschwelle der bestimmten Tatsachen gelten.[155] Damit wird dem Umstand Rechnung getragen, dass diese Erkenntnisse den Charakter von Zufallsfunden haben. Der Straftatenkatalog soll sicherstellen, dass die Übermittlung von Zufallserkenntnissen zur Verhütung von Straftaten, die besonders bedeutende Rechtsgüter gefährden, möglich ist.[156]

Der Gesetzgeber hat damit zwar herausgearbeitet, welche Straftaten er als gewichtig genug ansieht, um einen weiteren Eingriff in Art. 10 GG, durch die Weitergabe der Telekommunikationsdaten, zu rechtfertigen. Ob die mit präventiv-polizeilichen Aufgaben betrauten Polizeibehörden die Daten verwenden dürfen, richtet sich aber wiederum nach den jeweiligen Polizeigesetzen.

IV. Übergesetzlicher Notstand

Fand sich in den Polizeigesetzen keine taugliche Ermächtigungsgrundlage für die Legitimation von Telefonüberwachungen zu präventiven Zwecken, so wurde unter Berufung auf §§ 32 und 34 StGB bzw. einen übergesetzlichen Notstand die Übermittlung von Kommunikationsdaten in Notfällen von den Telekommunikationsdiensteanbietern verlangt, die diesen Forderungen wohl auch nachkamen.[157]

---

153 Vgl. BT-Drucks. 15/3931, S. 17.

154 Vgl. BT-Drucks. 15/3931, S. 17.

155 Voraussetzung für das Vorliegen bestimmter Tatsachen ist, dass auf Grund der vorhandenen Erkentnisquellen ein bestimmter Sachverhalt nachgewiesen ist, der ein gefahrenabwehrbehördliches oder polizeiliches Einschreiten erfordert, so für die Erhebung personenbezogener Daten nach dem HSOG *Meixner/Fredrich*, § 13 HSOG, Rn. 9.

156 Vgl. BT-Drucks. 15/3931, S. 17.

157 Dies kommt in der Gesetzesbegründung des Landes Bayern zur präventiven Telekommunikationsüberwachung zum Ausdruck, LT- Drucks. 15/2096, S. 60. Auch im Bericht der thüringer Landesregierung über die präventiv-polizeiliche Telekommunikationsüberwachung im Jahr 2003 wird erwähnt, dass durch die thüringer Polizeibehörden Daten von den Telekommunikationsunternehmen unter Berufung auf § 34 StGB abgefordert wurden, obwohl diese Verfahrensweise seit In-Kraft-Treten von § 34 a ThPAG nicht mehr zulässig war, LT-Drucks. Th. 4/249, S. 3.

Die Anordnung einer präventiven Telekommunikationsüberwachung unter Rückgriff auf die Notwehr- bzw. Notstandsregelungen der §§ 32 und 34 StGB ist jedoch unzulässig.[158] Sie sind keine taugliche Ermächtigungsgrundlage für hoheitliches Handeln.[159]

Mit der Begründung, dass sich die Funktionsweise der Polizei ins Gegenteil verkehren würde, wollte man ihr das Recht absprechen, in den Fällen der §§ 32 und 34 StGB Hilfe zu leisten, obwohl sie gerade zur Gefahrenabwehr in diesen Situationen besonders ausgebildet ist, werden die §§ 32 und 34 StGB als Ermächtigungsgrundlagen angeführt.[160] Dabei wird verkannt, dass eine strafrechtliche Rechtfertigung des Amtswalters nicht notwendig zu einem Rückschluss auf dessen hoheitliche Befugnis zwingt.[161] Die Verletzung des Fernmeldegeheimnisses ist in § 206 StGB mit Strafe bedroht. Damit können zwar Eingriffe in das Fernmeldegeheimnis nach §§ 32 und 34 StGB gerechtfertigt sein, eine Eingriffsermächtigung für Behörden gegenüber denjenigen, die den Zugriff auf die Telekommunikation erst ermöglichen, ist darin aber nicht enthalten.[162]

Selbst wenn ein und dasselbe Verhalten vor dem Hintergrund der Einheit der Rechtsordnung[163] nicht zugleich (straf)rechtsmäßig und (polizei)rechtswidrig sein könnte[164], qualifiziert dies die §§ 32 und 34 StGB ebenfalls nicht als Ermächtigungsgrundlagen. Polizeiliches Handeln mag sicherlich rechtswidrig sein, wenn es strafbar ist. Ein Umkehrschluss ist aber schon deshalb nicht haltbar, weil strafbar nur ist, was ausdrücklich unter Strafe gestellt ist.[165] Im Rahmen der Eingriffsverwaltung ist jedoch nur rechtmäßig, was ausdrücklich erlaubt

---

158 Vgl. *Mann/Müller*, ZRP 1995, 180 (184 f.); *Riegel*, NVwZ 1985, 639 (641); *Lisken*, DRiZ 1989, 401 (402); *Schatzschneider*, NJW 1993, 2029 (2030) unter Hinweis auf BVerfG NJW 1992, 1875.

159 Nach *Jarass*, in: Jarass/Pieroth, Art. 10 GG, Rn. 17 scheidet die Notstandsregelung des § 34 StGB schon deswegen aus, weil das Zitiergebot nicht gewahrt ist; nach *Gusy*, in: v.Mangoldt/Klein/Starck (Hrsg.), Art. 10 GG, Rn. 71 entspricht § 34 StGB nicht den Anforderungen des Bestimmtheitsgebots.

160 Vgl. *Spendel*, in: LK, § 32 StGB, Rn. 268 und 277.

161 Vgl. *Riegel*, NVwZ 1985, 639 (640). Nach *Lisken*, DRiZ 1989, 401 (402) kann ein Verweis auf private Nothilfebefugnisse nicht genügen, weil staatliches Eingriffshandeln gemäß Art. 20 Abs. 3 GG aufgrund öffentlich-rechtlicher Normen und niemals aufgrund privat-rechtlicher Jedermannbefugnisse statthaft ist.

162 Vgl. *Zerres*, in: Scheurle/Mayen (Hrsg.), § 85 TKG, Rn. 42; *Loewer*, in: v.Münch/Kunig (Hrsg.), Art. 10 GG, Rn. 23.

163 Vgl. dazu das Kapitel „Grundrechtliche Anforderungen".

164 Vgl. *Mann/Müller*, ZRP 1995, 180 (184); *Spendel*, in: LK, § 32 StGB, Rn. 273. Zur überzeugenden Gegenmeinung vgl. *Würtenberger*, in: Achterberg/Püttner/Würtenberger (Hrsg.), Band II, § 21, Rn. 348, der zu dem Ergebnis kommt, dass eine Maßnahme unmittelbaren Zwangs straf- und zivilrechtlich gerechtfertigt sein mag, aber polizeirechtswidrig ist, wenn sie den polizeirechtlichen (Verfahrens-)Vorschriften widerspricht. Siehe dazu ausführlich auch *Felix*, 1998, S. 60 ff.

165 Art. 103 Abs. 2 GG.

ist.[166] Greift der Staat in die Rechte eines Bürgers ein, befreit ihn dies auch dann nicht vom Vorbehalt des Gesetzes, wenn seine Ziele noch so achtenswert sind und die Handlung des Beamten strafrechtlich gerechtfertigt ist.[167]

Die strafrechtlichen Rechtfertigungsregeln stehen auch nicht in Einklang mit den verfassungsrechtlichen Anforderungen an eine öffentlich-rechtliche Befugnisnorm,[168] da berechtigte Bedenken jedenfalls hinsichtlich der Gesetzgebungskompetenz bestehen.[169] Das Polizeirecht unterfällt nach Art. 70 Abs. 1 GG der Gesetzgebungskompetenz der Länder. Folglich hat sich der Bund jeglicher Gesetzgebung in diesem Bereich zu enthalten.[170] Ein Rückgriff auf die §§ 32; 34 StGB würde dabei die Vorgaben des Landesgesetzgebers zur Datenverarbeitung und die getroffene Normsystematik des Polizeirechts weitgehend aushebeln.[171]

V. Fazit

Es zeigt sich, dass eine präventive Telekommunikationsüberwachung aufgrund der bislang bestehenden Regelungen für die Polizeibehörden der Länder rechtlich nicht möglich war. Die Überwachung scheiterte jedenfalls am Zitiergebot sowie den grundrechtlichen Anforderungen an den Vorbehalt des Gesetzes.

Eine gesetzliche Regelung ist auch im Interesse der zu schützenden Rechtsgüter unverzichtbar. Dies gilt ebenfalls im Hinblick auf doppelfunktionale Maßnahmen. Diese polizeilichen Maßnahmen verfolgen präventive und repressive Zwecke und lassen sich daher sowohl auf eine polizeirechtliche als auch auf eine strafprozessuale Ermächtigungsgrundlage stützen.[172]

---

166 Vgl. *Mann/Müller,* ZRP 1995, 180 (184); *Erichsen*, in: Erichsen/Ehlers (Hrsg.), § 15 Rn. 15, gibt zu bedenken, dass was strafrechtlich als gerechtfertigte Tat erscheinen mag, als Staatsakt den Grundsätzen des staatlichen Sonderrechts unterliegt. Der Vorrang des Gesetzes verbiete es, außerhalb der gesetzlich zugewiesenen Zuständigkeiten tätig zu werden und von dem gesetzlich geregelten Verfahren abzuweichen.

167 Vgl. *Mann/Müller,* ZRP 1995, 180 (184).

168 Zur Anwendung von § 34 StGB im öffentlichen Recht vgl. *Lange*, NJW 1978, 784 ff., der zu dem Ergebnis kommt, dass hoheitliche Maßnahmen nur für eine kurze Übergangsfrist auf § 34 StGB gestützt werden können.

169 Vgl. *Mann/Müller,* ZRP 1995, 180 (185). Auch im Hinblick auf den Bestimmtheitsgrundsatz könnten Bedenken bestehen. Allerdings sind die Voraussetzungen des § 34 StGB konturiert, die Verhältnismäßigkeit wird in „handliche Bausteine" zerlegt und der Rechtsgüterschutz durch den Grad der Gefahr relativiert, vgl. *Lange*, JZ 1976, 546 (548).

170 Vgl. *Mann/Müller,* ZRP 1995, 180 (185); *Randl*, NVwZ 1992, 1070 f.; siehe auch *Schoch*, JuS 1994, 391 (394), der einen guten Überblick über die Gesetzgebungskompetenzen im Gefahrenabwehrrecht gibt.

171 Vgl. *Mann/Müller,* ZRP 1995, 180 (185); *H.J. Hirsch*, in: LK § 34 StGB, Rn. 19; *Amelung*, NJW 1977, 833 (840); *W.-R. Schenke/R.P. Schenke*, in: Steiner (Hrsg.), Kap. II J, Rn. 302.

172 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 188 ff.

Sind diese Maßnahmen kumulativ dem Recht der Gefahrenabwehr und der Strafverfolgung zuzuordnen, müssen je nach Zweck und Schwergewicht der Maßnahmen auch gefahrenabwehrrechtliche und strafverfolgungsrechtliche Ermächtigungsgrundlagen gegeben sein, die der Polizei ein (rechtssicheres) Einschreiten zu beiden Zwecken ermöglichen. [173]

Auch unter rechtspolitischen Gesichtspunkten ist eine Ermächtigungsgrundlage auf der Ebene der „einfachen Gefahrenabwehr“ zu begrüßen. Denn selbst wenn den Gefahrenabwehrbehörden die Kommunikationsdaten der Strafverfolgungsbehörden und Nachrichtendienste zur Verfügung stehen, ist dies kein adäquater Ersatz für eine eigene Datenerhebung. Der Datenübermittlung ist immanent, dass sie Informationen beinhaltet, die von einer anderen Stelle erhoben wurden. Dies bedeutet, dass die Erhebungsbehörde entschieden hat, welche Daten erhoben werden. Eine Empfängerbehörde ist daher stets dem Risiko ausgesetzt, dass die erhobenen Daten für ihre Zwecke nicht brauchbar sind, da sie nicht selbst am Entscheidungsprozess über die Datenerhebung partizipiert hat. Eine originäre Datenerhebung kann dadurch nicht ersetzt werden. Zudem kommt die Verwendung von Kommunikationsdaten anderer Behörden wegen der strengen Voraussetzungen im Hinblick auf das hohe Schutzgut des Fernmeldegeheimnisses nur in Ausnahmefällen in Betracht.

---

173 Vgl. *Weitemeier/Große*, Kriminalistik 1997, 335 (336). Dies verdeutlicht auch die Gesetzesbegründung Bayerns, die anklingen lässt, dass der Rechtsgedanke des § 34 StGB als Befugnisnorm von den Diensteanbietern immer wieder in Frage gestellt wurde, LT-Drucks. 15/2096, S. 60.

Kapitel 3: Der Zugriff auf die Telekommunikationsdaten

§ 34 a ThPAG, § 33 a – c Nds.SOG, Art. 34 a – c PAG, § 31 POG und § 15 a HSOG gestatten die Datenerhebung durch die Überwachung der Telekommunikation zu präventiven Zwecken. Welche Daten von dieser Erhebung betroffen sind und wie der Zugriff auf diese Daten erfolgt, erschließt sich nicht direkt aus den Polizeigesetzen, sondern ergibt sich erst aus dem Zusammenspiel mit dem Telekommunikationsgesetz (TKG).[174]

I. Die Regelungen in den Polizeigesetzen

1. Das Bayerische Polizeiaufgabengesetz

Gemäß Art. 34 a PAG kann die Polizei[175] personenbezogene Daten durch die Überwachung und Aufzeichnung der Telekommunikation erheben.[176] Dabei haben geschäftsmäßige Telekommunikationsdiensteanbieter der Polizei die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen.[177] Der Begriff der Telekommunikation richtete sich nach der Definition im Telekommunikationsgesetz.[178] Die Überwachungs- und Aufzeichnungsermöglichung richtet sich nach Maßgabe der Regelungen des Telekommunikationsgesetzes und der darauf beruhenden Rechtsverordnungen.[179]

---

174 Das Telekommunikationsgesetz vom 01.08.1996, BGBl. I, S. 1120, ist mit Gesetz vom 22.06.2004, BGBl. I, S. 1190, neu gefasst und zuletzt geändert worden durch Art. 3 des Gesetzes zur Änderung telekommunkationsrechtlicher Vorschriften vom 18.02.2007, BGBl. I, S. 106. Die Landespolizeigesetze sind allesamt vor der Neufassung des TKG geändert bzw. neu gefasst worden; eine Ausnahme gilt für Bayern. Daher beziehen sich die Regelungen zur präventiven Telekommunikationsüberwachung und die Ausführungen in den Gesetzesbegründungen der Landesgesetze auf die Normen der TKG vor seiner Neufassung. Inhaltliche Unterschiede sind dadurch nur in geringem Ausmaß zu verzeichnen. Soweit Normen des TKG vom 01.08.1996 zitiert werden, werden diese durch den Zusatz TKG 1996 gekennzeichnet.

175 Polizei im Sinne des PAG sind gemäß Art. 1 Abs. 1 PAG die im Vollzugsdienst tätigen Dienstkräfte der Polizei des Freistaates Bayern, Art. 1 Abs. 1 PAG; vgl. die Parallelregelungen in § 1 ThPAG, § 2 Nr. 5 und Nr. 6 Nds.SOG. Auch § 31 POG und § 15 HSOG ermächtigen den Polizeivollzugsdienst zur Telekommunikationsüberwachung. Das POG vollzieht in § 1 Abs. 1 die Aufgabentrennung zwischen Ordnungspolizeibehörde und der Polizei (früher: Vollzugspolizei). Die Polizei ist nur dann originär zuständig, wenn es eine ausdrückliche Zuweisung gibt, vgl. *Roos*, § 1 POG, Rn. 1. Die Wahrnehmung von Aufgaben der Gefahrenabwehr ist in Hessen Sache der Gefahrenabwehrbehörden (Verwaltungs- und Ordnungsbehörden) und der Polizeibehörden § 1 Abs. 1, Satz 1 HSOG. Der Begriff „Polizeibehörden“ ist den Vollzugspolizeidienststellen vorbehalten, vgl. *Meixner/Fredrich*, Einführung HSOG, Rn 38.

176 Vgl. die Parallelregelungen in § 34 a Abs. 1 ThPAG, § 33 a Abs. 1 Nds.SOG, § 31 Abs. 1 POG, § 15 Abs. 1 und 2 HSOG.

177 Art. 34 b Abs. 1 PAG. Siehe auch § 34 a Abs. 4, Satz 1 ThPAG; § 33 a Nds.SOG; § 31 Abs. 6 POG; § 15 Abs. 1 HSOG.

178 Vgl. LT-Drucks. Bayern 15/2096, S. 51. So auch LT-Drucks. Th. 3/2128, S. 34 f.; LT-Drucks. Nds. 15/240, S. 17; LT-Drucks. RhPf. 14/2287, S. 47.

179 Vgl. LT-Drucks. Bayern 15/2096, S. 59. So auch LT-Drucks. Th. 3/2128, S. 35; LT-Drucks. Nds. 15/240, S. 17; LT-Drucks. RhPf. 14/2287, S. 47; LT-Drucks. Hessen 16/2351, S. 19.

Die Polizei kann gemäß Art. 34 b Abs. 2, Satz 1 PAG die Diensteanbieter verpflichten, ihr vorhandene Telekommunikationsverkehrsdaten[180] zu übermitteln, Auskunft über zukünftige Telekommunikationsverkehrsdaten zu erteilen oder spezifische Kennungen für die Ermittlung des Standorts eines Mobilfunkgerätes mitzuteilen.[181] Dies gilt gemäß Art. 34 b Abs. 2, Satz 2 PAG auch für Daten aus Telekommunikationsverbindungen, die zur betroffenen Person hergestellt worden sind.[182] Art. 34 b Abs. 3 PAG enthält eine Aufzählung der Telekommunikationsdaten, die von der Übermittlungspflicht umfasst werden. Dies sind u.a. die Kennungen und Rufnummern sowie der Beginn und das Ende von Verbindungen.[183] Ob diese Daten auch bei den Dienstanbietern vorhanden sind, ergibt sich aus dem PAG nicht. Hierzu muss das TKG herangezogen werden.[184]

In Art. 34 a Abs. 2 PAG ist der Einsatz des IMSI-Catchers zur Kennung- und Standortermittlung geregelt. Auch wird der Polizei die Möglichkeit eröffnet, Kommunikation zu unterbrechen oder zu verhindern.[185]

2. Die Abweichungen in den anderen Polizeigesetzen

Die Polizeigesetze der Länder Thüringen, Niedersachsen, Rheinland-Pfalz und Hessen nehmen ebenfalls geschäftsmäßige Telekommunikationsdienstleistungsunternehmen in die Pflicht, um der Polizei die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen. Niedersachsen, Rheinland-Pfalz und Hessen sehen diese Verpflichtung direkt in

---

180 Der vormals verwendete Begriff der „Verbindungsdaten“ wurde entsprechend den Formulierungen im europäischen Recht ersetzt, vgl. *Reimann*, DuD 2004, 421. Der Begriff der Verkehrsdaten ist nun in § 96 TKG enthalten.

181 Vgl. dazu die Regelungen in § 34 Abs. 1, Satz 1 ThPAG, § 33 a Abs. 1 und 2 Nds.SOG, § 31 Abs. 2 POG, § 15 a Abs. 1 und 2 HSOG.

182 Art. 34 b Abs. 2, Satz 2 PAG regelt damit die sog. Zielwahlsuche. Mit der Zielwahlsuche sollen unbekannte Anschlussnummern ermittelt werden, von denen Telekommunikationsverbindungen zu einem Anschluss der betroffenen Person hergestellt worden sind (= eingehender Telekommunikationsverkehr), vgl. *Meyer-Goßner*, § 100 g StPO, Rn. 11.

183 Eine abschließende Aufzählung der Daten ist aufgrund der weiter fortschreitenden Entwicklung darin nicht zu erblicken, vgl LT-Drucks. Bayern 15/2096, S. 60. Dass die Aufzählung nicht abschließend ist, ergibt sich auch aus der Formulierung „insbesondere“ in Art. 34 b Abs. 3 PAG. Das Nds.SOG verweist für die Definition der Kommunikationsverbindungsdaten auf die Regelung des § 100 g Abs. 3 StPO, vgl. § 33 a Abs. 2 Nr. 2 iVm § 33 Abs. 1 Nds.SOG.

184 Gleiches gilt für die übrigen Polizeigesetze; vgl. LT-Drucks. 3/2128, S. 35, LT-Drucks. Nds. 15/240, S. 17, LT-Drucks. 14/2287, S. 47, LT-Drucks. Hessen 16/2352, S. 19.

185 Art. 34 a Abs. 4 PAG. Eine ähnliche Regelung enthält § 33 b Abs. 2 Nds.SOG. Der niedersächsische Gesetzgeber sieht mit der Formulierung in § 33 b Abs. 2 Nds.SOG vor, dass die Unterbrechung und Verhinderung der Telekommunikation auch mit anderen technischen Mitteln als dem IMSI-Catcher möglich ist, vgl. Schriftlicher Bericht zum Entwurf eines Gesetzes zur Änderung des Niedersächsischen Gefahrenabwehrgesetzes, LT-Drucks. Nds. 15/776, S. 8.

ihren Polizeigesetzen vor[186], während das ThPAG auf die Regelungen des G-10-Gesetzes verweist.[187]

Der Einsatz des IMSI-Catchers ist ebenfalls in Niedersachsen, Rheinland-Pfalz und Hessen geregelt. Das Nds.SOG enthält wie das PAG die Möglichkeit, Telekommunikationsverbindungen mittels IMSI-Catcher zu unterbrechen und zu verhindern.

Die Zielwahlsuche zu präventiven Zwecken ist lediglich im PAG vorgesehen.

II. Die Telekommunikationsdaten

In der Bundesrepublik Deutschland war die Telekommunikationsordnung bis zum Inkrafttreten des TKG[188] am 1.8.1996 durch staatliche Monopole gekennzeichnet. Mit der zum 01.01.1995 in Kraft getretenen so genannten Postreform II[189] erfolgte neben der Umwandlung der Deutschen Bundespost Telekom in eine Aktiengesellschaft zugleich auch eine Befristung derjenigen Gesetze bis zum 31.12.1997, welche die ordnungspolitischen Rahmenbedingungen im Telekommunikationsbereich unter Aufrechterhaltung der Monopole für Netze und Sprachtelefondienst regelten.[190] Diese wurden durch das TKG 1996 ersetzt.

Im Jahr 2002 sind mehrere europäische Richtlinien in Kraft getreten, die in nationales Recht umzusetzen waren.[191] Die Umsetzung war nach Ansicht der Bundesregierung nicht allein

---

186 Vgl. § 33 a Nds.SOG; § 31 Abs. 6 POG; § 15 Abs. 1 HSOG.

187 Vgl. § 34 a Abs. 4, Satz 1 ThPAG, der auf die Vorschrift des § 2 Abs. 1, Sätze 3 und 4; Abs. 2 und 3 des G-10-Gesetzes verweist. Siehe dazu die Ausführungen unter IV.3.

188 BGBl. I, S. 1120, im Folgenden TKG 1996. Einen Überblick über die Entwicklung – insbesondere der datenschutzrechtlichen Vorschriften – des Telekommunikationsrechts gibt *Elbel*, 2005, S. 3 ff.

189 Gesetz über die Neuordnung des Postwesens und der Telekommunikation vom 14.09.1994, BGBl. I, S. 2325.

190 Es handelte sich dabei um das Gesetz über die Regulierung der Telekommunikation und des Postwesens (PTRegG), das Fernmeldeanlagengesetz (FAG), das Telegraphenwegegesetz (TWegG) und das Gesetz zur Vereinfachung des Planverfahrens für Fernmeldelinien (PlVereinfG), die allesamt durch das TKG ersetzt wurden, vgl. *Scheurle*, in: Scheurle/Mayen (Hrsg.), § 1 TKG, Rn. 1.

191 Richtlinie 2002/21/EG vom 07.03.2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und –dienste (Rahmenrichtlinie), ABl. EG Nr.L 108, S. 33; Richtlinie 2002/20/EG vom 07.03.2002 über die Genehmigung elektronischer Kommunikationsnetze und –dienste (Genehmigungsrichtlinie), ABl. EG Nr. L 108, S. 21; Richtlinie 2002/19/EG vom 07.03.2002 über den Zugang an elektronischen Kommunikationsnetzen und zugehörigen Einrichtungen sowie deren Zusammenschaltung (Zugangsrichtlinie), ABl. EG Nr. L 108, S. 7; Richtlinie 2002/22/EG vom 07.03.2002 über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und –diensten (Universaldienstrichtlinie), ABl. EG Nr. L 108, S. 51; sowie Richtlinie 2002/58/EG vom 12.07.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. EG Nr. L 201, S. 37.

durch Änderungen des bestehenden Telekommunikationsgesetzes möglich, sondern machte vielmehr eine Neufassung und damit weitreichende Überarbeitung des Gesetzes erforderlich.[192] Das TKG ist am 26.06.2004 in Kraft getreten.[193] Das neue TKG ist gegenüber dem TKG 1996 detaillierter. Die früher außerhalb des TKG 1996 zu einzelnen Teilbereichen bestehenden Verordnungen[194] sind nunmehr direkt im Gesetz enthalten.[195]

Das TKG teilt die bei Telekommunikationsvorgängen anfallenden Daten in vier Kategorien ein: Bestandsdaten, Verkehrsdaten, Standortdaten und Nachrichteninhalte.

1. Bestandsdaten

Bestandsdaten sind nach § 3 Nr. 3 TKG Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden.[196]

Zu den Bestandsdaten, gehören insbesondere Anrede, Name, Vorname, Geburtsdatum, Straße, Postleitzahl, Ort, Kundennummer, Rufnummern, Art der Anschlüsse, Endeinrichtung, Betriebsmöglichkeiten, Angaben zur Leitungsführung, Störungshistorie (zur vertragsgemäßen Erfüllung von Störungsbeseitigungspflichten), Rückrufnummern (soweit sie von den Anschlussnummern abweichen), Verrechnungs-Nummern sowie Rechnungsdaten (z.B. Rechnungsanschrift, Bankverbindung, Lastschriftermächtigungen usw.).[197]

---

192 Vgl. Entwurf eines Telekommunikationsgesetzes der Bundesregierung, BT-Drucks. 15/2316, S. 1.

193 BGBl. I, S. 1190, zuletzt geändert durch Art. 2 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007, BGBl. I, S. 3198.

194 Telekommunikations-Universaldienstverordnung vom 31.01.1997, BGBl. I, S. 141; Telekommunikations-Datenschutzverordnung vom 18.12.2000, BGBl. I, S. 1740, geändert durch das Gesetz zur Bekämpfung des Missbrauchs von 0190er-/0900er-Mehrwertdiensterufnummern vom 09.08.2003, BGBl. I, S. 1590; Telekommunikations-Entgeltregulierungsverordnung vom 01.10.1996, BGBl. I, S. 1492; Frequenzzuteilungsverordnung vom 26.04.2001, BGBl. I, S. 829; Netzzugangsverordnung vom 23.10.1996, BGBl. I, S. 1568.

195 Zum neuen TKG siehe *Heun*, CR 2004, 893 ff.; *Reimann*, DuD 2004, 421 ff.; *Scherer*, NJW 2004, 3001 ff. Zur Kritik an den Änderungen durch das TKG-Änderungsgesetz vom 18.02.2007, BGBl. I, S. 106, siehe *Gola/Klug*, NJW 2007, 2452 (2454).

196 Ausführlich zu den Bestandsdaten *Elbel*, 2005, S. 117 ff. Siehe auch *Holznagel/Enaux/Niehaus*, 2006, Rn. 665 ff.; *Meister/Laun*, in: Wissmann (Hrsg.), Kapitel 14, Rn. 45 ff.

197 Vgl. *Königshofen*, § 5 TDSV, Rn. 4.

Bei der Erbringung von Telekommunikationsdiensten, die auf dem Internet-Protokoll (IP)[198] basieren, ist es für Diensteanbieter, die als Access-Provider Nutzern den Zugang zum Internet ermöglichen, unter Umständen notwendig, diesen eine feste IP-Nummer für Adressierungszwecke zuzuweisen. Insbesondere größere Unternehmen, die über eine Standleitung ins Internet verfügen, erhalten feste IP-Adressen. Diese IP-Nummer ist dann ein Bestandsdatum.[199]

Bestandsdaten darf der Telekommunikationsdiensteanbieter speichern. Einige Bestandsdaten, nämlich die Rufnummern, den Namen und die Anschrift des Rufnummerninhabers, das Datum des Vertragsbeginns, bei natürlichen Personen deren Geburtsdatum sowie bei Festnetzanschlüssen auch die Anschrift des Anschlusses und ein etwaiges Vertragsende hat der geschäftsmäßige Diensteerbringer sogar zu erheben und zu speichern.[200] Die Bestandsdaten sind bei Beendigung des Vertragsverhältnisses mit Ablauf des auf die Beendigung folgenden Kalenderjahres zu löschen.[201]

2. Verkehrsdaten

Die Diensteanbieter dürfen nach § 96 Abs. 1 TKG die dort aufgeführten Verkehrsdaten[202] erheben und verwenden. Es sind dies u.a. die Nummern oder Kennungen des anrufenden und

---

198 Das Internetprotokoll ist das Standardtransportprotokoll mit dem die Benutzeranfragen nach bestimmten Internetseiten „verschickt werden", vgl. *Balzert,* 2001, S. 944.

199 Vgl. *Königshofen*, § 5 TDSV, Rn. 4. Der von Access-Providern bereitgestellte Internet – Zugang erfolgt jedoch in der Regel durch die dynamische Vergabe von IP-Nummern (so genannte temporäre IP-Adresse), vgl. *Nack*, in: KK, § 100 g StPO, Rn. 11. Diese ändern sich bei jeder Neueinwahl ins Internet. Da diese IP-Adresse nicht einer bestimmten oder bestimmbaren Person zugeordnet werden können, handelt es sich bei diesem Datum nicht um ein Bestandsdatum, sondern um ein Verbindungsdatum, vgl. *Königshofen*, § 5 TDSV, Rn. 5. *Tinnefeld/Schuster*, DuD 2005, 78 (81); *Gnirck/Lichtenberg*, DuD 2004, 598 (600); LG Bonn DuD 2004, 628; aA LG Stuttgart, NJW 2005, 614; *Nack*, in: KK, § 100 g StPO Rn. 11 und auch im Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, BT-Drucks. 16/5864, S. 27, wird davon ausgegangen, dass eine dynamische IP-Adresse ein Bestandsdatum ist. Aus der Gesetzesbegründung zum TKG ergibt sich jedoch, dass § 96 Abs. 1 Nr. 1 TKG (in der Begründung noch § 94 Abs. 1 Nr. 1 TKG) sinngemäß auf IP-Adressen Anwendung findet, soweit sie der Erbringung von Telekommunikationsdiensten dienen, während E-Mail-Adressen und statischen IP-Adressen zu den nach § 95 TKG (in der Begründung noch § 93 TKG) erhobenen Daten gehören, vgl. BT-Drucks. 15/2316, S. 89, 97.

200 § 111 Abs. 1 TKG. Vgl. zu dieser Verpflichtung die Ausführungen zu den Auskunftsansprüchen der Polizei in diesem Kapitel unter III. 3. a).

201 § 95 Abs. 3 TKG.

202 Verkehrsdaten sind allgemein nach § 3 Nr. 30 TKG Daten, die bei Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Ausführlich zu den Verkehrsdaten *Elbel*, 2005, S. 135 ff; *Holznagel/Enaux/Nienhaus*, 2006, Rn. 668 f.; *Meister/Laun*, in: Wissmann (Hrsg.), Kapitel 14, Rn. 48 ff; *Hartung*, in: Wilms/Masin/Jochum (Hrsg.), § 96 TKG, Rn. 1, 12, 29 ff.

angerufenen Anschlusses oder der Endeinrichtung (z.B. Fax-Kennung), personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen die IMSI, die IMEI[203] und die Standortdaten.[204] Auch Positionsdaten, die bereits im Vorfeld der mobilen Kommunikation erhoben werden (Mobilfunkgerät betriebsbereit am Netz angemeldet), fallen unter die Verkehrsdaten.[205] Weiter sind Verkehrsdaten auch das Datum, die Uhrzeit, die Dauer der Verbindung, der vom Nutzer in Anspruch genommene Telekommunikationsdienst und die dynamische IP-Adresse.

Die gespeicherten Verbindungsdaten dürfen gemäß § 96 Abs. 2 Satz 1 TKG über das Ende der Verbindung hinaus nur verarbeitet oder genutzt werden, soweit sie zum Aufbau weiterer Verbindungen oder für die Entgeltermittlung und –abrechnung, einen Einzelverbindungsnachweis, zur Beseitigung von Störungen an Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten sowie zur netzübergreifenden Auskunft bei bedrohenden oder belästigenden Anrufen benötigt werden oder wenn sie für die durch andere gesetzliche Vorschriften begründeten Zwecke erforderlich sind[206]; ansonsten sind sie vom Diensteanbieter unverzüglich zu löschen.[207] Sobald also beispielsweise die Störungs- bzw. Fehlerursache erkannt ist, sind die Daten unverzüglich zu löschen, sollten sie nicht noch für andere erlaubte Zwecke (z.B. Entgeltabrechnung) weiterverwendet werden dürfen.[208]

Die Verbindungsdaten, die für die Berechnung des Entgelts erforderlich sind, dürfen nach § 97 Abs. 3, Satz 3 TKG bis höchstens sechs Monate nach Versendung der Rechnung gespeichert werden. Die Vorschrift des § 100 Abs. 3, Satz 2 TKG sieht kein eigenständiges Speicherungsrecht vor, sondern regelt lediglich, wie mit den schon vorhandenen Verbindungsdaten für Zwecke der Missbrauchsbekämpfung vorzugehen ist.[209]

---

203 Nach BGH CR 1998, 738 (740) unterfallen die IMEI und wohl auch die IMSI dem Begriff der Kennung. Vgl. auch *Hartung*, in: Wilms/Masing/Jochum (Hrsg.), § 96 TKG, Rn. 40.

204 Bei der Standortkennung identifiziert sich die Funksende- und Empfangsanlage, in dessen Reichweite sich das gerade betriebene Handy befindet. Zum Begriff der Funkzelle vgl. § 2 Nr. 5 TKÜV.

205 Vgl. BGH RDV 2001, 182 f.; LG Aachen StV 1999, 590 (591) mit Anmerkung von *Bernsmann/Jansen*, StV 1999, 591 ff.; LG Ravensburg NStZ-RR 1999, 84 (85); *Königshofen*, § 6 TDSV, Rn. 4.

206 Dass Verkehrsdaten auch genutzt werden dürfen, wenn sie für die durch andere gesetzliche Vorschriften begründeten Zwecke erforderlich sind, wurde erst durch das Telekommunikationsänderungsgesetz vom 18.02.2007, BGBl. I, S. 106 eingefügt. Zur hieran erhobenen Kritik vgl. *Gola/Klug*, NJW 2007, 2452 (2454).

207 § 96 Abs. 2 TKG.

208 Vgl. *Königshofen*, § 9 TDSV, Rn. 10.

209 Vgl. *Königshofen*, § 9 TDSV, Rn. 29. Nach dem Wortlaut des § 100 Abs. 3, Satz 2 TKG wäre davon auszugehen, dass nur Verbindungsdaten genutzt und verarbeitet werden dürfen, die nicht älter als sechs Monate sind. Der Verordnungsgeber zur TDSV ist jedoch nach der amtlichen Begründung davon ausge-

Auch eine Speicherung von IP-Adressen findet in der Praxis statt.[210] Diese Speicherung ist zulässig zur Verhinderung von Missbrauch und zur Datensicherheit, sofern die IP-Adressen der Erbringung von Telekommunikationsdiensten dienen.[211] Ob IP-Adressen auch zu Abrechnungszwecken gespeichert werden dürfen, ist nicht abschließend geklärt.[212]

Aufgrund des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG § 113 a TKG besteht nunmehr eine Verpflichtung der Anbieter von öffentlichen zugänglichen Telekommunikationsdiensten zur Speicherung der in § 113 a Abs. 2 TKG genannten Verkehrsdaten für die Dauer von sechs Monaten.[213]

3. Standortdaten

Wie sich aus § 96 Abs. 1 Nr. 1 TKG ergibt, sind die Standortdaten[214] ein Unterfall der Verkehrsdaten.[215] Standortdaten sind für Mobilfunkanschlüsse von Bedeutung. Ist das Mobil-

---

gangen, dass diese Frist der Speicherhöchstfrist zu Entgeltzwecken entspricht, vgl. BR-Drucks. 300/00, S. 18. Diese Frist beginnt jedoch erst mit dem Versand der Rechnung. Demzufolge war § 9 Abs. 2 TDSV auch in diesem Sinne zu verstehen, vgl. *Königshofen*, § 9 TDSV, Rn. 28. § 100 TKG folgt der Regelung des § 9 TDSV nach, vgl. BT-Drucks. 15/2316, S. 90.

210 Vgl. *Gnirck/Lichtenberg*, DuD 2004, 598 (599); *Hartung*, in: Wilms/Masing/Jochum (Hrsg.), § 96 TKG, Rn. 35 ff.

211 Vgl. BT-Drucks. 15/2316, S. 90. Die Einschränkung „sofern sie der Erbringung von Telekommunikationsdiensten dienen" erklärt sich dadurch, dass IP-Adressen auch Nutzungsdaten iSd § 6 TDDSG sein können, vgl. *Tinnefeld/Schuster*, DuD 2005, 78 (81).

212 Das Regierungspräsidium Darmstadt hat in einer Mitteilung, abgedruckt in DuD 2003, 177, an alle Kunden des größten deutschen Internet-Zugangsproviders, die sich bei der Aufsichtsbehörde über die Speicherung dynamischer IP-Adressen bei Nutzung einer Flatrate beschwert hatten, diese Praxis als datenschutzrechtlich zulässig bezeichnet. Zur Gegenansicht, die davon ausgeht, dass die Speicherung von IP-Adressen weder bei normalen Online-Tarifen noch bei einer Flatrate notwendig ist, vgl. *Dix*, DuD 2003, 234 (235) und *Heidrich*, DuD 2003, 237. Nach *Tinnefeld/Schuster*, DuD 2005, 78 (81) ist jedenfalls bei einem Flatrate-Tarif eine Speicherung nicht erlaubt und die Zuteilung der IP-Adresse nach Beendigung der Verbindung zu löschen. Das AG Darmstadt hat mit Urteil vom 30.06.2005 – 300 C 397/04 – entschieden, dass die dynamische IP-Adresse gelöscht werden muss, sobald sie für Abrechnungszwecke nicht mehr erforderlich ist, vgl. *Gola/Klug*, NJW 2005, 2434 (2437). Siehe ausführlich auch *Hartung*, in: Wilms/Masing/Jochum (Hrsg.), § 96 TKG, Rn. 35 ff.

213 Die Speicherpflicht wird durch die einstweilige Anordnung des BVerfG vom 11.03.2008 – 1 BvR 256/08 nicht berührt. Lediglich die Weitergabe der Daten ist den Telekommunikationsanbietern bis zur Entscheidung in der Hauptsache nur unter den Voraussetzungen des § 100 a Abs. 1 und 2 StPO erlaubt (vgl. Beschluss des BVerfG vom 11.02.2008, Rn. 176).

214 § 3 Nr. 19 TKG. Siehe zu den Standortdaten *Elbel*, 2005, S. 203 ff; *Wittern*, in: BeckTKG-Komm, § 98 TKG, Rn. 4 f.

215 Vgl. *Hartung*, in: Wilms/Masing/Jochum (Hrsg.), § 98 TKG, Rn. 13. Standortdaten für Dienste mit Zusatznutzen sind darüber hinaus z.B. Beratung hinsichtlich der billigsten Tarifpakete, Navigationshilfen, Verkehrsinformationen, Wettervorhersagen und touristische Informationen, vgl. *Holznagel/Enaux/Neinhaus*, 2006, Rn. 670.

funkgerät auf „Stand-by“ geschaltet, übermittelt es Daten an die jeweilige Funkzelle, in der es sich gerade befindet. So kann der Standort funkzellengenau ermittelt werden.[216]

Standortdaten dürfen gemäß § 98 Abs. 1 TKG nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden. Voraussetzung ist, dass die Daten anonymisiert werden oder der Teilnehmer seine Einwilligung erteilt hat.

4. Nachrichteninhalte

Das Aufzeichnen von Nachrichteninhalten ist nur erlaubt, wenn es Gegenstand des angebotenen Dienstes oder aus technischen Gründen Bestandteil des Dienstes ist (z.B. Mailbox-Dienste von Mobilfunkunternehmen, T-Net-Box).[217] Die weitere Verarbeitung darf nur unter den Voraussetzungen des § 107 Abs. 1 TKG erfolgen.

III. Die Erhebung der Telekommunikationsdaten

Die Polizeibehörden erlangen Zugriff auf die Telekommunikationsdaten durch die Inanspruchnahme von Diensteanbietern[218] oder den Einsatz des IMSI-Catchers[219].

1. Der Schutz des Fernmeldegeheimnisses nach § 88 TKG

Nach § 88 TKG unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war, dem Fernmeldegeheimnis.

§ 88 TKG wird als die einfachgesetzliche Ausprägung des durch Art. 10 GG geschützten Fernmeldegeheimnisses angesehen.[220] Die beiden Vorschriften haben jedoch unterschiedli-

---

216 Eine Mobilfunkzelle kann in einem der D-Netze einen Durchmesser von mehreren Kilometern besitzen, vgl. *Fox*, DuD 2002, 212 (213). Ist ein Endgerät jedoch mit einem GPS-Empfänger verbunden, so lässt sich der Standort mit wenigen Metern Abweichung exakt bestimmen, vgl. *Wittern*, in: BeckTKG-Komm, § 98 TKG, Rn. 1.

217 Vgl. *Wittern*, in: BeckTKG-Komm, § 107 TKG, Rn. 2.

218 Vgl. § 34 a Abs. 1, Satz 1 ThPAG; §§ 33 a Abs. 7, 33 c Nds.SOG; Art. 34 b Abs. 1, Abs. 2 PAG; § 31 Abs. 6 POG; § 15 a Abs. 1 HSOG.

219 Vgl. § 33 b Abs. 1 Nds.SOG, Art. 34 a Abs. 2 – 4 PAG, § 31 Abs. 1 und 2 POG und § 15 a Abs. 3 HSOG.

che Adressatenkreise: Art. 10 GG richtet sich gegen staatliche Eingriffe in die Telekommunikation, § 88 Abs. 1 und 2 TKG wendet sich an private (geschäftsmäßige) Erbringer von Telekommunikationsdiensten.[221]

Durch die Regelungen über das Fernmeldegeheimnis und den Datenschutz im siebten Teil des TKG erfüllt der Gesetzgeber seine aus der objektiven Wertentscheidung der Verfassung folgenden Schutzpflichten[222], da sich auch nach der Umwandlung der Unternehmen der ehemaligen deutschen Bundespost und der Liberalisierung des Telekommunikationsmarktes die Theorie einer unmittelbaren Drittwirkung des Art. 10 GG nicht hat durchsetzen können.[223]

§ 88 Abs. 1 TKG stellt den Inhalt der Telekommunikation und deren nähere Umstände gleich. Zum Inhalt gehört grundsätzlich alles, was während des jeweiligen Telekommunikationsvorgangs ausgesandt, übermittelt oder empfangen wird, insbesondere also das stattfindende Gespräch, aber auch übermittelte Zeichen, Töne und Bilder.[224] Zu den näheren Umständen der Telekommunikation zählen alle Verkehrsdaten und sonstigen Umstände, die den jeweiligen Telekommunikationsvorgang individualisierbar machen.[225] Die Bestandsdaten unterfallen dagegen nicht dem Schutz des Fernmeldegeheimnisses.[226]

---

220 Vgl. *Bock*, in: BeckTKG-Komm, § 88 TKG, Rn. 1; *Zerres*, in: Scheurle/Mayen (Hrsg.), § 85 TKG, Rn. 1; *Lammich*, § 85 TKG, Rn. 1; *Etling-Ernst*, § 85 TKG Rn. 1.

221 Es werden weder Behörden noch andere Private, die nicht an der Erbringung von Telekommunikationsdiensten beteiligt sind, zur Wahrung des Fernmeldegeheimnisses verpflichtet. Diese Pflicht besteht für Behörden unmittelbar auf Grund des Art. 10 GG, vgl. *Bock*, in: BeckTKG-Komm, § 88 TKG, Rn. 1. Sonstige Private werden durch § 201 StGB, siehe dazu *Lenckner*, in: Schönke/Schröder, § 201 StGB, Rn. 2 und § 89 TKG verpflichtet, Eingriffe in nichtöffentliche Telekommunikationsvorgänge zu unterlassen, vgl. *Bock*, in: BeckTKG-Komm, § 88 TKG, Rn. 1. Das Interesse, den Inhalt und die näheren Umstände der Telekommunikation gegenüber Dritten geheim zu halten, wird daher von § 88 TKG nicht umfassend, sondern im Hinblick auf bestimmte Dritte geschützt; nämlich gegenüber denjenigen, deren sich der Bürger zur Übermittlung der Nachrichten bedient. So zu Art. 10 GG auch BVerfGE 85, 386 (396); siehe dazu *Groß*, JZ 1999, 326 (332).

222 Dazu *Hermes*, in: Dreier (Hrsg.), Art. 10 GG, Rn. 83: Aus der Bedeutung des Art. 10 GG als objektives Prinzip der gesamten Rechtsordnung, folgt die Verpflichtung aller grundrechtsgebundener Hoheitsträger, die Vertraulichkeit des Brief- und Fernmeldeverkehrs gegenüber Übergriffen nichtstaatlicher Dritter zu schützen. (...) Soweit Beeinträchtigungen des Geheimnisschutzes von Seiten privater Dritter zu besorgen sind, hat der Gesetzgeber durch den Einsatz straf-, zivil- und verwaltungsrechtlicher Instrumente für einen effektiven Schutz Sorge zu tragen. Siehe auch *Meister/Laun*,in: Wissmann (Hrsg.) Kapitel 14, Rn. 3.

223 Vgl. *Zerres*, in: Scheurle/Mayen (Hrsg.), § 85 TKG, Rn. 2; *Schmitt Glaeser*, in: HStR VI, § 129, Rn. 66; *Groß*, JZ 1999, 326 (329); *Lang*, Archiv PT 1997, 298 (299). Die frühere Doppelfunktion des Art. 10 GG, nicht nur den Bürger vor staatlichen Eingriffen, sondern auch das staatliche Unternehmen Post gegenüber anderen staatlichen Stellen zu schützen, ist daher nicht mehr erforderlich, vgl. BVerfGE 85, 386 (396); E 67, 157 (172).

224 Vgl. *Zerres*, in: Scheurle/Mayen (Hrsg.), § 85 TKG, Rn. 15; *Trute*, in: Trute/Spoerr/Bosch, § 85 TKG, Rn. 8.

225 Vgl. *Meister/Laun*, in: Wissmann (Hrsg.), Kapitel 14, Rn. 6 ff.; *Bock*, in: BeckTKG-Komm, § 88 TKG, Rn. 13 ff.; *Zerres*, in: Scheurle/Mayen (Hrsg.), § 85 TKG, Rn. 17; BVerfGE 67, 157 (172); E 85, 386

2. Die verpflichteten Diensteanbieter

Nach § 88 Abs. 2 TKG ist jeder Diensteanbieter zur Wahrung des Fernmeldegeheimnisses verpflichtet. Die §§ 91 ff. TKG[227] regeln den Schutz personenbezogener Daten bei deren Erhebung und Verwendung durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste erbringen oder an deren Erbringung mitwirken.[228]

Die untersuchten Landesgesetze verpflichten geschäftsmäßige Erbringer von Telekommunikationsdiensten zur Auskunftserteilung und Überwachungsermöglichung.[229]

a) Geschäftsmäßige Diensteanbieter

Diensteanbieter im Sinne des Telekommunikationsgesetzes ist nach § 3 Nr. 6 TKG jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt. Dabei bedeutet das „geschäftsmäßige Erbringen von Telekommunikationsdiensten“ das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht.[230]

---

(396). Dabei unterfällt auch der Ort des Telekommunikationsvorgangs den näheren Umständen. So schon BGH DuD 1999, 478; BGH ArchPT 1993, 184.; LG Dortmund DuD 1998, 472; LG Ravensburg NStZ-RR 1999, 84 (85); VG Darmstadt NJW 2001, 2273 (2274); kritisch *Zerres*, in: Scheurle/Mayen (Hrsg.), § 85 TKG, Rn. 18, der den Sinn der für die Überwachung des Fernmeldeverkehrs einschlägigen Überwachungsbefugnisse nicht darin sieht, ein Bewegungsbild des Überwachten zu erlangen. *Nack*, in: KK, § 100 a StPO, Rn. 14, sieht bei der Erstellung von Bewegungsprofilen weniger einen Eingriff in Art. 10 GG als in Art. 1 Abs. 1 iVm Art. 2 Abs. 1 GG. § 96 Abs. 1 Nr. 1 TKG unterstellt die Standortdaten nunmehr aber eindeutig den Verkehrsdaten.

226 Allgemeine Meinung, vgl. nur *Bock*, in: BeckTKG-Komm, § 88 TKG, Rn. 14.

227 Die Bundesregierung hatte gemäß § 89 Abs. 1 TKG 1996 durch die Telekommunikations-Datenschutzverordnung vom 01.10.1996 (TDSV), BGBl. I, S. 1492, Vorschriften zum Schutze personenbezogener Daten der an der Telekommunikation Beteiligten erlassen. Um den gesamten Telekommunikationsdatenschutz zu straffen und um Redundanzen zu vermeiden, wurden die Vorschriften der TDSV in das TKG übernommen, BT-Drucks. 15/2316, S. 88.

228 Vgl. *Robert*, in: BeckTKG-Komm, § 91 TKG, Rn. 1.

229 Dass die Landesgesetze geschäftsmäßige Diensteanbieter verpflichten, obwohl im TKG nun überwiegend der Begriff Diensteanbieter verwendet wird, erklärt sich dadurch, dass das TKG 1996 vorwiegend geschäftsmäßige Erbringer von Telekommunikationsdiensten als Verpflichtete vorsah. Das Erfordernis der Geschäftsmäßigkeit ist nun in der Definition des Diensteanbieters im neuen TKG enthalten.

230 § 3 Nr. 10 TKG. Durch das Merkmal des geschäftsmäßigen und nicht etwa gewerbsmäßigen Erbringens von Telekommunikationsdiensten ist der Kreis der Verpflichteten sehr weit gezogen. Dem liegt die Erwägung zugrunde, dass es auch bei Telekommunikationsangeboten, die ohne Gewinnerzielungsabsicht erfolgen, ein schützenswertes Interesse an der Geheimhaltung des Inhalts und der näheren Umstände der Telekommunikation gibt. Ein entsprechendes Schutzbedürfnis ist gerade in geschlossenen Nutzergruppen, die häufig nicht gewerblich arbeiten, jedoch sensible Geschäftsdaten oder unter das Berufsgeheimnis fallende Daten übermitteln, offenkundig, vgl. *Zerres*, in: Scheurle/Mayen (Hrsg.), § 85 TKG, Rn. 21.

Das nachhaltige Angebot von Übertragungswegen erfordert eine dauerhafte Erbringung; gelegentlich erbrachte Telekommunikationsdienste reichen für die Schutzverpflichtung mangels durchschlagendem Schutzinteresse nicht aus.[231]

Da der Telekommunikationsdienst gegenüber Dritten erbracht werden muss, unterfallen Corporate Networks, Nebenstellenanlagen in Hotels, Krankenhäusern, Betrieben und Behörden, Clubtelefone etc. der Verpflichtung, wenn diese zugleich den Beschäftigten für private Gespräche zur Verfügung gestellt werden.[232] Anderes gilt bei privaten Endgeräten, Haustelefonanlagen, Sprechanlagen etc., die regelmäßig nicht Dritten zur Verfügung gestellt sind.[233]

Dass dadurch eine Einschränkung gegenüber dem verfassungsrechtlichen Begriff des Fernmeldegeheimnisses erfolgt, der auch Kommunikation auf eigenen Übertragungswegen ebenso wie die nicht auf Dauer angelegte Kommunikation umfasst[234], ist dadurch zu erklären, dass § 88 Abs. 2 TKG nur die Schutzpflicht der nunmehr privaten Telekommunikationsunternehmen enthält und das Fernmeldegeheimnis in das Horizontalverhältnis zwischen Informationsmittler und Nutzer transformiert, nicht aber den Anwendungsbereich des Fernmeldegeheimnisses gegenüber staatlichen Stellen und sonstigen Dritten regelt.[235]

b) Angebot von Telekommunikation

Die Diensteanbieter müssen geschäftsmäßig Telekommunikation anbieten. Nach § 3 Nr. 22 TKG ist Telekommunikation der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen.[236] Zur Telekommunikation zählt nicht nur die klassische Sprachtelefonie, sondern auch die moderne Datenübertragung, sei es in Form des Faxes, des Bildschirmtextes oder der digitalen Nachrichtenübertragung

---

231 Vgl. *Meister/Laun*, in: Wissmann (Hrsg.), Kapitel 14, Rn. 10; *Trute*, in: Trute/Spoerr/Bosch, § 85 TKG, Rn. 11. *Zerres*, in: Scheurle/Mayen (Hrsg.), § 85 TKG, Rn. 23.

232 Vgl. *Bock*, in: BeckTKG-Komm, § 88 TKG, Rn. 24; *Meister/Laun*, in: Wissmann (Hrsg.), Kapitel 14, Rn. 12; *Trute*, in: Trute/Spoerr/Bosch, § 85 TKG, Rn. 11; Kritisch zu dieser Erweiterung des Anwendungsbereichs des Elften Teils des TKG 1996 *Wuermeling/Felixberger*, CR 1997, 230 ff.; *Gola/Müthlein*, RDV 1997, 193 f.

233 Vgl. *Bock*, in: BeckTKG-Komm, § 88 TKG, Rn. 24; *Trute*, in: Trute/Spoerr/Bosch, § 85 TKG, Rn. 11; BT-Drucks. 13/3609, S. 53.

234 Vgl. *Hermes*, in: Dreier (Hrsg.), Art. 10 GG, Rn. 37.

235 Vgl. *Bock*, in: BeckTKG-Komm, § 88 TKG, Rn. 1; *Meister/Laun*, in: Wissmann (Hrsg.), Kapitel 14, Rn. 3; *Trute*, in: Trute/Spoerr/Bosch, § 85 TKG, Rn. 11 und dieses Kapitel unter III. 1.

236 Telekommunikationsanlagen sind nach § 3 Nr. 23 TKG technische Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können.

zwischen Computern.[237] Denn während für den herkömmlichen Fernmeldeverkehr mehrere Kommunikationsbeteiligte erforderlich sind, erfasst die moderne Kommunikation auch die Verbindung zwischen Menschen und Computern sowie die automatisch geregelte Datenübertragung zwischen Computern.[238]

Diese Begriffsweite der Telekommunikation wirft eine Reihe von Abgrenzungsfragen auf.[239] Erhebliche Abgrenzungsprobleme bestehen im Hinblick auf die sich fortentwickelnden Multimedia-Dienste[240]. Während das TKG auf den technischen Vorgang der Telekommunikation, also die Übertragung von Daten ausgerichtet ist, beziehen sich Telemediendienste auf Inhalte und Nutzungsformen.[241]

Nach § 1 Abs. 1, Satz 1 TMG sind Telemedien alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 TKG, telekommunikationsgeschützte Dienste nach § 3 Nr. 25 TKG oder Rundfunk nach § 2 des Rundfunkstaatsvertrages sind.

---

237 Vgl. *Meister/Laun*, in: Wissmann (Hrsg.), Kapitel 14, Rn. 6; *Zerres*, in: Scheurle/Mayen, § 85 TKG, Rn. 6; *Wuermeling/Felixberger*, CR 1997, 230 (233); *Jarass*, in: Jarass/Pieroth, Art. 10 GG, Rn. 5; *Trute*, in: Trute/Spoerr/Bosch, § 85 TKG, Rn. 6.

238 Nach Ansicht von *Vassilaki*, JR 2000, 446 (447) liegt danach Telekommunikation vor bei Abfrage angekommener Nachrichten durch einen Handy-Besitzer und der vom Computer ferngesteuerten Antwort. Denn der Computer beantworte eine konkrete Frage einer konkreten Person. Diese Situation sei vergleichbar mit der Konstellation, dass der Rezeptionist eines Hotels den Gast nach Überprüfung seines Faches informiert, dass keine Nachrichten für ihn vorhanden sind.

239 Vgl. dazu *Zerres*, in: Scheurle/Mayen (Hrsg.), § 85 TKG, Rn. 10 ff.

240 Bund und Länder hatten den weder technisch, noch inhaltlich, noch funktional eindeutig zu trennenden Regelungsbereich der Multimediadienste aufgrund der unterschiedlichen Gesetzgebungskompetenzen in „Teledienste“ und „Mediendienste“ unterteilt. Für Teledienste galt das Teledienstegesetz (TDG) und für Mediendienste der Mediendienste-Staatsvertrag (MDStV). Zur Abgrenzung zwischen Telediensten und Mediendiensten vgl. *Würtenberger/Heckmann*, 2005, Rn. 547. Diese Unterscheidung ist wohl nunmehr mit dem neuen Telemediengesetz vom 26.02.2007, BGBl. I, S. 179, obsolet geworden, vgl. *Hoeren*, NJW 2007, 801 (802).

241 Die Anwendungsbereiche des MDStV und des TDG schlossen sich gegenseitig aus. Ein Mediendienst war nach § 2 Abs. 1 MDStV „das Angebot und die Nutzung von an die Allgemeinheit gerichteten Informations- und Kommunikationsdiensten ... in Text, Ton und Bild ...“. Als nicht abschließende Beispiele nannte § 2 Abs. 2 MDStV Fernseheinkauf, Verteildienste, Fernsehtext, Video-on-Demand und multimediale Presse. Nach § 2 Abs. 1 TDG waren Teledienste „elektronische Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind ...“. Beispielhaft nannte § 2 Abs. 2 TDG Telebanking, Telespiele, Datendienste und Angebote zur Nutzung des Internets. Das Telemediengesetz als Teil des Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr–Vereinheitlichungsgesetz) vom 26.02.2007, BGBl. I, S. 179 hat diese Differenzierung nunmehr mit dem einheitlichen Begriff „Telemedien“ oder „Telemediendienste“ aufgehoben, § 1 Abs. 1, Satz 1 TMG.

Dem Schutz des Fernmeldegeheimnisses und damit auch den Schutzvorschriften der §§ 88 ff. TKG unterliegen individuelle Kommunikationsvorgänge.[242] Damit hat insbesondere eine Abgrenzung zwischen Telekommunikation und den Telemediendiensten zu erfolgen, die elektronische Informations- und Kommunikationsdienste zur individuellen Nutzung beinhalten.[243]

Da die Nutzung von Telemedien durch (Tele-)Kommunikation erfolgt[244], bedarf es damit auch der Feststellung, wer diese Telekommunikation anbietet und Diensteanbieter im Sinn des TKG ist. Diensteanbieter nach § 2 Nr. 1 TMG ist, wer eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt. Soweit die Übermittlung durch Telekommunikation erfolgt, sind die Diensteanbieter (auch) den Vorschriften des TKG unterworfen.[245] Wer dagegen nur eigene Inhalte anbietet oder sich fremde Inhalte zu eigen macht, ist lediglich Telemedienanbieter.[246]

Deutlich wird diese Abgrenzung beim Versand einer E-Mail. Der Nutzer wählt sich über seinen Zugangsprovider ins Internet ein und besucht die Seite seines Webmail-Providers. Bei der vom Zugangsprovider erbrachten Leistung handelt es sich um Telekommunikation.[247]

Bei dem Angebot, einen E-Mail-Dienst über eine im Internet angebotene Oberfläche zu versenden, handelt es sich um einen Telemediendienst.[248] Der konkrete Versand der E-Mail erfolgt wieder mittels Telekommunikation.[249] Auch die dann abrufbereit gespeicherte, aber

---

242 Vgl. *Hermes*, in Dreier (Hrsg.), Art. 10 GG, Rn. 38, *Jarras*, in: Jarras/Pieroth, Art. 10 GG Rn. 10; *Loewer*, in: v.Münch/Kunig (Hrsg.), Art. 10 GG, Rn. 12. Daher kann die Abgrenzung zu Mediendiensten als an die Allgemeinheit gerichtete Kommunikationsdienste unterbleiben. Vgl. zur Abgrenzung Individualkommunikation/Massenkommunikation auch *Vassilaki*, JR 2000, 446 (448).

243 Z.B. Telebanking, Telespiele, Datendienste und Angebote zur Nutzung des Internets.

244 Vgl. *Würmeling/Felixberger*, CR 1997, 230 (233); *Zerres*, in: Scheurle/Mayen (Hrsg.), § 85 TKG, Rn. 12.

245 Vgl. *Hoeren*, NJW 2007, 801 (802).

246 Vgl. *Zerres*, in: Scheurle/Mayen (Hrsg.), § 85 TKG, Rn. 12; *Ebert/Honnacker/Seel*, Vorb. § 34 a ThPAG, Rn. 33. Eine Ausweitung des Auskunftsanspruchs aus § 100 g StPO auf Teledienstnutzungsdaten hat der Gesetzgeber abgelehnt, vgl. BT-Drucks. 14/7679, S. 7.

247 Vgl. *Wittern/Schuster*, in: BeckTKG-Komm, § 3 TKG, Rn. 49; *Bock*, in: BeckTKG-Komm, § 88 TKG, Rn. 22; *Hoeren*, NJW 2007, 801 (802); *Breyer*, DuD 2003, 491; *Tinnefeld/Schuster*, DuD 2005, 78 (81); OLG Hamburg MMR 2000, 611 (613); AG Wiesbaden MMR 2002, 563; aA RP Darmstadt, DuD 2003, 177.

248 Vgl. *Tinnefeld/Schuster*, DuD 2005, 78 (81).

249 Vgl. *Tinnefeld/Schuster*, DuD 2005, 78 (81).

noch nicht gelesene Nachricht in der Mailbox des Empfängers fällt unter den Begriff der Telekommunikation, da der Kommunikationsvorgang noch nicht abgeschlossen ist.[250]

Verpflichtete nach dem TKG können demnach nicht nur Telekommunikationsunternehmen sein, die Telefondienste anbieten, sondern auch Access-Provider oder sonstige Service-Provider, die (Internet-)Telekommunikation anbieten.[251]

3. Die Weitergabe der Telekommunikationsdaten an Dritte

§ 88 Abs. 3 TKG enthält Verhaltensregeln für die in § 88 Abs. 2 TKG auf den Schutz des Fernmeldegeheimnisses Verpflichteten. Diese bestehen aus Unterlassungsgeboten, die sich auf die Kenntnisnahme von Informationen beziehen, die dem Fernmeldegeheimnis unterfallen. Auch sehen sie die Festlegung von Verwendungszwecken für durch das Fernmeldegeheimnis geschützte Informationen vor.[252] Den zu Wahrung des Fernmeldegeheimnisses Verpflichteten ist es grundsätzlich untersagt, sich Kenntnis über den Inhalt und die näheren Umstände der Telekommunikation zu verschaffen.

---

250 Vgl. *Meister/Laun*, in: Wissmann (Hrsg.), Kapitel 14, Rn. 8; *Bock*,in: BeckTKG-Komm, § 88 TKG, Rn. 17; *Vassilaki*, JR 2000, 446 (447). So auch BGH CR 1996, 488 (489) für den Zugriff auf Handy-Mailboxen und *Kudlich*, JuS 1998, 209 (212 ff.), der zur Begründung einen effektiven Grundrechtsschutz anführt, da die Gefahr für staatliche Zugriffe in erhöhtem Maß besteht, wenn die Kommunikation nicht in Echtzeit abgeschlossen ist, sondern Speicherphasen einen zeitlich erheblich längeren Zugriff ermöglichen; aA *Bär*, CR 1996, 490 (491); *Bizer*, DuD 1996, 627; *Palm/Roy*, NJW 1996, 1791 (1793) mit dem Argument, dass es sich bei der Zwischenspeicherung um keine Weiterbeförderung der Nachricht handele. Siehe dazu auch *Roggan*, 2003, S. 60 ff., nach dem die auf Mailboxen zwischengespeicherten Daten de lege lata nicht dem Zugriff der Polizei unterliegen und es sich insoweit um eine „überwachungsfreie Enklave" handelt. Aus dem Urteil des BVerfG vom 02.03.2006 in NJW 2006, 976 ff. ergibt sich nichts Gegenteiliges. Das Gericht hatte u.a. über die Rechtmäßigkeit der Beschlagnahme eines Mobiltelefons und die Auswertung der darin gespeicherten Telekommunikationsdaten zu befinden. Das BVerfG hat die nach Abschluss des Kommunikationsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Daten dem Schutz des Rechts auf informationelle Selbstbestimmung und nicht dem Fernmeldegeheimnis unterstellt, da der Übertragungsvorgang beendet war und der Empfänger somit eigene Schutzvorkehrungen gegen den ungewollten Datenzugriff treffen konnte, vgl. BVerfG NJW 2006, 976 (978 f.).

251 Zu den unterschiedlichen Arten von Internet Service Providern vgl. *Summa*, in: Holznagel/Nelles/Sokol, S. 25. Bezogen auf Access-Provider muss bei jeder einzelnen Dienstleistung eines solchen Anbieters geschaut werden, ob die Transportleistung im Vordergrund steht oder der transportierte Inhalt. Besteht der Dienst „überwiegend" in der Übertragung von Signalen, soll er zugleich Telekommunikationsdienst nach dem TKG und Telemediendienst sein. So die Gesetzesbegründung zum TKG für den „Internet-Zugang", vgl. BT-Drucks. 16/3078, S. 17.

252 Vgl. *Holznagel/Enaux/Nienhaus*, 2006, Rn. 647; *Meister/Laun*, in: Wissmann (Hrsg.), Kapitel 14, Rn. 15 f.; *Trute*, in: Trute/Spoerr/Bosch, § 85 TKG, Rn. 15.

Das Verbot sich Kenntnis zu verschaffen, verbietet den Einsatz technischer oder sonstiger Mittel, um Telekommunikation zu entschlüsseln, abzuhören, Verkehrsdaten zu erheben oder in sonstiger Weise zu überwachen.[253]

Erlaubt ist die Kenntnisverschaffung von Informationen, die für die geschäftsmäßige Erbringung von Telekommunikationsdiensten erforderlich sind. Die Kenntnisse dürfen nur zu diesem Zweck verwendet werden.[254]

Die Weitergabe von Kenntnissen über den Inhalt und die näheren Umstände der Telekommunikation durch den Dienstanbieter ist gemäß § 88 Abs. 3, Satz 3 TKG nur zulässig, wenn das TKG oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht.[255] Für die Weitergabe von Kenntnissen sieht das TKG folgende Regelungen vor:

a) Die Auskunft

Das TKG unterscheidet zwischen der Auskunft über Bestandsdaten[256] und der Auskunft über Verkehrsdaten. Auskunft über Bestandsdaten kann nach den §§ 112 Abs. 2 und 4 und 113 Abs. 1 TKG verlangt werden. Für die Auskunft über Verkehrsdaten ist eine gesetzliche Vorschrift im Sinne von § 88 Abs. 3, Satz 3 TKG erforderlich.

aa) Die Auskunft nach § 112 Abs. 4 TKG

Nach § 112 Abs. 2 Nr. 2 und Abs. 4, Satz 1 TKG haben die Polizeivollzugsbehörden des Bundes und der Länder für Zwecke der Gefahrenabwehr Anspruch auf Erteilung von Aus-

---

253 Vgl. *Bock*, in: BeckTKG-Komm, § 88 TKG, Rn. 26; *Trute*, in: Trute/Spoerr/Bosch, § 85 TKG, Rn. 17. § 88 Abs. 3, Satz 1 TKG bezieht sich allein auf ein aktives Tun zur Verschaffung von Informationen, die dem Fernmeldegeheimnis unterfallen und enthält nicht etwa ein Verbot des Vorhandenseins solcher technischer Vorrichtungen, wogegen schon etwaige Verpflichtungen aus § 110 TKG sprechen, sondern allein das Verbot ihres Einsatzes.

254 § 88 Abs. 3, Satz 1 und 2 TKG. Siehe *Bock*, in: BeckTKG-Komm, § 88 TKG, Rn. 28.

255 Vgl. zur Auskunft und Überwachung nach dem TKG 1996 *Wuermeling/Felixberger*, CR 1997, 555 ff.

256 Nach BVerwG NJW 2004, 1191 ff. betrifft die Pflicht der Anbieter von Telekommunikationsdiensten, im öffentlichen Strafverfolgungs- und Sicherheitsinteresse Kundendateien zu führen und in diese bestimmte, dem automatisierten Abruf durch die Regulierungsbehörde für Telekommunikation und Post unterliegende Daten aufzunehmen nur diejenigen Kundendaten, die sie zuvor nach Maßgabe des für die Vertragsabwicklung Erforderlichen in zulässiger Weise erhoben haben. Die Anbieter sind darüber hinaus nicht zur Erhebung der einschlägigen Daten bei den Kunden verpflichtet. Diese Rechtsprechung dürfte durch die Regelung in § 111 Abs. 1, Satz 3, 2. Halbsatz TKG zumindest teilweise überholt sein.

künften aus den Kundendateien derjenigen, die Telekommunikationsdienste für die Öffentlichkeit erbringen.[257] Der Anspruch richtet sich gegen die Bundesnetzagentur[258] und umfasst gemäß § 111 Abs. 1 TKG Auskunft über die Rufnummern, Name und Anschrift des Rufnummerninhabers, das Datum des Vertragsbeginns, bei natürlichen Personen deren Geburtsdatum sowie bei Festnetzanschlüssen auch die Anschrift des Anschlusses.

bb) Die Auskunft nach § 113 Abs. 1 TKG

§ 113 Abs. 1, Satz 1 TKG gibt den zuständigen Stellen einen Anspruch gegen diejenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, auf Übermittlung der nach § 95 und § 111 TKG erhobenen Daten, soweit dies für die Verfolgung von Straftaten und Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtensdienstes, des Militärischen Abschirmdienstes sowie des Zollkriminalamtes erforderlich ist.

Auskunft kann auch über solche Daten verlangt werden, mittels derer der Zugriff auf andere Daten, die dem Fernmeldegeheimnis unterliegen, möglich ist.[259] Für den dann erfolgenden tatsächlichen Zugriff auf durch das Fernmeldegeheimnis geschützte Daten, ist jedoch eine einschlägige Ermächtigungsgrundlage erforderlich.[260]

cc) Die Auskunft gemäß den gesetzlichen Vorschriften im Sinne des § 88 Abs. 3, Satz 3 TKG[261]

Können die Polizeibehörden Auskunft von der Bundesnetzagentur und den Dienstanbietern über Bestandsdaten verlangen, so nützt ihnen dies für die angestrebte Telekommunikations-

---

257 Nach § 90 Abs. 3 Nr. 2 und Abs. 4 TKG 1996 waren geschäftsmäßige Telekommunikationsdiensteanbieter verpflichtet. Die sachgerechte Begrenzung in § 112 TKG entspricht der bisherigen Praxis, vgl. BT-Drucks. 15/2316, S. 95.

258 Siehe zur Bundesnetzagentur § 116 TKG.

259 Z. B. PIN, PUK, Passwort, vgl. BT-Drucks. 15/2316, S. 97.

260 Vgl. BT-Drucks. 15/2316, S. 97.

261 Die Vorschrift des § 88 Abs. 3, Satz 3 TKG ist nicht als Eingriffsermächtigung für Dritte ausgestaltet, sondern als Erlaubnistatbestand für die nach § 88 Abs. 2 TKG Verpflichteten, vgl. *Zerres*, in: Scheurle/Mayen (Hrsg.), § 85 TKG, Rn. 39. Die Erlaubnis bezieht sich nur auf die nach § 88 Abs. 3, Satz 1 TKG zulässigerweise erlangten Kenntnisse, da sie den Dienstanbietern keine weitergehenden Befugnisse zu Eingriffen in das Fernmeldegeheimnis gewährt. Es dürfen daher nur Kenntnisse weitergegeben werden, die zur Erbringung des Telekommunikationsdienstes einschließlich des Schutzes der technischen Systeme erforderlich waren; eine darüber hinausgehende Inhaltsüberwachung der Diensteanbieter wird durch § 88 Abs. 3, Satz 3 TKG nicht gestattet, vgl. *Tinnefeld/Schuster*, DuD 2005, 78 (80 f.).

überwachung nicht viel. Soll offen gelegt werden, mit wem vom überwachten Anschluss aus kommuniziert wurde, muss die Kennung des Anschlusses des Kommunikationspartners in Erfahrung gebracht werden. Diese Kennung ist ein Verbindungs-/Verkehrsdatum. Erst wenn dieses bekannt ist, können die dahinter stehenden Bestandsdaten erfragt werden. Gleiches gilt für die E-Mail-Kommunikation. Beim Zugang über den Access-Provider vergibt dieser für jede Einwahl ins Internet eine IP-Adresse.[262]

Ruft der Internetnutzer eine Webseite auf, werden Datenpakete (Header) übermittelt, die auch die IP-Adresse enthalten.[263] Ist die IP-Adresse bekannt, kann durch eine WHOIS-Abfrage[264] der Internet Provider ermittelt werden und von diesem dann Auskunft über den hinter der Adresse stehenden Kunden verlangt werden.

Der Zugriff auf die Verbindungsdaten wie die Anschlusskennung oder die dynamische IP-Adresse eröffnet sich den Polizeibehörden über gesetzliche Vorschriften im Sinne des § 88 Abs. 3, Satz 3 TKG. Diese Verbindungsdaten können dann herausverlangt werden, wenn eine gesetzliche Ermächtigungsgrundlage vorhanden ist, die den Anforderungen des § 88 Abs. 3, Satz 3 TKG entspricht.[265]

---

262 Diese Adressen sind international standardisiert. Eine IP-Adresse ist eine aus vier Ziffernblöcken bestehende Nummer, die sich aus Zahlen zwischen 0 und 255 zusammensetzt, vgl. *Gnirck/Lichtenberg*, DuD 2003, 598. Die Vergabe von IP-Adressen bzw. –Netzen wird von der Internet Assigned Numbers Authority (IANA) vergeben und seit Februar 2005 an fünf regionale Vergabestellen weitergegeben. Das Réseaux IP Européens Network Coordination Centre (RIPE NCC) ist für Europa, den Mittleren Osten und Zentralasien zuständig. Die regionalen Vergabestellen vergeben die ihnen zugeteilten Netze an lokale Vergabestellen. Dies sind in der Regel die Internet Service Provider, die die Adressen an ihre Kunden weitergeben. Die jeweiligen Adressen können dann entweder permanent oder dynamisch zugewiesen werden. Die dynamische IP-Adresse wird dem Kunden für die Dauer der Internetnutzung (Session) vergeben und danach einem anderen Kunden zugewiesen, vgl. *Gnirck/Lichtenberg*, DuD 2003, 598 (599).

263 Zum sog. „Header" vgl. *Spiegel*, DuD 2003, 265 (266). Einem E-Mail-Header können neben weiteren Informationen die vollständige IP-Adresse des Absenders sowie Uhrzeit und Datum des Versands entnommen werden. So kann an den Zugangsanbieter herangetreten und die Herausgabe der Personalien des Kunden gefordert werden, der zu diesem Zeitpunkt die IP-Adresse zugeteilt bekommen hatte, siehe dazu *Gehde*, DuD 2003, 496 (500).

264 Über den WHOIS-Dienst sind zu jedem registrierten Domainnamen bestimmte Informationen wie Identität des Registrars und Name und Anschrift abrufbar, vgl. zum WHOIS-Dienst und den geplanten Neuerungen *Roessler*, DuD 2002, 666 ff. und DuD 2003, 239.

265 Vgl. *Zerres*, in: Scheurle/Mayen (Hrsg.), § 85 TKG, Rn. 39; aA *Trute*, in: Trute/Spoerr/Bosch, § 85 TKG, Rn. 20, nach dessen Ansicht die Gesetzesbegründung in BT-Drucks. 13/3609, S. 53 dafür spricht, dass die Vorschrift des § 85 Abs. 2, Satz 3 TKG sowohl für die Überwindung des Fernmeldegeheimnisses wie auch für die bloße Zweckänderung gelten sollte, da in Bezug auf den letzten Halbsatz ausgeführt wird, dass die Befugnisnorm für den Eingriff so gestaltet sein müsse, dass der Wille des Gesetzgebers, das Fernmeldegeheimnis zurücktreten zu lassen, deutlich werde. Nach *Eckhardt*, DuD 2002, 197 (199) tritt dieser Konflikt im Rahmen des § 100 g StPO auf, da dieser für sein Auskunftsverlangen auch die Speicherung und Erhebung von Daten vorsehe, die nach dem TKG nicht erhoben und gespeichert werden dürfen; aA *Nack*, in: KK, § 100 g StPO Rn. 6 und *Meyer-Goßner*, § 100 g Rn. 10 unter Hinweis auf BT-

Voraussetzung ist, dass sich das die Weitergabe und Verwendung der Kenntnisse vorsehende Gesetz ausdrücklich auf Telekommunikationsvorgänge bezieht. Dieses so genannte „kleine Zitiergebot“[266] soll sicherstellen, dass der Gesetzgeber eine bewusste Abwägung von Fernmeldegeheimnis und Auskunfts- oder Weiterverwendungsinteresse vorgenommen hat. Die im Konfliktfall erforderliche Abwägung zwischen dem Fernmeldegeheimnis und dem durch die Weitergabe der Kenntnisse verfolgten Interesse darf nicht dem einzelnen Rechtsanwender überlassen werden.[267] Eine wörtliche Erwähnung oder ein Zitat des § 88 TKG ist dafür jedoch nicht erforderlich.[268]

b) Die Überwachung[269]

§ 110 TKG und die dazu erlassene Telekommunikationsüberwachungsverordnung (TKÜV)[270] regeln im Wesentlichen die technische Gestaltung der Überwachungseinrichtungen, nicht aber deren Zulässigkeit.[271] Die Zulässigkeit bestimmt sich vielmehr – insoweit die Regelungstechnik des § 88 Abs. 3, Satz 3 TKG aufnehmend – nach anderen gesetzlichen

---

Drucks. 14/7258, S. 4, wonach der Auskunftsanspruch auf solche Daten beschränkt ist, die seitens der Dienstanbieter aufgrund bestehender Regelungen zulässigerweise erhoben und gespeichert werden. Von der Ermöglichung der Anordnung einer Verpflichtung, auch sonstige Verbindungsdaten aufzuzeichnen, sei entgegen im Gesetzgebungsverfahren mehrfach geäußerten Wünschen abgesehen worden, weil die Diensteanbieter hinsichtlich solcher Daten, die sie nach dem Telekommunikationsrecht nicht erheben und speichern dürfen, lediglich zur Ermöglichung der Überwachung und Aufzeichnung unter den Voraussetzungen der §§ 100 a und 100 b StPO verpflichtet bleiben sollten. Zumindest für das ThPAG ist dies ohne Belang, da nach der Gesetzesbegründung Auskunftsansprüche nur über Daten vorgesehen sind, die nach dem TKG erhoben und gespeichert werden dürfen, vgl. LT-Drucks. Th. 3/2128, S. 25. Dies sieht auch LT-Drucks. Nds. 15/240, S. 17 vor; durch den Verweis auf § 100 g StPO dürfte sich der gesetzgeberische Wille nicht geändert haben. LT-Drucks. Bayern 15/2096, S. 60 stellt zusätzlich zum eindeutigen Wortlaut klar, dass Gegenstand der Übermittlung vorhanden Verkehrsdaten (§ 34 b Abs. 2 Nr. 1 PAG) und Kennungen (§ 34 b Abs. 2 Nr. 3 PAG) sind, soweit sie bei den Diensteanbietern vorliegen. Nach der Gesetzessystematik muss dies auch für die zukünftigen Daten nach § 34 b Abs. 2 Nr. 2 PAG gelten. Auch in der Gesetzesbegründung zum HSOG ist festgehalten, dass die Vorschriften die Unternehmen nicht zur Speicherung verpflichten, sondern der Polizei lediglich den Zugriff auf Daten ermöglichen, soweit und solange diese gespeichert sind, vgl. LT-Drucks. Hessen 16/2352, S. 19. Aus der rheinland-pfälzischen Gesetzesbegründung ergibt sich ebenfalls nicht Gegenteiliges, vgl. LT-Drucks. RhPf. 14/2287, S. 47 ff.

266 *Holznagel/Enaux/Nienhaus*, 2006, Rn. 647; *Zerres*, in: Scheurle/Mayen (Hrsg.), § 85 TKG, Rn. 40.

267 Vgl. *Zerres*, in: Scheurle/Mayen (Hrsg.), § 85 TKG, Rn. 40.

268 Vgl. *Zerres*, in: Scheurle/Mayen (Hrsg.), § 85 TKG, Rn. 40; aA wohl *Bock*, in: BeckTKG-Komm § 88 TKG, Rn. 28.

269 Zu den neuern Entwicklungen der Telekommunikationsüberwachung vgl. *Eckhardt*, CR 2002, 770 ff. Zur neuen TKÜV vgl. *Meister/Laun*, in: Wissmann (Hrsg.), Kapitel 14, Rn. 93.

270 Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation**,** BGBl. I, 2005, S. 3136.

271 Vgl. *Bock*, in: BeckTKG-Komm, § 110 TKG, Rn. 4; *Meister/Laun*, in: Wissmann (Hrsg.), Kapitel 14, Rn. 84 f.; *Trute*, in: Trute/Spoerr/Bosch, § 88 TKG, Rn. 4. *R.P. Schenke*, MMR 2002, 8 nimmt die TKÜV zum Anlass, das komplizierte Zusammenspiel zwischen förmlichem Gesetz und Rechtsverordnung nachzuzeichnen und einer verfassungsrechtlichen Überprüfung zu unterziehen.

Vorschriften.[272] Nur wenn die in diesen Normen vorgesehenen Voraussetzungen vorliegen, darf den berechtigten Stellen die Überwachung und Aufzeichnung ermöglicht werden.[273]

aa) Die Adressaten der Überwachungsanordnung

Wer eine Telekommunikationsanlage[274] betreibt, mit der Telekommunikationsdienste[275] für die Öffentlichkeit erbracht werden, hat gemäß § 110 Abs. 1, Satz 1 Nr. 1 TKG auf eigene Kosten technische Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation vorzuhalten und organisatorische Vorkehrungen für deren unverzügliche Umsetzung zu treffen. Wer Telekommunikationsdienste für die Öffentlichkeit erbringt ohne hierfür eine Telekommunikationsanlage zu betreiben, hat sich bei Auswahl des Betreibers der dafür genutzten Telekommunikationsanlage zu vergewissern, dass dieser Anordnungen zur Überwachung der Telekommunikation unverzüglich umsetzen kann.[276]

Darüber hinaus ist jeder Betreiber einer Telekommunikationsanlage, der im Rahmen seines Angebotes für die Öffentlichkeit Netzabschlusspunkte[277] überlässt, verpflichtet, den gesetzlich zur Überwachung der Telekommunikation berechtigten Stellen auf deren Anforderung Netzabschlusspunkte für die Übertragung der im Rahmen einer Überwachungsmaßnahme anfallenden Informationen bereitzustellen.[278] Dadurch soll sicher gestellt werden, dass die im Rahmen der Telekommunikationsüberwachung anfallenden Informationen unverzüglich an

---

272 Vgl. *Trute*, in: Trute/Spoerr/Bosch, § 88 TKG, Rn. 4.

273 Vgl. *Bock*, in: BeckTKG-Komm, § 110 TKG, Rn. 4.

274 Vgl. die Legaldefinition in § 3 Nr. 23 TKG.

275 Vgl. die Legaldefinition in § 3 Nr. 24 TKG.

276 § 110 Abs. 1, Satz 2 TKG. Durch § 110 Abs. 1, Satz 6 TKG wird klargestellt, dass die Vorschriften der landesgesetzlichen Regelungen zur präventiv-polizeilichen Telekommunikationsüberwachung nicht durch die Vorschrift des § 110 TKG eingeschränkt werden, vgl. BT-Drucks. 15/2316, S. 93. Gleiches gilt für die Ausnahmen nach der TKÜV, vgl. § 3 Abs. 2, Satz 3 TKÜV. Soweit die geschäftsmäßigen Diensteanbieter nicht zugleich Betreiber von Telekommunikationsanlagen sind, mit denen Telekommunikationsdienste für die Öffentlichkeit erbracht werden, trifft sie zwar keine Pflicht technische Maßnahmen vorzuhalten und Vorkehrungen für die Umsetzung der Überwachungsmaßnahmen zu treffen, zur Überwachungs- und Aufzeichnungsermöglichung sind sie aber dennoch verpflichtet, siehe *Bock*, in: BeckTKG-Komm, § 110 TKG, Rn. 11. Zu den weiteren Ausnahmen siehe *Meister/Laun*,in: Wissmann (Hrsg.), Kapitel 14, Rn. 95 ff.

277 Der Begriff des „Netzabschlusspunktes“ wurde unter Anpassung an den Sprachgebrauch des TKG übernommen. Mit „Netzabschlusspunkt“ ist ein Netzanschluss bzw. -zugang gemeint, vgl. BT-Drucks. 15/2316, S. 94.

278 § 110 Abs. 6, Satz 1 TKG.

die überwachende Behörde übermittelt werden,[279] da der überwachende Betreiber nicht immer über Übertragungsmöglichkeiten zur jeweiligen Überwachungsbehörde verfügt.[280]

bb) Die technische Umsetzung der Überwachung

Die technische und organisatorische Umsetzung der Überwachungsmaßnahmen erfolgt durch die Telekommunikationsüberwachungsverordnung (TKÜV).[281] Die TKÜV enthält u.a. Regelungen über den Kreis der Verpflichteten[282], den Umfang der bereitzustellenden Kommunikation und die technische Umsetzung der Anordnung. Die technischen Einzelheiten werden gemäß § 11 TKÜV in einer Technischen Richtlinie[283] festgelegt.

Der nach § 3 Abs. 1 TKÜV Verpflichtete hat der berechtigten Stelle am Übergabepunkt[284] eine vollständige Kopie der Telekommunikation bereitzustellen, die über seine Telekommunikationsanlage unter der zu überwachenden Kennung[285] abgewickelt wird.[286] Die Polizei richtet die Abhörstelle ein und stellt die erforderlichen Geräte bereit, sofern diese nicht zur

---

279 Vgl. *Bock*, in: BeckTKG-Komm, § 110 TKG, Rn.103.

280 Vgl. *Bock*, in: BeckTKG-Komm, § 110 TKG, Rn. 103.

281 Zur neuen TKÜV vgl. *Meister/Laun*, in: Wissmann (Hrsg.), Kapitel 14, Rn. 93. Durch das TKG 1996 war eine Anpassung der bisherigen Vorschriften zur technischen und organisatorischen Umsetzung der Überwachungsmaßnahmen erforderlich geworden. Bis zu diesem Zeitpunkt waren diese Vorschriften in der Fernmeldeverkehr-Überwachungsverordnung (FÜV) vom 18.05.1995, BGBl. I, S. 722, geändert durch Art. 4 des Gesetzes vom 26.06.2001, BGBl. I, S. 1254, enthalten. Die Ermächtigungsgrundlage für die FÜV in § 10 b, Satz 2 FAG wurde durch § 99 Abs. 1 Nr. 3 TKG 1996 ersatzlos gestrichen und durch eine Ermächtigungsgrundlage für die Telekommunikationsüberwachungsverordnung (TKÜV) in § 88 Abs. 2 TKG 1996 ersetzt. Mit dem Inkrafttreten der TKÜV vom 22.01.2002, BGBl. I, S. 458 ist die FÜV außer Kraft getreten (§ 31 TKÜV a.F.). Durch die Neufassung des TKG im Jahr 2004 war auch eine Anpassung der TKÜV erforderlich. Die Änderung der TKÜV erfolgte in Form einer Ablöseverordnung, vgl. BR-Drucks. 631/05, S. 2.

282 Vgl. § 3 Abs. 1 TKÜV. Die in § 3 Abs. 2 TKÜV genannten Unternehmen sind zwar von der Verpflichtung befreit, technische Einrichtungen zur Umsetzung von Überwachungsmaßnahmen vorzuhalten und vorbereitende Maßnahmen dazu zu treffen. Aufgrund der Vorschriften der StPO, des G-10-Gesetzes, des ZFdG und der Vorschriften des Landesrechts bleiben sie aber verpflichtet, im Bedarfsfall die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen, § 3 Abs. 2, Satz 3 TKÜV.

283 Technische Richtlinie zur Beschreibung der Anforderungen an die Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Ausgabe 5.0, Dezember 2006, bearbeitet und herausgegeben von der Regulierungsbehörde für Post- und Telekommunikation, www.bundesnetzagentur.de/media/archive/8255.pdf.

284 Der Übergabepunkt ist der Punkt der technischen Einrichtung des Verpflichteten, an dem er die Überwachungskopie bereitstellt; der Übergabepunkt kann als systeminterner Übergabepunkt gestaltet sein, der am Ort der Telekommunikationsanlage nicht physisch dargestellt ist, § 2 Nr. 11 TKÜV. Der Übergabepunkt muss den Vorgaben der Technischen Richtlinie entsprechen und ist nach Maßgabe des § 8 Abs. 2 TKÜV zu gestalten.

285 Die zu überwachende Kennung ist definiert in § 2 Nr. 17 TKÜV. Was alles unter den Begriff der Kennung fällt, ergibt sich genauer aus der Technischen Richtlinie unter 7.2.6.

286 § 5 Abs. 2 TKÜV.

Verfügung stehen.[287] Die zu überwachende Telekommunikation umfasst den Inhalt und die Daten über die näheren Umstände der Telekommunikation.[288]

Bei den bereitzustellenden Daten[289] handelt es sich nicht nur um Verkehrsdaten, die schon Gegenstand eines Auskunftsverlangens nach § 88 Abs. 3, Satz 3 TKG sein können, sondern auch um sonstige Daten, die von den Diensteanbietern nicht erhoben oder gespeichert werden dürfen.[290]

Der Verpflichtete muss die Überwachung für mehrere Bedarfsträger gleichzeitig realisieren können[291]. Diese Verpflichtung beruht auf dem Trennungsgebot zwischen Polizei und Verfassungsschutzbehörden und soll sicherstellen, dass verschiedene Behörden unabhängig voneinander und unter Umständen auch in sich überschneidenden Überwachungszeiträumen die Telekommunikation ein und derselben Person überwachen können.[292] Daneben muss der verpflichtete Betreiber Engpässe, die bei gleichzeitiger Durchführung mehrerer Überwachungsmaßnahmen auftreten, unverzüglich beseitigen.[293]

IV. Die polizeigesetzlichen Regelungen als „andere gesetzliche Vorschriften" im Sinne von § 88 Abs. 3, Satz 3 TKG

Die Polizeibehörden in Thüringen, Niedersachsen, Bayern, Rheinland-Pfalz und Hessen können eine Auskunfterteilung über Verkehrs-, Inhalts- und Standortdaten sowie eine Überwachungsermöglichung von den Telekommunikationsanbietern dann verlangen, wenn die in ihren Polizeigesetzen enthaltenen Ermächtigungsnormen gesetzliche Vorschriften im Sinne des § 88 Abs. 3, Satz 3 TKG sind. Dafür müssen die landesgesetzlichen Regelungen der § 34 a ThPAG, § 33 a – c Nds.SOG, Art. 34 a – c PAG, § 31 POG und § 15 a HSOG die Verwendung und Weitergabe des Inhalts und der näheren Umstände der Telekommunikation an ihre

---

287 Vgl. *Meyer-Goßner*, § 100 b StPO, Rn. 5. Die Bereitstellung durch die Polizei ist von Nöten, wenn die Betreiber nach § 110 Abs. 2 Nr. 2 c TKG; § 3 Abs. 2 TKÜV von ihrer Vorhaltepflicht befreit sind.

288 § 5 Abs. 1 TKÜV.

289 Diese sind in § 7 TKÜV aufgeführt.

290 § 7 Abs. 1 Nr. 7 TKÜV nennt dabei den Standort eines Mobiltelefons. Der Standort des Mobiltelefons wird bei der Entgeltberechnung nicht ausschlaggebend sein und ist deswegen zu löschen, so dass eine Auskunft nach § 88 Abs. 3, Satz 3 TKG nicht zu erlangen ist. Durch die Überwachungsanordnung kann aber auf solche Daten zugegriffen werden; so auch *Meyer-Goßner*, § 100 g StPO Rn. 5 für die Telekommunikationsüberwachung nach den §§ 100 a ff. StPO.

291 § 6 Abs. 4 TKÜV.

292 Vgl. *I.M. Pernice*, DuD 2002, 207 (209).

293 § 5 Abs. 6 TKÜV.

Polizeibehörden vorsehen und sich dabei ausdrücklich auf Telekommunikationsvorgänge beziehen.

Zunächst ist jedoch zu klären, ob ein Landesgesetz überhaupt „gesetzliche Vorschrift“ im Sinne des § 88 Abs. 3, Satz 3 TKG sein kann, da solche Gesetze bis zur Einführung der landesgesetzlich geregelten präventiven Telekommunikationsüberwachung in den Polizeigesetzen der Länder Thüringen, Niedersachsen, Bayern, Rheinland-Pfalz und Hessen ausschließlich Bundesgesetze waren.[294] Weiter ist zu prüfen, ob die jeweiligen landesgesetzlichen Normen auf Telekommunikationsvorgänge Bezug nehmen. Zuletzt ist auf die Besonderheit des ThPAG einzugehen, welches die Weitergabe der Telekommunikationsdaten an seine Polizeibehörden nicht direkt regelt.

1. Die Regelung durch Landesgesetz

Zwar verzichtet Art. 10 Abs. 2, Satz 1 GG - anders als Art. 117 WRV[295] - darauf, die einschränkenden Gesetze dem Bundesgesetzgeber vorzubehalten und so folgt aus der Formulierung „aufgrund eines Gesetzes“, dass auch der Landesgesetzgeber einschränkende Gesetze erlassen darf.[296] Ausgehend von der ausschließlichen Gesetzgebungskompetenz des Bundes nach Art. 73 Nr. 7 GG über das Postwesen und die Telekommunikation, ist eine Regelung durch Landesgesetz jedoch kritisch betrachtet worden.[297]

Die Landesgesetzgeber haben sich nahezu einvernehmlich auf den Standpunkt gestellt, dass dem Bund lediglich die Gesetzgebungskompetenz zur Regelung der technischen Seite der Telekommunikation zukommt. Durch die Schaffung einer polizeilichen Eingriffskompetenz in die Telekommunikationsfreiheit für den präventiven Bereich würde dagegen in erster Linie materielles Polizeirecht geregelt. Der Schwerpunkt dieser Regelungen liege im Gefahrenabwehrbereich, weshalb die Landesgesetzgebungskompetenz gegeben sei.[298] Tatsächlich

---

294 Siehe dazu auch § 1 Abs. 1 Nr. 1 TKÜV in der Fassung vom 22 01.2002, BGBl. I, S. 458.

295 Art. 117 der Weimarer Reichsverfassung vom 11.08.1919 lautet: „Das Briefgeheimnis sowie das Post-, Telegraphen- und Fernsprechgeheimnis sind unverletzlich. Ausnahmen können nur durch Reichsgesetz zugelassen werden.“

296 Vgl. *Loewer*, in: v.Münch/Kunig (Hrsg.), Art. 10 GG, Rn. 29.

297 Gegen eine Landesgesetzgebungskompetenz spricht sich *Kutscha*, LKV 2003, 114 (116) aus. Siehe dazu auch *Schenke*, AöR 125 (2000), 1 (7 ff.), der ausführlich eine mögliche Bundesgesetzgebungskompetenz erörtert, im Ergebnis aber eine Gesetzgebungskompetenz der Länder bejaht.

298 Vgl. LT-Drucks. Th. 3/2128, S. 34; LT-Drucks. Nds. 15/240, S. 15; LT-Drucks. RhPf. 14/2287, S. 47; LT-Drucks. Hessen 16/2352, S. 18, 19. In Bayern wird die Frage der Gesetzgebungskompetenz unter dem

geht auch der Bundesgesetzgeber wie selbstverständlich davon aus, dass eine Gesetzgebungskompetenz für die Länder gegeben ist.[299]

Auch das BVerfG geht in seinem Urteil zur präventiven Telekommunikationsüberwachung nach dem Nds.SOG 2005 ebenfalls von einer grundsätzlichen Gesetzgebungskompetenz der Länder aus.[300] Es führt an, dass die Verhütung einer Straftat in der Gesetzgebungskompetenz der Länder zur Gefahrenabwehr liege und zwar auch dann, wenn sie vorbeugend für den Zeitraum vor dem Beginn einer konkreten Straftat vorgesehen werde. Wie weit der Gesetzgeber eine derartige Maßnahme in das Vorfeld künftiger Rechtsgutsverletzungen legen darf, sei eine Frage des materiellen Rechts, berühre aber nicht die Gesetzgebungskompetenz des Landes.[301] Seiner Ansicht nach besteht bei der Telekommunikationsüberwachung zur Verhinderungsvorsorge[302] keine konkurrierende Gesetzgebung des Bundes nach Art. 74 Abs. 1 Nr. 1 GG, da das Tatbestandsmerkmal der Verhütung von Straftaten Maßnahmen erfasse, die drohende Rechtsgutverletzungen von vornherein und in einem Stadium verhindern sollen, in dem es noch nicht zu strafwürdigem Unrecht gekommen ist.[303]

Was jedoch die Telekommunikationsüberwachung zur Vorsorge für die Verfolgung von Straftaten (Verfolgungsvorsorge)[304] betrifft, soll dafür eine Gesetzgebungskompetenz der Länder nicht gegeben sein.[305] Die Vorsorge für die Verfolgung noch nicht begangener Straftaten gehört nach Ansicht des BVerfG zum gerichtlichen Verfahren. Von der in Art. 74 Abs. 1 Nr. 1 GG normierten konkurrierenden Gesetzgebung zur Strafverfolgung habe der Bundes-

---

Aspekt thematisiert, ob den Diensteanbietern im Rahmen der Telekommunikationsüberwachung durch Landesgesetz Verpflichtungen auferlegt werden können. Dabei wird auf § 110 Abs. 1, Satz 6 TKG verwiesen, der klarstellt, dass landesgesetzliche Regelungen zur präventiv-polizeilichen Telekommunikationsüberwachung nicht durch die Vorschrift des § 110 TKG eingeschränkt werden, vgl. LT-Drucks. Bayern 15/2096, S. 59.

299 Siehe nur § 110 Abs. 1, Satz 6 TKG und § 1 Nr. 1 d) TKÜV.

300 Vgl. BVerfGE 113, 349 (367 ff.).

301 Vgl. BVerfGE 113, 349 (368 ff.).

302 Die Verhinderungsvorsorge ist Tatbestand einer vorbeugenden Bekämpfung von Straftaten und Ordnungswidrigkeiten und damit Maßnahme der Gefahrenabwehr. Sie dient der Verhütung künftiger Straftaten, vgl. *Würtenberger/Heckmann*, 2005, Rn. 179.

303 Derartige Maßnahmen seien allenfalls insoweit der Bundeskompetenz zuzuordnen, als sie zu einem von ihr erfassten Sachbereich in einem notwendigen Zusammenhang stehen, insbesondere für den wirksamen Vollzug der Bundesregelung erforderlich sind, vgl. BVerfGE 113, 349 (369).

304 Die allgemeine Verfolgungsvorsorge dient dazu, bei künftigen strafprozessualen Ermittlungen die Aufklärung des Sachverhalts zu unterstützen, vgl. *Würtenberger/Heckmann*, 2005, Rn. 181.

305 Dieser Ansicht folgt auch der bayerische Gesetzgeber, vgl. LT-Drucks. Bayern 15/4097, S. 3. Zustimmend auch *Puschke/Singelnstein*, NJW 2005, 3534 (3535), die jedoch auch Schwierigkeiten bei der praktischen Umsetzung sehen, da eine deutliche Abgrenzung zwischen Verfolgungsvorsorge einerseits und Verhütungsvorsorge andererseits nur schwer möglich sei bzw. sich die Bereiche in weiten Teilen überschneiden dürften. Siehe dazu auch *W.-R. Schenke*, in: FG für Hilger, S. 226 ff.

gesetzgeber im Bereich der Telekommunikationsüberwachung abschließend Gebrauch gemacht, so dass die Länder gemäß Art. 72 Abs. 1 GG von der Gesetzgebung ausgeschlossen seien.[306]

Zur Begründung führt das BVerfG an, dass die Regelung zur Verfolgungsvorsorge die Sicherung von Beweisen für ein künftiges Strafverfahren bezwecke. Die Verfolgungsvorsorge erfolge in zeitlicher Hinsicht präventiv, betreffe aber gegenständlich das repressiv ausgerichtete Strafverfahren. Die Daten würden zu dem Zweck der Verfolgung einer in der Zukunft möglicherweise verwirklichten konkreten Straftat und damit letztlich nur zur Verwertung in einem künftigen Strafverfahren, also zur Strafverfolgung erhoben. Es gehe um die Beweisbeschaffung zur Verwendung in künftigen Strafverfahren, nicht um eine präventive Datenerhebung zur Verhütung von Straftaten.[307]

Dass der Bundesgesetzgeber von seiner Kompetenz abschließend Gebrauch gemacht hat, schließt das BVerfG daraus, dass die bestehenden Vorschriften der StPO eine konzeptionelle Entscheidung gegen zusätzliche, in das erweiterte Vorfeld einer Straftat verlagerte Maßnahmen erkennen lassen würden. Der Bundesgesetzgeber habe die Überwachung der Telekommunikation zu Zwecken der Strafverfolgung abschließend in den §§ 100 a ff. StPO nach Umfang, Zuständigkeit und Zweck sowie hinsichtlich der für die jeweilige Maßnahme erforderlichen Voraussetzungen umfassend geregelt. Der Bundesgesetzgeber sei sich – wie die §§ 81 b und 81 g StPO zeigen – durchaus der kompetenzrechtlichen Möglichkeit bewusst gewesen, im Bereich der Strafverfolgung auch präventive Regelungen zu treffen.[308]

Der Gesetzgeber habe die tatbestandlichen Voraussetzungen der Telekommunikationsüberwachung im Interesse rechtsstaatlicher Bestimmtheit und Verhältnismäßigkeit und unter der Berücksichtigung der Vorgaben der verfassungsgerichtlichen Rechtsprechung möglichst genau zu regeln versucht und an den Verdacht von Straftaten oder ihre Vorbereitung angeknüpft. Diese gezielten Eingrenzungen könnten hinfällig werden, wenn die Länder vergleichbare Maßnahmen zur Telekommunikationsüberwachung ebenfalls mit dem Ziel der Sicherung späterer Strafverfolgung unter anderen, etwa geringeren, Voraussetzungen normieren könnten. Damit entstünde das Risiko widersprüchlicher Regelungen oder von Über-

306 Vgl. BVerfGE 113, 349 (369 f.).
307 Vgl. BVerfGE 113, 349 (370 f.).
308 Vgl. BVerfGE 113, 349 (373).

schneidungen unterschiedlicher Normen.[309] Nach § 33 a Abs. 1 Nr. 2 und 3 Nds.SOG 2005 würden Vorfeldmaßnahmen möglich, die nach der Strafprozessordnung gerade ausgeschlossen sein sollten. Für das BVerfG ist nicht erkennbar, dass der Bundesgesetzgeber einen solchen Widerspruch hätte in Kauf nehmen wollen.[310]

Auch § 484 Abs. 4 StPO steht der Annahme einer abschließenden bundesgesetzlichen Regelung nach Ansicht des BVerfG nicht entgegen. Nach dieser Norm richtet sich die Verwendung personenbezogener Daten, die für Zwecke künftiger Strafverfahren in Dateien der Polizei gespeichert sind oder werden, nach den Polizeigesetzen. Anhaltspunkte dafür, dass der Bundesgesetzgeber damit die präventive Datenerhebung zum Zwecke späterer Strafverfolgung durch die Polizeibehörden voraussetzen und von seiner Kompetenz zur Regelung dieses Bereichs gerade nicht abschließend Gebrauch machen wollte, würden weder die Gesetzesbegründung zu § 484 Abs. 4 StPO noch der Sinn dieser Regelung bieten.[311]

Entgegen der Auffassung des BVerfG ist die Gesetzgebungskompetenz der Länder nicht nur für die Abwehr von Gefahren und die vorbeugende Bekämpfung von Straftaten in Form der Verhinderungsvorsorge, sondern auch für den Bereich der Verfolgungsvorsorge gegeben.[312]

Im Unterschied zur Verhinderungsvorsorge mag bei der Verfolgungsvorsorge ein stärkerer strafprozessualer Bezug gegeben sein; denn zukünftige Strafverfahren werden durch die vorbereitenden Maßnahmen erleichtert. Gleichwohl sind diese Maßnahmen dem präventiven und nicht dem repressiven Aufgabenfeld der Polizei zuzuordnen.[313] Denn tatsächlich dienen Datensammlungen im Bereich der Verhinderungsvorsorge regelmäßig auch der Verfolgungsvorsorge, so dass die Verfolgungsvorsorge lediglich ein strafverfahrensrechtlicher Nebeneffekt der polizeilichen Aufgabe ist, künftige Straftaten zu verhindern.[314] Verhinderungs-

---

309 Vgl. BVerfGE 113, 349 (373 f.).

310 Vgl. BVerfGE 113, 349 (375).

311 Vgl. BVerfGE 113, 349 (375). Siehe auch *W.-R. Schenke*, in: FG für Hilger, S. 231 f.

312 AA *W.-R. Schenke*, in: FG für Hilger, S. 229 ff., der wegen des engen Zusammenhanges mit der Strafverfolgung die hierauf gerichtete Strafverfolgungsvorsorge jedenfalls unter dem Aspekt der Annexkompetenz des gerichtlichen Verfahren im Sinn des Art. 74 Nr. 1 GG zuordnet.

313 Vgl. BVerwGE 26, 169 (170); BVerwG NJW 1990, 2768 (2769); VGH Mannheim NJW 1987, 3022; *Götz*, 2001, Rn. 86; 544; *Würtenberger/Heckmann*, 2005, Rn. 181; *Walden*, 1996, S. 156 ff.; *Mußmann*, 1994, Rn. 150 und 259; *Ahlf*, KritV 1988, 136 (146 ff.); *Kniesel*, ZRP 1987, 377 (380); *Kniesel/Vahle*, DÖV 1987, 953 (955 f.); aA BVerfGE 113, 349 (370 f.); *Zöller*, 2002, S. 89 ff. *Wolter*, GA 1999, 158 (176); *Denninger*, CR 1988, 51 (54).

314 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 182; *Walden*, 1996, S. 164 f.; *Behrendes*, Die Polizei 1988, 220 (225); *Honnacker*, CR 1986, 287 (290). Demgegenüber sieht die Gegenansicht die Vorsorge für die Ver-

und Verfolgungsvorsorge stehen nicht isoliert von einander, sondern sind Bestandteile der polizeilichen Aufgabe Straftaten vorbeugend zu bekämpfen.[315] So sieht auch § 1 Abs. 1, Satz 2 VEME PolG vor, dass die Polizei im Rahmen ihrer (Gefahrenabwehr-)Aufgabe für die Verfolgung von Straftaten vorzusorgen und Straftaten zu verhüten (vorbeugende Bekämpfung von Straftaten) sowie Vorbereitungen zu treffen hat, um künftige Gefahren abwehren zu können (Vorbereitung auf die Gefahrenabwehr).[316]

Dass in § 33 a Abs. 1 Nr. 2 Nds.SOG 2005 die Verfolgungsvorsorge als selbstständiges Eingriffsmerkmal normiert ist, lässt die Verbindung zur Gefahrenabwehr nicht entfallen. Dient die Verfolgungsvorsorge dazu, bei künftigen strafprozessualen Ermittlungen die Aufklärung eines Sachverhalts, insbesondere durch die Anfertigung, Aufbewahrung und systematische Zusammenstellung von Unterlagen und Datensammlungen zu beschleunigen und zu erleichtern[317], so findet diese noch zeitlich vor einem Ermittlungsverfahren, also im präventiven Bereich statt. Wie weit der Gesetzgeber Maßnahmen in das Vorfeld künftiger Gefahrenlagen verlegen darf, ist – wie das BVerfG richtig ausführt – eine Frage des materiellen Rechts und berührt nicht die Gesetzgebungskompetenz.[318] Dass die Datensammlungen darüber hinaus auch der Verhinderungsvorsorge dienen können und sollen, ergibt sich aus dem Gesetzentwurf zum Nds.SOG 2005 und dem schriftlichen Bericht des Landtagsausschusses für Inneres und Sport.

Der im Gesetzentwurf vorgesehene § 33 a Abs. 1 Nr. 2 Nds.SOG 2005[319] sollte die Polizei zur Telekommunikationsüberwachung gegenüber Personen ermächtigen, bei denen Tatsachen die Annahme rechtfertigen, dass sie künftig besonders schwerwiegende Straftaten begehen und die Datenerhebung zur vorbeugenden Bekämpfung dieser Straftaten erforderlich ist. In der Begründung wird dazu ausgeführt: „Nummer 2 trägt der Tatsache Rechnung, dass die Polizei ihre Aufgabe der Verhütung von Straftaten in bestimmten Kriminalitätsbereichen,

---

folgung künftiger Straftaten als eine unabdingbare Hilfsfunktion der Strafverfolgung und als strafprozessuale Aufgabe der Strafverfolgungsbehörden an, vgl. *Siebrecht*, JZ 1996, 711 (713 f.); *Denninger*, CR 1988, 51 (54); *Schoreit*, KritV 1988, 157 (171) und wohl auch *W.-R. Schenke*, JZ 2001, 997 (1002); *ders.*, 2005, Rn. 30.

315 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 179 ff.; *Walden*, 1996, S. 156 ff.; *Kniesel*, ZRP 1987, 377 (380); *Götz*, 2001, Rn. 86.

316 Vgl. Musterentwurf eines einheitlichen Polizeigesetzes des Bundes und Länder in der Fassung des Vorentwurfs zur Änderung des MEPolG, abgedruckt als Anhang bei *W.-R. Schenke*, 2007, S. 395 ff.

317 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 181; VGH Baden-Württemberg NJW 1987, 3022.

318 So BVerfGE 113, 349 (368 f.) zur Verhinderungsvorsorge.

319 Vgl. LT-Drucks. Nds. 15/240, S. 4.

in denen besonders schwerwiegende Straftaten begangen werden, nur noch dann effektiv erfüllen kann, wenn sich ihre Eingriffsbefugnisse an die Handlungs- und Organisationsformen anpassen, die sich gerade im Bereich der Organisierten Kriminalität (OK-Bereich) entwickelt haben. (...) Die Bekämpfung dieser Kriminalitätsformen erfordert daher die Eingriffsbefugnis der präventiven Telekommunikationsüberwachung, um Sachverhalte abzuklären, kriminelle Strukturen zu erhellen und dadurch letztlich auch Anhaltspunkte zur Begründung eines konkreten Anfangsverdachts einer Straftat zu ermitteln".[320]

Durch die Aufnahme der Verfolgungsvorsorge in die Vorschrift des § 33 a Nds.SOG 2005 sollte es zu keiner Änderung der gesetzgeberischen Intention kommen. Die Änderungen waren vielmehr redaktioneller Natur und dienten der sprachlichen Anpassung an die Regelung in § 34 Abs. 1, Satz 1 Nds.SOG 2005.[321] Im Gesetzentwurf lautete § 33 a Abs. 1 Nr. 2 Nds.SOG 2005: „... und die Datenerhebung zur vorbeugenden Bekämpfung von Straftaten erforderlich ist".[322] In der gesetzgewordenen Fassung heißt es in § 33 a Abs. 1 Nr. 2 Nds.SOG 2005: „... wenn die Vorsorge für die Verfolgung oder die Verhütung dieser Straftaten auf andere Weise nicht möglich erscheint". Daran zeigt sich, dass auch der niedersächsische Gesetzgeber davon ausgeht, dass Verhinderungs- und Verfolgungsvorsorge zur polizeilichen Aufgabe der vorbeugenden Bekämpfung von Straftaten zählen.

Selbst wenn man sich mit dem BVerfG auf den Standpunkt stellen wollte, dass die Verfolgungsvorsorge in den Bereich der konkurrierenden Gesetzgebung nach Art. 74 Abs. 1 Nr. 1 GG fällt, so hat der Bundesgesetzgeber durch die Vorschriften der §§ 100 a ff. StPO nicht abschließend von seiner Gesetzgebungskompetenz Gebrauch gemacht.[323] § 100 a StPO setzt einen Anfangsverdacht in Bezug auf eine bereits begangenen Straftat oder einen Straftatenversuch voraus. Bevor dieser nicht vorliegt, kann § 100 a StPO nicht zur Anwendung kommen.

Das BVerfG stützt sich darauf, dass sich der Gesetzgeber angesichts der Regelungen in §§ 81 b und 81 g StPO der kompetenzrechtlichen Möglichkeit bewusst war, im Bereich der Straf-

---

320 Vgl. LT-Drucks. Nds. 15/240, S. 18.
321 Vgl. schriftlicher Bericht des Landtagsausschusses für Inneres und Sport, LT-Drucks. 15/776, S. 6.
322 Vgl. LT-Drucks. Nds. 15/240, S. 4.
323 Siehe dazu *Würtenberger/Heckmann*, 2005, Rn. 590 (Fn. 148). So aber wohl *W.-R. Schenke*, 2007, Rn. 30.

verfolgung auch präventive Regelungen zu treffen.[324] Es übersieht aber, dass, soweit § 81 b StPO Maßnahmen für erkennungsdienstliche Zwecke gestattet, es sich um in die StPO als Fremdkörper aufgenommenes materielles Polizeirecht handelt.[325] Die Bundeskompetenz ergibt sich dabei aus dem Gedanken des Sachzusammenhangs.[326] Diese Maßnahmen dienen nicht der Überführung des Beschuldigten in bestimmten Strafverfahren, sondern der vorsorglichen Bereitstellung von sächlichen Hilfsmitteln für die Erforschung und Aufklärung von Straftaten; sie sind rein vorbeugender und sichernder Natur.[327]

Gleiches gilt für § 81 g StPO, der Maßnahmen zur Identitätsfeststellung in künftigen Strafverfahren erlaubt. Damit handelt es sich um erkennungsdienstliche Zwecke, so dass die Vorschrift ebenfalls einen Fremdkörper in der StPO darstellt.[328] § 81 b und § 81 g StPO regeln zudem den Fall, dass eine Beschuldigteneigenschaft vorliegt und damit die Maßnahmen im repressiven Bereich erfolgt. Sie ermöglichen die Verwendung repressiv gewonnener Daten für präventive Zwecke, nicht aber eine „präventive" Datenerhebung. Somit können diese Vorschriften nicht zur Begründung herangezogen werden, der Bundesgesetzgeber habe im Bereich der Verfolgungsvorsorge eine (landesgesetzliche) Regelung ausschließen wollen.[329] Auch der Wortlaut des § 484 Abs. 4 StPO spricht dafür, dass die Verfolgungsvorsorge entgegen der Annahme des BVerfG in den Bereich der Gefahrenabwehr fällt.[330] Nach dieser Regelung richtet sich die Verwendung personenbezogener Daten, die für die Zwecke künftiger Strafverfahren – also die Verfolgungsvorsorge – in Dateien der Polizei gespeichert sind, nach den Polizeigesetzen. Diese Begrenzung des Regelungsbereichs der StPO ist sachgerecht, weil sich die Regelungen der Verfolgungsvorsorge in einer Gemengelage zwischen

---

324 Vgl. BVerfGE 113, 349 (373).

325 Vgl. BVerwGE 11, 181 (182); OVG Münster DÖV 1983, 603 (604); VG Freiburg NJW 1980, 901; *Meyer-Goßner*, § 81 b StPO, Rn. 3; *Geerds*, Jura 1986, 7 (8); siehe auch *Dreier*, JZ 1987, 1009 (1010 ff.); aA *Schweckendieck*, ZRP 1989, 125 (127); *Kramer*, JR 1994, 224 (228).

326 Vgl. BVerwGE 26, 169 (171); *Meyer-Goßner*, § 81 b StPO, Rn. 3; *Fugmann*, NJW 1981, 2227 (2228); *Riegel*, DÖV 1978, 17 (19); kritisch *Dreier*, JZ 1987, 1009 (1012 ff.).

327 Vgl. *Meyer-Goßner*, § 81 b StPO, Rn. 3.

328 Vgl. *Meyer-Goßner*, § 81 g StPO, Rn. 2; aA BVerfGE 103, 21 (31) welches in der Vorschrift „genuines Strafprozessrecht" sieht, weil es auf Zwecke der (künftigen) Strafverfolgung, nicht auf Zwecke der Gefahrenabwehr ausgerichtet sei. Die Gesetzgebungskompetenz sei deshalb unmittelbar aus § 74 Abs. 1 Nr. 1 GG zu entnehmen.

329 Auch *Zöller*, 2002, S. 86 f. und 91 f. begründet die Gesetzgebungskompetenz des Bundes damit, dass es sich bei der Strafverfolgungsvorsorge um die Speicherung von Daten handelt, die in früheren Strafverfahren gewonnen wurden. Siehe auch *W.-R. Schenke*, 2007, Rn. 30, 418, der davon ausgeht, dass soweit die im Rahmen der StPO geschaffenen Ermächtigungsgrundlagen nicht unmittelbar einschlägig sind, noch Raum bleibt für landespolizeirechtliche Regelungen der Strafverfolgungsvorsorge.

330 Dem Wortlaut des Grundgesetzes lässt sich nicht entnehmen, ob die Verfolgungsvorsorge in den Bereich der Gefahrenabwehr oder der Strafverfolgung fällt. Der Begriff Verfolgungsvorsorge ist in den Artikeln 72 ff. GG nicht genannt.

Polizei- und Strafverfahrensrecht bewegen, in der die präventiven Aspekte überwiegen.[331] So ist auch in der Gesetzesbegründung festgehalten, dass sich die der Gefahrenabwehr dienenden Polizeidateien und die Verwendung der darin enthaltenen Informationen nach den Polizeigesetzen richten, während die StPO nur Anwendung findet, soweit es um die Verwendung der Daten in einem konkreten Strafverfahren geht.[332] Zwar kann der einfache Gesetzgeber nicht über die Kompetenzordnung des Grundgesetzes bestimmen, doch lässt sich dem Grundgesetz nicht entnehmen, ob die Verfolgungsvorsorge zwingend in den Bereich der Gefahrenabwehr oder der Strafverfolgung fällt.[333]

Das Argument des BVerfG, es seien widersprüchliche Regelungen oder Überschneidungen unterschiedlicher Normen zu befürchten, wenn die Länder ebenfalls für den Bereich der Verfolgungsvorsorge Regelungen zur Telekommunikationsüberwachung treffen würden, trägt ebenfalls nicht. Gerade im Bereich des Gefahrenabwehr- und Strafverfolgungsrechts kommt es zu zahlreichen Gemengelagen, in denen zweifelhaft sein kann, ob die Polizei präventiv oder repressiv tätig ist. Zu differenzieren ist anhand des Schwerpunkts der Maßnahme.[334] Richten sich aber schon Maßnahmen der strafverfahrensbedingten Verfolgungsvorsorge[335] nach den Polizeigesetzen, so ist erst recht bei einer landespolizeigesetzlichen Regelung der allgemeinen Verfolgungsvorsorge ein Widerspruch zu den Regeln der StPO nicht zu befürchten. Das Polizeirecht eröffnet einen größeren Spielraum als die StPO. Was für den in Art. 1 Abs. 1, Satz 2 und Art. 2 Abs. 2 GG verankerten Schutzauftrag geboten ist, muss nicht für die dem Rechtsgüterschutz nur mittelbar dienende Strafverfolgung zur Verfügung stehen.[336]

---

331 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 182.

332 Vgl. BT-Drucks. 14/1484, S. 33.

333 Da die Verfolgungsvorsorge in den Art. 72 ff. GG nicht genannt wird, kommt es für die Gesetzgebungskompetenz darauf an, ob Maßnahmen der Verfolgungsvorsorge der repressiven oder präventiven Tätigkeit der Polizei zugeordnet werden.

334 Vgl. BVerwGE 47, 255 (265); OVG Münster DÖV 1980, 574;VGH Baden-Württemberg VBl.BW 1989, 16 (17); *Würtenberger/Heckmann*, 2005, Rn. 189; *Mußmann*, 1994, Rn. 535; *Götz*, NVwZ 1994, 652 (658); aA *W.-R. Schenke*, 2007, Rn. 423.

335 Stützen sich Maßnahmen der Verhinderungs- und Verfolgungsvorsorge auf Informationen, die anlässlich eines konkreten Strafverfahrens gewonnen wurden, spricht man von *strafverfahrensbedingter Verhinderungs- und Verfolgungsvorsorge*, vgl. hierzu ausführlich *Würtenberger/Heckmann*, 2005, Rn. 184.

336 Vgl. *Kniesel*, ZRP 1987, 377 (380).

2. Das „kleine Zitiergebot“[337]

Ist eine landesgesetzliche Regelung zur Datenweitergabe im Sinne des § 88 Abs. 3, Satz 3 TKG möglich, so ist die Verwendung der Kenntnisse für andere Zwecke nur zulässig, wenn sich das gestattende Gesetz ausdrücklich auf Telekommunikationsvorgänge bezieht. Die jeweilige Norm muss dabei klar erkennen lassen, dass der Gesetzgeber eine bewusste Abwägung von Fernmeldegeheimnis und Auskunfts- und Weiterverwendungsinteresse vorgenommen hat.[338]

Dies ist bei § 34 a ThPAG, §§ 33 a und 33 b Nds.SOG, Art. 34 a – c PAG, § 31 POG und § 15 a HSOG der Fall. Die Normen nehmen ausdrücklich auf Telekommunikationsvorgänge Bezug und enthalten insofern eine Abwägung des Gesetzgebers über den Vorrang der Gefahrenabwehr vor dem Fernmeldegeheimnis.[339]

3. Die Regelung im Thüringer Polizeiaufgabengesetz

Während sich die Gesetzgeber der Länder Niedersachsen, Bayern, Rheinland-Pfalz und Hessen wohl an der Regelungstechnik des Bundesgesetzgebers zu § 100 a ff. StPO orientiert haben[340], indem sie in § 33 a Abs. 1 Nds.SOG, Art. 34 a PAG, § 31 Abs. 1 POG und § 15 a Abs. 1 HSOG die Ermächtigung zur Datenerhebung durch die Polizei regeln und in §§ 33 a Abs. 7; 33 c Nds.SOG, Art. 34 b PAG, § 31 Abs. 6 POG und § 15 a Abs. 1 HSOG die Verpflichtung der geschäftsmäßigen Telekommunikationsdienstleister zur Auskunftserteilung und Überwachungsermöglichung vorgesehen haben, hat sich der thüringer Gesetzgeber eines anderen Instrumentariums der Gesetzestechnik bedient.

In § 34 a Abs. 1 ThPAG ist dem Wortlaut nach die Ermächtigung der Polizei enthalten, von geschäftsmäßigen Telekommunikationsdienstleistern Auskunft über den Inhalt, einschließlich der innerhalb des Telekommunikationsnetzes in Datenspeichern abgelegten Inhalte und die näheren Umstände der Telekommunikation einschließlich der Daten über den Standort

---

337 Vgl. *Holznagel/Enaux/Nienhaus*, 2006, Rn. 647; *Zerres*, in: Scheurle/Mayen (Hrsg.), § 85 TKG, Rn. 40.

338 Vgl. *Zerres*, in: Scheurle/Mayen (Hrsg.), § 85 TKG, Rn. 40.

339 Vgl. LT-Drucks. Th 3/2128, S. 34; LT-Drucks. Nds. 15/240, S. 15 ff., 18; LT-Drucks. Bayern 15/2096, S. 2 und 51; LT-Druck. RhPf 14/2287, S. 33 f., 47; LT-Drucks. Hessen 16/2352, 18 f.

340 § 100 a StPO enthält die Voraussetzungen unter denen eine Telekommunikationsüberwachung angeordnet werden kann. In § 100 b StPO ist Anordnung und Ausführung der Telekommunikationsüberwachung geregelt.

nicht ortsfester Telekommunikationsanlagen zu verlangen. In § 34 a Abs. 4 ThPAG ist zusätzlich der Verweis auf die Bestimmungen des G-10-Gesetzes in ihrer jeweils geltenden Fassung enthalten, welche die Mitwirkungsverpflichtung der geschäftsmäßigen Telekommunikationsdienstleister beinhalten, die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen sowie Auskunft über die näheren Umstände zu erteilen.

Aus der Gesetzesbegründung ergibt sich, dass § 34 a Abs. 1 ThPAG die Ermächtigungsgrundlage der Polizei gegenüber dem Bürger/Betroffenen und die Verweisung in § 34 a Abs. 4 ThPAG die Verpflichtung der Telekommunikationsunternehmen enthalten soll.[341]

Kompetenznormen sind aufgrund ihrer rechtsstaatlichen Schutz- und Ordnungsfunktion zwingendes Recht; sie sind grundsätzlich übertragungsfeindlich und müssen daher von dem Träger wahrgenommen werden, dem sie von der Rechtsordnung zugeteilt sind.[342] Art. 30 GG, nach dem die Ausübung der staatlichen Befugnisse und die Erfüllung staatlicher Aufgaben Sache der Länder ist, soweit das Grundgesetz keine andere Regelung trifft oder zulässt, ist kein dispositives Recht.[343] Für die Wahrnehmung der Aufgaben und Befugnisse durch Bund und Länder hat dies zunächst zur Folge, dass jede bundesstaatliche Ebene die ihr zugewiesenen Aufgaben und Befugnisse selbstständig und eigenverantwortlich wahrnimmt, soweit das Grundgesetz nicht Mit- und Einwirkungsrechte anderer föderaler Organe vorsieht. Dies gilt für Gesetzgebungsbefugnisse ebenso wie für Verwaltungs- oder Rechtsprechungsaufgaben.[344] Deswegen ist weder die förmliche Übertragung einzelner Gesetzgebungsbefugnisse, außerhalb der Art. 71 und 72 Abs. 1 und 2 GG, noch die stillschweigende Duldung von bzw. die ausdrückliche Zustimmung zu Übergriffen der einen auf die jeweils andere legislative Ebene zulässig.[345] Dieses Verbot gilt wechselseitig im Bund-Länder-Verhältnis.[346]

---

341 Vgl. LT-Drucks. Th. 3/2128, S. 34 und 37.

342 Vgl. *März*, in: v.Mangoldt/Klein/Starck (Hrsg.), Art. 30 GG, Rn. 26; *Sannwald*, in: Schmidt-Bleibtreu/Klein, Art. 30 GG, Rn. 8; *Rengeling*, in: HStR IV, § 100, Rn. 12.

343 Vgl. *Pieroth*, in: Jarass/Pieroth, Art. 30 GG, Rn. 8; *Gubelt*, in v.Münch/Kunig (Hrsg.), Art. 30 GG, Rn. 21.

344 Vgl. *März*, in: v.Mangoldt/Klein/Starck (Hrsg.), Art. 30 GG, Rn. 27.

345 In BVerfGE 1, 14 (35) heißt es: „Über seine Gesetzgebungskompetenz kann ein Land nicht verfügen. Und der Bund kann eine Gesetzgebungszuständigkeit, die ihm das Grundgesetz nicht gewährt, auch nicht durch Zustimmung des Landes gewinnen“.

346 Vgl. *März*, in: v.Mangoldt/Klein/Starck (Hrsg.), Art. 30 GG, Rn. 27; *Pieroth*, in: Jarass/Pieroth, Art. 30 GG, Rn. 8.

Eine Duldung der Rechtsetzung durch das hierfür föderal nicht zuständige Organ kann darin liegen, dass der Bundes- oder Landesgesetzgeber im Rahmen seiner Rechtsetzung auf Normen verweist, die der anderen bundesstaatlichen Ebene angehören.[347] Dies gilt jedenfalls bei der dynamischen Verweisung[348], da der Gesetzgeber dabei eventuell spätere Änderungen der inkorporierten Vorschrift durch den hierfür zuständigen Normgeber akzeptiert und dadurch Rechtsetzungsbefugnisse, deren selbstständige Inanspruchnahme und inhaltliche Ausfüllung er regelmäßig nicht weiter kontrollieren wird, überträgt und dadurch entgegen Art. 30 GG eigene Zuständigkeiten aufgibt und auf einen von der föderalen Rechtsordnung nicht vorgesehenen Normgeber verschiebt.[349]

Das BVerfG billigt die dynamische Verweisung grundsätzlich, sofern die Verweisung den Prinzipien der Rechtsstaatlichkeit, insbesondere der hinreichenden Bestimmtheit der in Bezug genommenen Vorschriften[350], der Demokratie und der Bundesstaatlichkeit entspricht[351] und der grundrechtliche Gesetzesvorbehalt nicht verletzt wird[352].

Die Verweisung in § 34 a Abs. 4 ThPAG bedarf daher unter zwei Gesichtspunkten einer genaueren Betrachtung: Erstens, ob die dynamische Verweisung den Anforderungen des Bundesverfassungsgerichts genügt und zweitens, ob damit dem „kleinen Zitiergebot“ des § 88 Abs. 3, Satz 3 TKG Rechnung getragen ist.

Durch die Verweisung auf die Normen des G-10-Gesetzes werden rechtsstaatliche Verfassungsprinzipien nicht verletzt. Eine Verlagerung von Gesetzgebungsbefugnissen kann zwar

---

347 Vgl. *März*, in: v.Mangoldt/Klein/Starck (Hrsg.), Art. 30 GG, Rn. 28.

348 Für die statische Verweisung, bei der der Gesetzgeber „punktgenau“ auf eine andere Norm in einer ganz bestimmten Fassung Bezug nimmt und sie seiner Rechtsetzung inkorporiert, wird der Inhalt der verwiesenen Norm zum korporierten Bestandteil des verweisenden Gesetzes. Die statische Verweisung kann damit nicht unter bundesstaatlichen Gesichtspunkten beanstandet werden, da die verwiesene Norm Geltungskraft, Ranghöhe und prozessrechtliches Schicksal der verweisenden Norm teilt, vgl. *März*, in: v.Mangoldt/Klein/Starck (Hrsg.), Art. 30 GG, Rn. 28.

349 Vgl. *März*, in: v.Mangoldt/Klein/Starck (Hrsg.), Art. 30 GG, Rn. 29; siehe auch *Sachs*, NJW 1981, 1651 f. *Pieroth*, in Jarass/Pieroth, Art 30 GG, Rn. 9, *I. Pernice*, in: Dreier (Hrsg.), Art. 30 GG, Rn. 21 und *Gubelt*, in v.Münch/Kunig (Hrsg.), Art. 30 GG, Rn. 21, sehen die dynamische Verweisung als unzulässig an, da die Länder ihre Gesetzgebungskompetenzen nicht auf den Bund übertragen dürfen. Ausnahmen von diesem Verbot gelten dann, wenn der Bundesgesetzgeber auf Landesrecht verweist. In diesen Fällen liegt genau genommen keine Verlagerung von Bundeskompetenzen auf die Länder vor; der gesamtstaatliche Normgeber macht vielmehr von den Ermächtigungen der Art. 71 und 72 GG Gebrauch, indem er den Ländern deren Zuständigkeiten teilweise wieder eröffnet.

350 Vgl. BVerfGE 26, 338 (367).

351 Vgl. BVerfGE 78, 32 (36).

352 Vgl. BVerfGE 47, 285 (315 ff.), E 78, 32 (36).

unter dem Blickwinkel des Demokratieprinzips verfassungsrechtlich bedenklich sein, wenn es sich um grundrechtsrelevante Regelungen handelt, bei denen der Gesetzesvorbehalt eine eigenverantwortliche Prüfung durch den zuständigen Gesetzgeber erfordert oder wenn die verweisende und die in Bezug genommene Vorschrift zu ganz verschiedenen Rechtsbereichen gehören.[353] Diesen Anforderungen aber genügt § 34 a Abs. 4 ThPAG.

Der Zugriff auf die Daten der Betroffenen, der Eingriff in den Grundrechtsbereich, erfolgt aufgrund des § 34 a Abs. 1 ThPAG. Lediglich der Zugriff auf die Telekommunikationsunternehmen erfolgt durch die Verweisung auf das G-10-Gesetz. Regelungsgegenstand des G-10-Gesetzes und des ThPAG ist die Gefahrenabwehr. Zwar bezieht sich das G-10-Gesetz auf die Abwehr von Gefahren, die den Bestand und die Sicherheit der Bundesrepublik bedrohen, während das ThPAG die Abwehr von Gefahren innerhalb des Bundeslandes Thüringen regelt. Doch wurzeln beide Gesetze im präventiven Bereich und sehen mit der präventiven Telekommunikationsüberwachung identische Mittel zur Gefahrenabwehr vor. Eine Verletzung von Grundrechten der Diensteanbieter dadurch, dass das ThPAG den Zugriff über den Verweis auf das G-10-Gesetz vorsieht und nicht selbst die Zugriffsmöglichkeit festgelegt hat, liegt nicht vor. Denn der Bundesgesetzgeber selbst hat durch die Regelungen der §§ 88 und 110 TKG die Zugriffsmöglichkeit eröffnet.

Der Verweis auf das G-10-Gesetz steht auch dem „kleinen Zitiergebot“ nicht entgegen, da der Landesgesetzgeber selbst die Abwägung zwischen Fernmeldegeheimnis bzw. Datenschutz und Gefahrenabwehr vorgenommen hat.[354]

4. Fazit

Da die landesgesetzlichen Regelungen gesetzliche Vorschriften im Sinne des § 88 Abs. 3, Satz 3 TKG sind, kann die Polizei Auskunft sowohl über Daten verlangen, die die Telekommunikationsunternehmen im Rahmen ihrer Befugnisse künftig speichern, als auch über Daten, die bei den Diensteanbietern schon vorhanden sind. Dies sind die Verkehrsdaten und auch Nachrichteninhalte, die beispielsweise in einer Mailbox, T-Net-Box oder einem E-Mail-Posteingang abgelegt sind.[355]

---

353 Vgl. BVerfGE 47, 285 (315 ff.); so auch BayVerfGH NVwZ 1989, 1053 (1054).
354 Vgl. unter III. 4. b).
355 § 34 a Abs. 1, Satz 1 ThPAG; § 33 a Abs. 2 Nr.1 Nds.SOG; § 15 a Abs. 2 HSOG.

Die sonstige Kenntnis vom Nachrichteninhalt ist für die Polizeibehörden durch die Überwachung der Telekommunikation zu erlangen; dabei sind ihnen auch (weitere) Verbindungsdaten von den Betreibern von Telekommunikationsanlagen zur Verfügung zu stellen, beispielsweise Angaben zum Standort von Mobilfunkgeräten.

Die Polizeibehörden haben, sofern das materielle Polizeirecht entsprechende Ermächtigungsgrundlagen vorsieht, einen umfassenden Zugriff auf nahezu sämtliche Daten, die bei einem Telekommunikationsvorgang anfallen. Durch die Überwachungsermöglichung und Auskunftserteilung wissen sie nicht nur wer wann mit wem wie lange über welche Themen kommuniziert hat, sondern auch von wo aus die Kommunikation erfolgt ist.

V. Der IMSI-Catcher

Nach § 33 b Abs. 1 Nds.SOG, Art. 34 a Abs.2 – 4 PAG, § 31 Abs. 1 und 2 POG und § 15 a Abs. 3 HSOG dürfen technische Mittel, mit denen aktiv geschaltete Mobilfunkendeinrichtungen zur Datenabsendung an eine Stelle außerhalb des Telekommunikationsnetzes veranlasst werden, zur Ermittlung der Geräte- und Kartennummer und zur Ermittlung des Standorts einer Endeinrichtung eingesetzt werden. Der Polizei eröffnet sich damit die Möglichkeit der Nutzung des IMSI-Catchers. In Niedersachsen und Bayern ist zusätzlich die Möglichkeit der Verhinderung und Unterbrechung von Kommunikation vorgesehen.[356]

Bei jedem Telekommunikationsvorgang via Handy werden dem Telekommunikationsdienstleister die IMSI, die IMEI und der Standort des Mobilfunkgerätes übermittelt. Die IMSI (International Mobile Subscriber Identity) ist eine weltweit eindeutige Kennung, die den Teilnehmer (Vertragspartner des Netzbetreibers) eindeutig identifiziert. Sie ist auf der Chipkarte (SIM = Subscriber Identity Module) gespeichert, die ein Mobilfunkteilnehmer bei Abschluss seines Vertrages erhält.[357] Die IMEI (International Mobile Equipment Identity) ist die Serien- oder Gerätenummer eines Handys, die dann von Bedeutung ist, wenn das Mobiltelefon mit verschiedenen SIM-Karten betrieben wird.[358]

---

356 Siehe dazu diese Kapitel unter I. und LT-Drucks. Bayern 15/2096, S. 58.
357 Vgl. *Wolter*, in: FG für Hilger, S. 300; *Fox*, DuD 2002, 212 (213).
358 Vgl. *Wolter*, in: FG für Hilger, S. 300; *Fox*, DuD 2002, 212 (213).

Anhand der ersten Ziffern der IMSI lässt sich der Netzbetreiber feststellen, anhand der weiteren Ziffern kann über die beim Netzbetreiber gespeicherten Bestandsdaten der Mobilfunkteilnehmer ermittelt werden. Mit Hilfe der IMSI kann daher nicht nur die Identität des Teilnehmers, sondern auch die Mobilfunknummer bestimmt werden.[359]

Um Auskunft über Verbindungsdaten oder eine Überwachung der Telekommunikation verlangen zu können, muss der betroffene Anschluss genau bezeichnet werden. Dies gilt nicht nur, damit die technische Durchführung überhaupt möglich ist, sondern auch aufgrund der Anforderungen, die § 34 a Abs. 2, Satz 7 ThPAG, § 33 a Abs. 4 Nds.SOG, Art. 34 c Abs. 3 PAG, § 31 Abs. 5, Satz 2 POG und § 15 a Abs. 4, Satz 3 HSOG an eine Überwachungs- oder Auskunftsanordnung stellen.[360]

Unbekannte Mobilfunkrufnummern können durch den IMSI-Catcher ermittelt werden.[361] Unter einem IMSI-Catcher versteht man Geräte, die als „mobile Basisstation“ arbeiten. Sie verhalten sich wie eine feste Basisstation einer regulären Funkzelle eines Mobilfunknetzes und beheimaten einen Visitor Location Register (VLR) für alle Teilnehmer, die sich in der Funkzelle aufhalten.[362] Jedes eingeschaltete Handy mit einer SIM des simulierten Netzbetreibers im Empfangsbereich des IMSI-Catchers registriert und authentisiert sich daher unbemerkt gegenüber diesem IMSI-Catcher. Das Gerät kann nun durch Vortäuschung eines Fehlers von jedem Handy die Übersendung der IMSI erzwingen.[363] Zu dieser IMSI kann es beim Home Location Register (HLR) des Netzbetreibers die passenden Rufnummer anfordern.[364] Die IMEI wird durch den IMSI-Catcher auf technisch ähnliche Art wie die IMSI ermittelt.[365]

Vom Einsatz eines IMSI-Catchers ist nicht nur der Teilnehmer betroffen, auf dessen Anschluss die Maßnahme zielt.[366] Vielmehr werden alle Teilnehmer, die sich mit eingeschalte-

---

359 Vgl. *Fox*, DuD 2002, 212 (213).

360 Für die Anordnungen nach § 34 a Abs.2, Satz 7 ThPAG, Art. 34 c Abs. 3 PAG und § 15 a Abs. 4, Satz 3 HSOG genügt auch die Gerätenummer. § 33 a Abs. 4 Nds.SOG und § 31 Abs. 5, Satz 2 POG verlangen die Bezeichnung des Anschlusses.

361 Siehe *Roggan*, 2003, S. 71 f.

362 Vgl. *König*, 2005, S. 251; *Fox*, DuD 1997, 539.

363 Vgl. *Fox*, DuD 1997, 539; *ders.*, DuD 2002, 212 (213).

364 Vgl. *König*, 2005, S. 251; *Fox*, DuD 1997, 539; *Beheim*, DuD 1994, 327 (329).

365 Vgl. *Fox*, DuD 2002, 212 (213).

366 Vgl. *Roggan*, 2003, S. 73.

tem Handy in der Reichweite des Gerätes aufhalten, identifiziert, bis der gewünschte gefunden ist. Dies können je nach Funkzelle leicht einige hundert Teilnehmer sein.[367]

Der IMSI-Catcher ermöglicht eine relativ genaue Feststellung der Position eines Handys. Damit kann der Aufenthaltsort einer gesuchten Person eingegrenzt und ein polizeilicher Zugriff ermöglicht werden.[368] Normalerweise wird der Standort des Mobilfunkteilnehmers über die jeweilige Funkzelle ermittelt, über die die Telekommunikation abgewickelt wird.[369] Der Basisstation eines Netzbetreibers ist der Standort eines eingebuchten Mobilfunkgeräts aber nur „zellgenau“ und daher sehr grob bekannt, denn eine Mobilfunkzelle kann in einem der D-Netze leicht einen Durchmesser von mehreren Kilometern haben. Da der IMSI-Catcher üblicherweise eine Funkzelle mit geringer Leistung und damit erheblich geringerer Ausdehnung simuliert, kann so der Aufenthaltsort eines eingeschalteten Handys ziemlich stark eingegrenzt[370] und damit quasi „implizit“ geortet werden.[371] Die implizite Ortungsfunktion des IMSI-Catchers setzt in jedem Fall voraus, dass das von der gesuchten Person genutzte Mobilfunknetz und die IMSI bekannt sind, sich das Handy der gesuchten Person im Standby-Betrieb befindet und der IMSI-Catcher das Handy der gesuchten Person gefangen hat. Ohne Vorabkenntnis der IMSI des benutzten Handys und eine grobe Kenntnis des Aufenthaltsorts der gesuchten Person ist eine Ortung mit dem IMSI Catcher nicht möglich.[372]

---

367 Vgl. *Fox*, DuD 1997, 539.

368 Vgl. *Fox*, DuD 2002, 212 (213).

369 So kann dann auch ein Bewegungsbild erstellt werden, wie es die Gesetzesbegründung Niedersachsens LT-Drucks. 15/240, S. 18 vorsieht. Siehe zur Erstellung von Bewegungsbildern als strafprozessuale Maßnahme *Demko*, NStZ 2004, 57 ff.; *Roggan*, 2003, S. 73.

370 *Nack*, in: KK, § 100 a StPO, Rn. 3 nimmt einen Radius von 300 m für den Einzugsbereich des IMSI-Catchers an. *Meixner/Fredrich*, § 15 a HSOG, Rn. 3 gehen von einer Standortbestimmung bis auf 50 Meter aus.

371 Zu dieser Funktion des IMSI-Catchers führt die Gesetzesbegründung Niedersachsen LT-Drucks. 15/240 aus: „Weiterhin können aktivgeschaltete Handys konkret lokalisiert werden. Dabei ist im Vergleich zur Lokalisierungsmöglichkeit über das TKD-Unternehmen die Standortbestimmung mit einem IMSI-Catcher wesentlich genauer, weil die Basisstationen/Mobilfunkzellen des Unternehmens in bestimmten Bereichen einen Durchmesser von wenigen Kilometern abdecken. Demgegenüber fingiert der IMSI-Catcher eine Funkzelle des Mobilfunkunternehmens mit so starker Feldstärke, dass sich alle in seiner Reichweite – ca. 100 m – befindlichen betriebsbereiten Handys „einloggen“ und so dadurch die Funktionalität des Gerätes bestimmenden Informationen aufgenommen werden können. Dieser Vorteil des IMSI-Catchers ist im Rahmen der hier zulässigen Nutzung des Gerätes für die Polizei von besonderer Bedeutung, sofern Personen über Handy bzw. über SMS ihren Suizid ankündigen oder sonst bekannt ist, dass sie ein Mobiltelefon besitzen.“

372 Vgl. *Fox*, DuD 2002, 212 (213 f.).

Darüber hinaus ist es mittels eines IMSI-Catchers möglich, Telekommunikation zu unterbrechen oder zu verhindern.[373]

Der Einsatz der IMSI-Catchers ist, mangels Regelung im ThPAG, nur der Polizei in Niedersachsen, Bayern, Rheinland-Pfalz und Hessen vorbehalten. Das ThPAG erwähnt zwar die Standortbestimmung, diese Angabe gehört aber zu den Daten, die die Betreiber von Telekommunikationsanlagen im Rahmen der Telekommunikationsüberwachung bereitzustellen haben.[374] Diese Bestimmung ist aber nur möglich, wenn Rufnummer, IMSI oder IMEI bekannt sind. Eine Möglichkeit diese in Erfahrung zu bringen, steht der thüringer Polizei nur nach §§ 112 Abs. 4; 113 Abs. 1 TKG zur Verfügung.[375]

---

373 Vgl. LT-Drucks. Bayern 15/2096, S. 58 und Schriftlicher Bericht zum Entwurf eines Gesetzes zur Änderung des Niedersächsischen Gefahrenabwehrgesetzes LT-Drucks. Nds. 15/776, S. 8. Diese Möglichkeit ist vorgesehen in § 33 b Abs. 2 Nds.SOG und Art. 34 a Abs. 4 PAG.

374 § 7 Nr. 7 TKÜV.

375 *Ebert/Honnacker/Seel*, § 34 a ThPAG, Rn. 22 ff. sieht dagegen den Einsatz des IMSI-Catchers als einen außerhalb der Telekommunikationsvorgangs liegenden Eingriff an. Ob daher die thüringer Polizei den Einsatz des IMSI-Catchers auf eine andere Ermächtigungsnorm des ThPAG stützten kann, bleibt nach der Kommentierung aber offen.

Kapitel 4: Länderübergreifende Sachverhalte

„Die oftmals über Ländergrenzen hinaus vernetzt arbeitenden Täter treffen vielfach Absprachen über das Telefon und andere moderne Telekommunikationsmittel. Die präventivpolizeiliche Telekommunikationsüberwachung ist nicht nur zur Bekämpfung der Organisierten Kriminalität und des Terrorismus, sondern auch zur Verhinderung und Unterbindung anderer schwerwiegender Straftaten unverzichtbar.“ Diese Aussage ist in fast allen Gesetzesbegründungen der hier untersuchten Polizeigesetze mit nahezu identischem Wortlaut zu finden.[376] Daran zeigt sich, dass das grenzüberschreitende Handeln der potenziell zu überwachenden Personen, den Landesgesetzgebern wohl bewusst ist.

Kriminelle Organisationen und Vereinigungen lassen ihre Aktivitäten nicht an den Grenzen eines Bundeslandes enden. „Länderübergreifende Sachverhalte“ sind daher nicht nur denkbar, sondern regelmäßig zu erwarten. Die dabei entstehenden grenzüberschreitenden Kommunikationsvorgänge sind zum einen dadurch möglich, dass sich der Telefonanschluss des für die Gefahrensituation in einem Bundesland verantwortlichen Störers in einem anderen Bundesland befindet. Zum anderen kann das Telekommunikationsunternehmen, welches die gewünschten Daten und Abhöreinrichtungen zu Verfügung stellen soll, seinen Sitz in einem anderen Bundesland haben. Auch kann sich die Gefahrensituation, derentwegen eine Telekommunikationsüberwachung angeordnet werden soll über mehrere Bundesländer erstrecken. Denkbar ist ebenfalls, dass die zu überwachende Person mit ihrem Mobiltelefon die Grenze in ein anderes Bundesland überschreitet.

Ob daher eine Landespolizeibehörde Auskünfte über landesexterne Telekommunikationsteilnehmer einholen, ob sie Auskunftsersuchen auch an einen landesfremden Anbieter stellen kann und ob sie dieses Auskunftsersuchen auch stellen darf, wenn die Gefahrensituation eine überörtliche ist, die sich über die Landesgrenze hinaus erstreckt, wird in den Gesetzesbegründungen Thüringens, Niedersachsens, Rheinland-Pfalz und Hessens mit keinem Wort erwähnt.[377] Lediglich der bayerische Landesgesetzgeber scheint sich des Problems ansatz-

---

376 Vgl. LT-Drucks. Th. 3/2128, S. 1, 34; LT-Drucks. Nds. 15/240, S. 8; LT-Drucks. Bay. 15/2096, S. 26, 27; LT-Drucks. RhPf. 14/2287, S. 30. Hessen stellt zwar darauf ab, dass die neuen Befugnisnormen ausschließlich dem Schutz von Bürgern vor akuten Lebensgefahren, wie z.B. Suizid, dienen. Aber auch dabei sind länderübergreifende Sachverhalte denkbar, wenn die gefährdete Person die Ländergrenzen überschreitet.

377 Vgl. LT-Drucks. Th. 3/2128; LT-Drucks. Nds. 15/240; LT-Drucks. RhPf. 14/2287.

weise bewusst zu sein und erwähnt in der Gesetzesbegründung die Zugriffsmöglichkeit der Landespolizeibehörden auch auf Diensteanbieter, deren Firmensitz sich außerhalb Bayerns befindet.[378]

Wird die Einführung der präventiven Telekommunikationsüberwachung überwiegend mit dem effektiven Schutz der Bürger vor Gefahren der Organisierten Kriminalität und des internationalen Terrorismus begründet, so kann eine solche Gefahrenabwehr nur effektiv sein, wenn die einschlägigen Landesgesetze die zuständigen Behörden auch dazu ermächtigen, Anschlüsse über die Ländergrenzen hinweg zu überwachen.

Ob und wie eine länderübergreifende Telekommunikationsüberwachung verfassungsrechtlich zulässig sein kann und ob diese durch die Landespolizeigesetze den Polizeibehörden ermöglicht wird, soll im Folgenden untersucht werden.

I. Die Überwachung ausländischer Kommunikation

1. Die strategische (Auslands-)Überwachung

In seinem Urteil zur strategischen Fernmeldeüberwachung hat das BVerfG Ausführungen zur Überwachung ausländischer Kommunikation und zum räumlichen Geltungsbereich des Art. 10 GG getroffen.[379]

Gegenstand der strategischen Überwachung gemäß § 5 G-10-Gesetz durch den Bundesnachrichtendienst sind internationale Telekommunikationsbeziehungen, die hinsichtlich bestimmter Suchbegriffe ausgewertet werden.[380] Hierunter ist der Post- und Fernmeldeverkehr zwischen zwei bestimmten Eckpunkten in beiden Richtungen zu verstehen, wobei ein Eckpunkt sich außerhalb der Bundesrepublik befindet.[381]

---

378 Vgl. LT-Drucks. Bayern 15/2096, S. 29. Die Gesetzesbegründung bejaht dabei eine Zugriffsmöglichkeit auch auf externe Anbieter unter Hinweis auf die Entscheidung des BVerwG in BVerwGE 79, 339 ff. zur bundesweiten Geltung von Landesgesetzen und der Überlegung, dass diese Anbieter ihre Dienste auch in Bayern anbieten und damit auch in Bayern den Adressaten einer Maßnahme nach Art. 34 a PAG die Möglichkeit eröffnen, Telekommunikationsdienste zu nutzen, die durch die polizeilichen Maßnahmen überwacht werden sollen.

379 Vgl. BVerfGE 100, 313 (362 ff.).

380 Zum Verfahren vgl. *B. Huber*, NJW 2001, 3296 (3297).

381 Vgl. *Roewer*, § 3 G-10-Gesetz, Rn. 4. Aus der Stellungnahme der Bundesregierung im Verfahren über die Strategische Überwachung nach dem G-10-Gesetz ergibt sich, dass nach Ansicht der Bundesregierung Überwachungsmaßnahmen bei Telekommunikation, die im Ausland-Ausland-Verkehr geführt wird, nicht

Bei der strategischen Überwachung[382] erfolgt der Zugriff auf die Telekommunikation nicht über einen Diensteanbieter. Die Erfassung und Aufzeichnung des Telekommunikationsverkehrs erfolgt durch die Empfangsanlagen des Bundesnachrichtendienstes. Welche Telekommunikationsbeziehungen betroffen sind, legt das nach § 10 Abs. 1 G-10-Gesetz zuständige Bundesministerium fest.[383]

In dem Verfahren über die strategische Fernmeldeüberwachung hatte das BVerfG auch über die Einzelfallüberwachung nach § 3 G-10-Gesetz zu entscheiden. Drei der Beschwerdeführer sahen sich durch § 3 Abs. 2 G-10-Gesetz in ihrem verfassungsgemäßen Rechten verletzt. Diese Beschwerdeführer waren ein uruguayischer Staatsbürger, die Verlegerin einer deutschen Tageszeitung sowie ein Journalist mit Wohnsitz in Deutschland und Italien.[384]

Nach Ansicht des BVerfG entfaltet Art. 10 GG – jedenfalls dann, wenn die Erfassung und Auswertung des im Ausland geführten Telefonverkehrs auf deutschem Boden stattfindet – Bindungswirkung, unabhängig von der Nationalität oder dem Standort des Kommunikationsteilnehmers.[385] Auf Grund des Standes und der Entwicklung der Technik, die es ermöglicht, dass die Staatsgewalt ihre Tätigkeit auch auf das Gebiet anderer Staaten erstrecken kann, ohne dort durch Organgewalt körperlich anwesend sein zu müssen, dürfe gerade auch mit Blick auf das Völkerrecht die Geltung der Grundrechte bei einem Sachverhalt mit Auslandsbezug nicht gänzlich ausgeschlossen sein.[386] Die näheren Einzelheiten dieser Frage abschließend zu klären, hielt das Gericht nicht für erforderlich, da zum einen die Erfassung und Aufzeichnung des Telekommunikationsverkehrs auf deutschem Boden erfolgte und zum anderen

---

unter das G-10-Gesetz fallen, vgl. BVerfGE 100, 313 (339). Soweit der BND Fernmeldeaufklärung durch das Abhören internationaler Kommunikation, die ihren Ausgangs- bzw. Endpunkt jeweils im Ausland hat („offener Himmel“) betreibt, wird dies auf §§ 1 Abs. 1; 2 Abs. 1 BNDG gestützt, so *B. Huber*, NJW 2001, 3296 (3298) unter Hinweis auf die Äußerungen des BND in der mündlichen Verhandlung vor dem BVerfG.

382 Im Unterschied zur Individualkontrolle soll die strategische Kontrolle sach- und nicht personenbezogen sein. Personen sind als Brief- und Telefonpartner von der Überwachung betroffen, aber sie treten nicht aus ihrer Anonymität heraus. Es interessiert nur der Beitrag, den sie zur Sicherheit der Bundesrepublik beisteuern können, vgl. *Borgs*, in: Borgs-Maciejewski/Ebert, § 3 G-10-Gesetz, Rn. 2. So dürfen die Suchbegriffe keine Identifizierungsmerkmale enthalten, die zu einer gezielten Erfassung bestimmter Telekommunikationsanschlüsse führen, § 5 Abs. 2, Satz 2 G-10-Gesetz.

383 § 5 Abs. 1, Satz 2 G-10 Gesetz. Dazu *Borgs*, in: Borgs-Maciejewski/Ebert, § 3 G-10-Gesetz, Rn. 4.

384 Vgl. BVerfGE 100, 313 (333 f.).

385 Vgl. BVerfGE 100, 313 (363 f.); *Hermes*, in: Dreier (Hrsg.), Art. 10 GG, Rn. 41. Siehe zur Problematik des territorialen Schutzbereichs des Fernmeldegeheimnisses *Gröpl*, ZRP 1995, 13 (15); siehe auch *Arndt*, DÖV 1996, 459 (461 f.).

386 Vgl. BVerfGE 100, 313 (362 f.).

die Auswertung durch im Inland ansässige Behörden stattfand.[387] Jedenfalls damit sei der Gebietskontakt gegeben, so dass Art. 10 Abs. 1 GG uneingeschränkt Prüfungsmaßstab für das Handeln des Bundesnachrichtendienstes sei.[388] In diesem Zusammenhang hat das BVerfG jedoch betont, dass im Rahmen jener Verfassungsbeschwerdeverfahren über geheimdienstliche Tätigkeiten, die nicht dem G-10-Gesetz unterliegen, ebenso wenig zu entscheiden sei wie über die Frage, was für ausländische Kommunikationsteilnehmer im Ausland gelte.[389] Hintergrund war, dass die Verfassungsbeschwerde des uruguayischen Staatsangehörigen verworfen wurde, da er eine mögliche Rechtsverletzung nicht hinreichend dargelegt hatte[390] und die Verlegerin und der Journalist als juristische inländische Person bzw. deutscher Staatsbürger nicht von § 3 Abs. 2, Satz 3 G-10-Gesetz a.F. betroffen waren[391].

Das BVerfG hat damit zu verstehen gegeben, dass prinzipiell auch Telekommunikationsüberwachungen mit Auslandsbezug dem Schutz des Art. 10 GG unterliegen können. Folglich wären Einschränkungen dann an Art. 10 Abs. 2 GG iVm dem G-10-Gesetz zu messen.[392] Art. 10 GG war aus Sicht des BVerfG jedenfalls auf die internationalen Telekommunikationsverbindungen anzuwenden, die vom Ausland nach Deutschland oder von der Bundesrepublik ins Ausland geführt wurden, da mit der Erfassung, Aufzeichnung und Auswertung auf deutschem Hoheitsgebiet der erforderliche Gebietskontakt gegeben war.[393] Ob sich die Reichweite von Art. 10 GG auch für ausländische Kommunikationsteilnehmer im Ausland, also rein ausländische Kommunikation erstreckt, bleibt jedoch offen.[394]

---

387 Der EGMR hatte im Anschluss an das Urteil des BVerfG vom 14.07.1999 zu entscheiden, ob die Überwachung des Fernmeldeverkehrs ein unerlaubter Eingriff in die Souveränität der ausländischen Staaten sei, in denen die überwachten Personen wohnen, vgl. Urteil des EGMR vom 29.06.2006 in NJW 2007, 1433 ff. Da jedoch die von ausländischen Staaten ausgehenden Signale von Überwachungsanlagen auf deutschem Gebiet kontrolliert und die Daten in Deutschland verwendet wurden, war nach Ansicht des EGMR von den Beschwerdeführern nicht ausreichend vorgetragen und nachgewiesen, dass die Anwendung der strategischen Überwachung in die völkerrechtlich geschützte territoriale Souveränität ausländischer Staaten eingreifen, vgl. EGMR NJW 2007, 1433 (1435).

388 Vgl. dazu *Arndt*, NJW 2000, 47 (48 f.), der es als bedauerlich ansieht, dass das BVerfG die Frage des räumlichen Wirkungsbereichs von Art. 10 GG keiner eindeutigen und abschließenden Entscheidung zugeführt hat. Dazu auch *Möstl*, DVBl. 1999, 1394 (1397) und *Sachs*, JuS 2000, 597 (598).

389 Vgl. BVerfGE 100, 313 (364).

390 Vgl. BVerfGE 100, 313 (357).

391 Vgl. BVerfGE 100, 313 (384).

392 Vgl. hierzu *Möstl*, DVBl. 1999, 1394 (1397), der die Frage aufwirft, ob bei einer (möglichen) Anwendung von Art. 10 GG auf Ausländer im Ausland § 3 Abs. 2 Satz 3 G-10-Gesetz nicht als unverhältnismäßig und § 1 Abs 2 Satz 1 G-10-Gesetz nicht als unzureichende Rechtsgrundlage der Abhörpraxis außerhalb des G-10-Gesetzes gelten müssten.

393 BVerfGE 100, 313 (363 f.)

394 Vgl. *Sachs*, JuS 2000, 597 (598); *Möstl*, DVBl. 1999, 1394 (1397).

2. Die (Auslands-)Einzelfallüberwachung

Ob der Individualkontrolle nach dem G-10-Gesetz und den Gesetzen, die ebenfalls eine Telekommunikationsüberwachung vorsehen, auch ausländische Telefonanschlüsse unterfallen können, sagen die Gesetze nicht. Der Zugriff auf die Telekommunikationsdaten erfolgt jedoch immer über die einzelnen (inländischen) Diensteanbieter. Zur Überwachung eines bekannten inländischen Anschlusses ist es nahe liegend, den Betreiber des Anschlusses in die Pflicht zu nehmen, da über diesen alle Verbindungen zu der überwachten Kennung zu schalten sind und die Überwachung durch den Anschlussbetreiber das einfachste und zugleich zuverlässigste Verfahren ist.[395]

In § 4 Abs. 1 TKÜV ist geregelt, dass Telekommunikation nicht erfasst wird, wenn sich das Endgerät, das die zu überwachende Kennung nutzt, im Ausland befindet.[396] Ausnahmen gelten, wenn die zu überwachende Telekommunikation an einen im Inland gelegenen Telekommunikationsanschluss oder an eine im Inland befindliche Speichereinrichtung um- oder weitergeleitet wird. Damit ist Telekommunikation dann nicht ausgenommen, wenn sie vom Inland aus über den inländischen Diensteanbieter in ein ausländisches Teilnehmernetz weitergeleitet wird oder wenn SMS, MMS oder Nachrichten in der Mailbox eines „roamenden“[397] Teilnehmers hinterlassen werden.[398]

Das bedeutet für die präventive Telekommunikationsüberwachung, dass diese auch durchgeführt werden kann, wenn sich der potenzielle Störer im Ausland aufhält, er angerufen wird oder Nachrichten per SMS zugeschickt bekommt. Es kommt also darauf an, ob der Datenzugriff im Inland erfolgt.

In die neue TKÜV[399] ist mit § 4 Abs. 2 eine Regelung über die so genannte Auslandskopfüberwachung aufgenommen worden. Mit der Auslandskopfüberwachung soll anhand einer

---

395 So die Bundesregierung in ihrer Antwort auf die kleine Anfrage zur Auslandskopfüberwachung in der TKÜV, vgl. BT-Drucks. 15/5199, S. 3.

396 Die erfolgte Änderung des § 4 TKÜV a.F., die nicht mehr auf das von der überwachten Person genutzte Endgerät abstellt, erklärt sich dadurch, dass die Telekommunikationsanlage prinzipiell nicht erkennen kann, welche Person ein Endgerät nutzt, vgl. BR-Drucks. 631/05, S. 26.

397 Roaming bezeichnet die Nutzung eines Kommunikationsendgerätes oder auch nur die Nutzung der Teilnehmeridentität in einem anderen Netzwerk als dem Heimatnetzwerk. Durch das Einbuchen im besuchten Netz erfährt das Heimatnetz den Standort des Teilnehmers und kann ankommende Gespräche weitervermitteln.

398 Vgl. BR-Drucks. 631/05, S. 23.

399 BGBl. I 2005, S. 3136.

bekannten ausländischen Zielkennung bei Verbindungsaufbau aus dem Inland der Inhalt der Kommunikation oder die Kennung eines Anschlusses ermittelt werden, den eine Zielperson im Inland benutzt.[400] Die Telekommunikation, die von einem inländischen Anschluss an einen ausländischen Anschluss gerichtet ist, wird in der Bundesrepublik durch einen so genannten Auslandskopf[401] zum gesuchten ausländischen Anschluss geleitet. So lässt sich der gesuchte inländische Absenderanschluss feststellen. Die Auslandskopfüberwachung spielt dann eine Rolle, wenn die Anschlusskennung eines inländischen Kommunikationspartners nicht bekannt ist, aber damit gerechnet wird, dass eine Verbindung zu einem bestimmten Anschluss im Ausland aufgebaut werden wird. In diesem Fall steht in Ermangelung einer bekannten inländischen Anschlusskennung, von der aus die Kommunikation erfolgen soll, die Möglichkeit der inländischen Überwachung nicht zur Verfügung. Die gesuchte Kommunikation wird aber unter Angabe der bekannten Zieladresse durch einen Auslandskopf geleitet.[402]

Mit der Auslandskopfüberwachung kann nur die in das Ausland gerichtete, grenzüberschreitende Telekommunikation im Inland überwacht werden. Die übrige Telekommunikation des ausländischen Anschlusses – national, mit sonstigem Ausland, dort abgehend in das Inland– kann mit der Auslandskopfüberwachung nicht erfasst werden. Müssen derartige Verbindungen überwacht werden, besteht die Notwendigkeit eines Rechtshilfeersuchens.[403] Ein solches Rechtshilfeersuchen ist im Fall der Auslandskopfüberwachung gerade nicht notwendig, da eine Überwachung am Auslandskopf im Inland stattfindet und sie sich auf vom Inland in das Ausland aufgebaute grenzüberschreitende Telekommunikationsverbindungen bezieht, wodurch gerade nicht in die Souveränität anderer Staaten eingegriffen wird.[404]

Damit kommt es nicht vorrangig darauf an, wo sich der Telekommunikationsteilnehmer aufhält, sondern wo der Zugriff auf die Telekommunikationsdaten erfolgt. Im Falle des Auslandsaufenthalts des Betroffenen ist danach eine Kommunikationsüberwachung möglich,

---

400 Vgl. BR-Drucks. 631/05, S. 26.

401 Die Zusammenschaltung inländischer mit ausländischen TK-Netzen erfolgt durch Verbindung inländischer Knotenpunkte, sog. Auslandsköpfe, mit ausländischen Knotenpunkten, so BT-Drucks. 15/5199, S. 1.

402 Vgl. BT-Drucks. 15/5199, S. 3.

403 Vgl. BT-Drucks. 15/5199, S. 6.

404 Vgl. BR-Drucks. 631/05, S. 26; BT-Drucks. 15/5199, S. 5.

wenn die Kommunikation im Inland anfällt, weil dann der Zugriff auf diese Telekommunikation durch die Dienstanbieter erfolgt.

3. Outsourcing von Telekommunikationsanlagen

Aufgrund der Internationalisierung von (Telekommunikations-)Unternehmen kommt es häufiger vor, dass Teile von Telekommunikationsanlagen z.B. in ein anderes Land verlegt werden, um von dort die Leistungen der einzelnen nationalen Gesellschaften des Gesamtkonzerns zu erbringen. Hierbei ergeben sich einerseits Probleme, dass eine Überwachungsverpflichtung für die im Ausland betriebenen Telekommunikationsanlagen unter Umständen überhaupt nicht gegeben ist.[405] Abgesehen von den rechtlichen Problemen, ob ein Auskunftsersuchen durchsetzbar ist, können möglicherweise auch enorme Kosten entstehen, wenn die technischen Einrichtungen außerhalb des Geltungsbereichs des TKG liegen.[406]

Betreibt jedoch ein (deutsches) Unternehmen Telekommunikationsanlagen im Ausland oder lässt diese von einem (ausländischen) Dritten betreiben (Outsourcing), so besteht für das Unternehmen grundsätzlich die Verpflichtung aus § 110 Abs. 1, Satz 2 TKG sicherzustellen, dass der Betreiber Anordnungen zur Überwachung der Telekommunikation nach Maßgabe der TKÜV und der Technischen Richtlinie umsetzen kann[407], da es ansonsten für die Diensteanbieter einfach wäre sich ihrer Verantwortung aus § 110 TKG zu entziehen.

II. Der Geltungsbereich von Landesgesetzen

Voraussetzung für eine bundesländerübergreifende Telekommunikationsüberwachung ist, dass mit den landesgesetzlichen Ermächtigungsgrundlagen Regelungen geschaffen wurden, die nicht nur innerhalb der Landesgrenzen gelten, sondern bundesweit Geltung haben. Die Geltung von Landesgesetzen über die Ländergrenzen hinaus ist allerdings ungewohnt, besagt doch das Territorialitätsprinzip als ein allgemein anerkanntes Prinzip des Völkerrechts, dass jeder Staat Hoheitsakte nur wirksam auf seinem eigenen Territorium setzen kann.[408]

---

405 Bock, in: BeckTKG-Komm, § 110 TKG, Rn. 96.
406 Bock, in: BeckTKG-Komm, § 110 TKG, Rn. 98.
407 *Bock*, in: BeckTKG-Komm, § 110 TKG, Rn. 97.
408 Vgl. *K. Ipsen*, 2004, § 23, Rn. 66 ff.; *Buergenthal/Doehring/Kokott/Maier*, 2003, Rn. 327 ff.; *Stein/v.Buttlar*, 2005, Rn. 535 ff.; *Geiger*, 2002, § 45 und § 60 II; *Habscheid/Seidl-Hohenveldern*, in: Seidl-Hohenveldern (Hrsg.), S. 133 ff.

Berücksichtigt werden muss jedoch, dass die Regeln des Völkerrechts im Bundesstaat nur Mindestanforderungen darstellen, die wegen der engeren Integration im Bundesstaat und im Hinblick auf eine stärkere Solidarität zwischen Bund und Ländern sowie zwischen den Ländern, im Gegensatz zu zwischenstaatlichen Beziehungen, überschritten werden können und müssen.[409]

1. Die Beschränkung der Hoheitsgewalt durch die Verbandskompetenz und das Territorialitätsprinzip

In der föderalen Ordnung der Bundesrepublik Deutschland stehen sich Bund und Länder, sowie auch die Länder selbst als selbstständige Verwaltungsträger gegenüber. Den einzelnen Verwaltungsträgern sind eigene Wirkungskreise zur selbstständigen Erledigung ihrer Aufgaben zugewiesen. Diese Aufgabenverteilung und -zuordnung drückt sich in der organisationsrechtlichen Kategorie der Verbandskompetenz aus. Ein zentralisierter Einheitsstaat bedarf dieser Kompetenzzuweisung nicht. Im Verhältnis Bund, Länder, Gemeinden und sonstigen juristischen Personen des öffentlichen Rechts zueinander und untereinander ist sie dagegen von wesentlicher Bedeutung.[410]

Der dem Verwaltungsträger zustehende Aufgabenkreis ordnet diesem nicht nur einen eigenen Wirkungsbereich zu, sondern begrenzt diesen auch gegenüber den übrigen Verwaltungsträgern in seiner Betätigung. Außerhalb seiner Verbandskompetenz ist der Verwaltungsträger zur Aufgabenwahrnehmung nicht befugt; die Schranken seiner Kompetenz sind auch die Schranken seiner rechtlichen Gewalt.[411]

Die Unzulässigkeit kompetenzwidriger Aktivitäten ergibt sich im Verhältnis der Bundesländer nicht unmittelbar aus den Zuweisungen des Grundgesetzes. Art. 30 GG und die ihn konkretisierenden weiteren Kompetenzvorschriften des Grundgesetzes betreffen lediglich die Beziehungen zwischen Bund und Ländern.[412] Aus dem Fehlen entsprechender Kompetenzabgrenzungen zwischen den Bundesländern darf jedoch nicht geschlossen werden, dass solche Verstöße nicht die Verbandskompetenz verletzen können. Das Grundgesetz regelt die

---

409 Vgl. *Bleckmann*, NVwZ 1986, 1 (2); *ders.*,1993, Rn. 1096.
410 Vgl. *Oldiges*, DÖV 1989, 873.
411 Vgl. *Oldiges*, DÖV 1989, 873 (874).
412 Vgl. *Oldiges*, DÖV 1989, 873 (877); *I. Pernice*, in: Dreier (Hrsg.), Art. 30 GG, Rn. 15; *Pieroth*, in: Jarass/Pieroth, Art. 30 GG, Rn. 1.

Verbandskompetenz der Länder nicht ausdrücklich, vielmehr setzt es sie stillschweigend voraus.[413]

Für das Verhältnis zwischen den Bundesländern bedeutet dies, dass die Hoheitsgewalt eines Landes sich grundsätzlich nur auf das eigene Territorium bezieht und es die Landeshoheit nur innerhalb seiner räumlichen Grenzen ausüben darf.[414] Ein Bundesland besitzt damit legislatorische Gewalt nur über seinen eigenen Herrschaftsbereich; außerhalb der Landesgrenzen haben seine Gesetze keine Geltungskraft.[415] Es dürfen keine hoheitlichen Maßnahmen erlassen werden, die sich auf Personen oder Sachverhalte im Hoheitsgebiet eines anderen Bundeslandes beziehen.[416]

Eine Behörde, die Landesrecht auf Landesfremde anwendet, unterwirft ihm Personen, auf die sich sein Geltungsbereich nicht erstreckt. Darin liegt nicht nur ein formeller Rechtsmangel, nämlich die örtliche Unzuständigkeit der Landesbehörde gegenüber einem nicht gebietsansässigen Adressaten, sondern ein materiell-rechtlicher Fehler: Die Anwendung einer personell und territorial auf den Adressaten nicht zugeschnittenen Rechtsnorm verbietet sich ebenso, wie die Anwendung einer Rechtsnorm auf einen von ihr tatbestandlich nicht erfassten Sachverhalt.[417]

2. Der transnationale Verwaltungsakt

Die Überregionalität hoheitlicher Handlungen hat nicht nur Bedeutung für das Verhältnis zwischen Bundesländern. Durch die fortschreitende Europäisierung auf Verwaltungsebene hat dieses Thema auch aktuellen Bezug zur Geltung ausländischer, grenzüberschreitender Verwaltungshandlungen innerhalb von Staaten, also zur Berechtigung von Staaten zur Rege-

---

413 Vgl. *Oldiges*, DÖV 1989, 873 (877).

414 Vgl. BVerfGE 11, 6 (19); *Oldiges*, DÖV 1989, 873 (879); aA wohl *Bleckmann*, NVwZ 1986, 1 (3 ff.).

415 Vgl. *Oldiges*, DÖV 1989, 873 (878); *Ule*, JZ 1961, 622 (623); *Isensee*, in: HStR IV, § 98, Rn. 33.

416 Vgl. *Oldiges*, DÖV 1989, 873 (878).

417 Da die territoriale Beschränkung der Geltung von Landesrecht eine Konsequenz der territorialen Beschränkung der Verbandskompetenz des Landes ist, verstößt auch die Anwendung von Landesrecht auf einen Gebietsfremden gegen die Verbandskompetenz, vgl. *Oldiges*, DÖV 1989, 873 (878); *Mußmann*, 1994, Rn. 112. Zur Gegenauffassung, die die Verbandskompetenz der örtlichen Zuständigkeit zuordnet, vgl. *Drews/Wacke/Vogel/Martens*, 1986, S.111. Die Abgrenzung von örtlicher Zuständigkeit und Verbandskompetenz ist jedoch weitgehend anerkannt. Beim Kompetenzkonflikt zwischen Behörden verschiedener Bundesländer handelt es sich um eine Frage der örtlichen Zuständigkeit, wenn Bundesrecht, und eine Frage der Verbandskompetenz, wenn Landesrecht ausgeführt wird, *H. Meyer*, in: Knack (Hrsg.), Vor § 3 VwVfG, Rn. 3 und 17.

lung von Sachverhalten außerhalb ihres Hoheitsgebietes ohne Zustimmung betroffener anderer Staaten.[418] So verpflichten eine Reihe von EG-Richtlinien die nationalen Behörden, die Verwaltungsentscheidungen anderer Mitgliedstaaten wie eigene anzuerkennen.[419] Diese nationalen Verwaltungsakte haben dann – als Folge dieses Anerkennungsprinzips – nicht mehr nur nationale, sondern über die Staatsgrenzen hinaus reichende Wirkung.[420]

Der transnationale Verwaltungsakt ist eine „Entdeckung" des Europäischen Gemeinschaftsrechts.[421] Entsprechend wird er als Entscheidung definiert, die innerhalb der gesamten Gemeinschaft Wirkungen entfaltet.[422] Aber auch die über das Europarecht hinausreichende Bedeutung wird erkannt, indem er als besonders herausgehobener Tatbestand der grenzüberschreitenden Wirkung fremder Hoheitsakte[423] oder als Verwaltungsakt, dessen Wirkungen

---

418 Vgl. *Neßler*, NVwZ 1995, 863 (864); *Ruffert*, Die Verwaltung 34 (2001), 453 (455). Zur Entwicklung der grenzüberschreitenden internationalen polizeilichen Zusammenarbeit siehe *Baldus*, 2001, S. 31 ff. *Sydow*, 2004, S. 4 f. unterscheidet auf europäischer Ebene zwischen der vertikalen Kooperation der mitgliedstaatlichen Verwaltungen mit der EU-Eigenadministration, der horizontalen Kooperation der mitgliedstaatlichen Verwaltungen untereinander und der diagonalen Kooperation, die die Zusammenarbeit zwischen Behörden eines Mitgliedstaates mit Gerichten eines anderen Mitgliedstaates bezeichnet.

419 Europäische Richtlinien fordern z.B. die gegenseitige Anerkennung von Diplomen und Prüfungszeugnissen (RL 89/48EWG, ABl.EG 1989 Nr. L 19, S. 16), von Zulassungen im Gentechnikrecht (RL 90/220/EWG, ABl.EG 1990, Nr. 117, S. 15) sowie im Banken- (RL 85/611/EWG, ABl.EG 1985 Nr. L 375, S. 3; RL 89/646/EWG, ABl.EG 1989, Nr. L 386, S. 1) und Versicherungsrecht (RL 92/49/EWG, ABl.EG 1992, Nr. L 228, S. 1). Zur dogmatischen Herleitung der aus den Grundfreiheiten begründeten Kooperationspflichten und zur Kooperationsgesetzgebung vgl. *Sydow*, 2004, S. 30 ff. und S. 34 ff. Dieser führt aus, dass eine generelle und undifferenzierte Anerkennungspflicht für administrative Einzelentscheidungen anderer Mitgliedstaaten, die aus den Grundfreiheiten abzuleiten wäre, der Rechtsprechung nicht zu entnehmen ist (S. 30). Inhalt und Ausmaß administrativer Kooperationspflichten sind daher kaum präzise unmittelbar aus dem Primärrecht abzuleiten. Um dauerhaft vollzugsfähige Kooperationsbeziehungen zu etablieren, muss der europäische Gesetzgeber den Inhalt von Kooperationspflichten genau normieren (S. 34).

420 Vgl. *Neßler*, NVwZ 1995, 863 (864). Auf föderaler, nationaler Ebene gilt Vergleichbares: Dem Hoheitsakt eines Landes kommt dann überregionale Wirkung zu, wenn dies ein Bundesgesetz ausdrücklich oder implizit regelt; siehe BVerfGE 11, 6 (19) für den landeseigenen Vollzug von Bundesgesetzen. *Sydow*, 2004, S. 122 ff., unterscheidet beim Vollzug europäischen Rechts vier Modelle: Nach dem *Einzelvollzugsmodell* vollzieht jeder Mitgliedstaat europäisches Recht eigenständig und mit Wirkung allein für sein Hoheitsgebiet (S. 122). Beim *Transnationalitätsmodell* wird im horizontalen Verhältnis der Mitgliedstaaten eine Zentralisierung von Vollzugskompetenzen dadurch erreicht, dass der Vollzug einem einzigen Mitgliedstaat übertragen wird (S. 123). Wirkt die Referenzentscheidung eines Mitgliedstaates nicht ipso iure transnational, sondern wird in den übrigen Mitgliedstaaten einem Anerkennungsverfahren unterworfen, kommt das *Referenzmodell* zum tragen (S. 123). Als grundlegende Unterscheidung im Hinblick auf die drei vorgenannten Modelle ist noch das *Direktvollzugsmodell* zu nennen (S. 123). Es beruht auf originären und umfassenden Verwaltungskompetenzen der Europäischen Kommission oder anderer Behörden der EU-Eigenverwaltung (S. 216).

421 Vgl. *Ruffert*, Die Verwaltung 34 (2001), 453 (456); *Neßler*, 1994, S. 2; *Ehlers*, 1999, S. 9 ff.; *Hufen*, in: Schmidt-Aßmann/Hoffmann-Riem (Hrsg.), S. 99 (109).

422 Vgl. *Ruffert*, Die Verwaltung 34 (2001), 453 (456); *Becker*, DVBl. 2001, 855 (856); *Neßler*, 1994, S. 5; *Schoch*, in: Schmidt-Aßmann/Hoffmann-Riem (Hrsg.), S. 279 (308).

423 Vgl. *Ruffert*, Die Verwaltung 34 (2001), 453 (457); *Schmidt-Aßmann*, DVBl. 1993, 924 (935). Siehe auch *Sydow*, 2004, S. 138 der das völkerrechtliche Territorialitätsprinzip durch das *Transnationalitätsprinzip* durchbrochen sieht.

nicht auf das Staatsgebiet der erlassenen Behörde beschränkt sind[424], bezeichnet wird.[425] *Ruffert*[426] unterscheidet dabei drei Formen transnationaler Verwaltungsakte.

a) Der wirkungsbezogene transnationale Verwaltungsakt

Die erste Erscheinungsform des transnationalen Verwaltungsakts ist der Verwaltungsakt, dessen Transnationalität kraft seiner Rechtswirkungen vermittelt wird (wirkungsbezogener transnationaler VA).[427] So verpflichtet das Wiener Übereinkommen über den Straßenverkehr[428] die Vertragsparteien zur Anerkennung der jeweils von ihnen ausgestellten Führerscheine. Dies hat zur Folge, dass nicht nur derjenige in Deutschland ein Fahrzeug führen darf, der über einen Führerschein nach EG-Recht oder einen internationalen Führerschein verfügt, sondern auch jeder nicht in Deutschland wohnende mit einem gültigen ausländischen Führerschein.[429] Daraus ergibt sich, dass das Regelungsmuster für die wirkungsbezogene Transnationalität von Verwaltungsakten die Kombination aus völkerrechtlicher Anerkennungspflicht verbunden mit einer deutschen Rechtsnorm zum Vollzug der Anerkennung ist.[430]

b) Der adressatenbezogene transnationale Verwaltungsakt

Bei der zweiten Erscheinungsform folgt der transnationale Charakter daraus, dass sich die erlassende Behörde und der Adressat des Verwaltungsakts in unterschiedlichen Staaten befinden (adressatenbezogener transnationaler VA).[431] Diese Verwaltungsakte dringen tiefer in den Bereich der Gebietshoheit ein als diejenigen, deren Transnationalität von ihrer Wirkung herrührt. Von Bedeutung ist dabei, auf welcher Grundlage die Staaten den Übergriff durch

---

424 Vgl. *Ruffert*, Die Verwaltung 34 (2001), 453 (457); *Fastenrath*, Die Verwaltung 31 (1998), 277 (301); ähnlich *Neßler*, 1994, S. 22.

425 Siehe zur Entstehung einer internationalen polizeilichen Zusammenarbeit bereits im 19. Jahrhundert *Baldus*, 2001, S. 31 ff.

426 Vgl. *Ruffert*, Die Verwaltung 34 (2001), 453 ff. Zur transnationalen Wirkung von Rechtsakten vgl. *Neßler*, 1994, S. 10 ff. Die Transnationalität von der im Rahmen des *Transnationalitätsmodells* nach *Sydow* die Rede ist, ist eine wirkungsbezogene Transnationalität. Mit einbezogen werden jedoch auch die behördenbezogene und die adressatenbezogene Transnationalität, vgl. *Sydow*, 2004, S.139, Fn. 3.

427 Vgl. *Ruffert*, Die Verwaltung 34 (2001), 453 (457).

428 Art. 41 mit Anhang 7 des Übereinkommens vom 08.11.1968, BGBl. 1977 II, S. 809.

429 § 4 der deutschen Verordnung über den internationalen Kraftfahrzeugverkehr vom 12.11.1934 (RGBl. I, S. 1137).

430 Vgl. *Ruffert*, Die Verwaltung 34 (2001), 453 (458). Zur Transformation von Völkervertragsrecht in innerstaatliches Recht siehe *Maunz*, in: Maunz/Dürig, Art. 59 GG, Rn. 22 ff.; *Jarass*, in Jarass/Pieroth, Art. 59 GG, Rn. 15 ff.

431 Vgl. *Ruffert*, Die Verwaltung 34 (2001), 453 (464).

transnationale Handlungsformen in ihrem Gebiet zulassen. Beispiel für einen adressatenbezogenen transnationalen Verwaltungsakt ist die Abfallverbringungsgenehmigung[432] nach der Verordnung (EWG) Nr. 259/93[433].[434] Diese wird von der zuständigen Behörde des Bestimmungsstaates gegenüber dem Antragsteller im Versandstaat erteilt.[435] Der Genehmigung geht aber die Beteiligung des Versandstaates am Verfahren und gegebenenfalls eines oder mehrerer Transitstaaten voraus.[436] Rechtfertigende Grundlage für die Transnationalität ist daher die prozedurale Abstimmung der beteiligten Verwaltungen.[437]

c) Der behördenbezogene transnationale Verwaltungsakt

Als dritter Anwendungsfall des transnationalen Verwaltungsakts tritt die Situation hinzu, dass die ausländische Behörde selbst die Staatsgrenze überschreitet, um im Ausland Verwaltungsakte zu erlassen (behördenbezogener transnationaler VA).[438] Dieser transnationaleVerwaltungsakt zählt noch zu den Randerscheinungen, da bislang nur in seltenen Fällen Behörden in anderen Staaten die Kompetenz zum Grenzübertritt eingeräumt wird.[439] So erstreckt das bilaterale polizeirechtliche Abkommen zwischen der Schweiz und Deutschland die Kompetenzen zur Nacheile, verdeckter Ermittlung und grenzüberschreitender Observation auf präventiv-polizeiliche Maßnahmen und ermöglicht so den Erlass transnationaler Verwaltungsakte in Gestalt bestimmter Einzelfallanordnungen.[440]

---

432 Vgl. zur neuen Rechtsprechung des EuGH zur grenzüberschreitenden Abfallverbringung Urteil vom 16.12.2004 in NVwZ 2005, 309 ff.; sowie die Besprechung von *Begemann/Lustermann*, NVwZ 2005, 283 ff.

433 Verordnung (EWG) Nr. 259/93 des Rates vom 01.02.1993 zur Überwachung und Kontrolle der Verbringung von Abfällen in der, in die und aus der Europäischen Gemeinschaft, ABl. EG 1993, Nr. L 30, S. 1.

434 Vgl. *Schröder*, in: FS für Ritter, S. 964 ff.

435 Vgl. Art. 4 Abs. 2 und 5 der Verordnung.

436 Vgl. *Ruffert*, Die Verwaltung 34 (2001), 453 (465). So werden Einwände und Auflagen der anderen Staaten im Sinne einer „Konzentrationswirkung" in die Verbringungsgenehmigung mit einbezogen, vgl. *Schröder*, in: FS Ritter, S. 958. Hier kommt die „Nähe" zwischen der von *Sydow*, 2004, S. 122 begründeten Modelle, des *Transnationalitätsmodells* und des *Referenzmodells* zum Ausdruck. Beide Modelle beruhen auf der Anerkennung einer ausländischen Verwaltungsentscheidung. Sie erfolgt im Rahmen des *Transnationalitätsmodells* durch gesetzliche Anerkennungs- bzw. Geltungserstreckungsklauseln, während sie beim *Referenzmodell* im Einzelfall durch eigenständige Verwaltungsentscheidung ausgesprochen wird, vgl. *Sydow*, 2004, S. 182 f.

437 Vgl. *Ruffert*, Die Verwaltung 34 (2001), 453 (466).

438 Vgl. *Ruffert*, Die Verwaltung 34 (2001), 453 (467).

439 Vgl. *Ruffert*, Die Verwaltung 34 (2001), 453 (467).

440 Vgl. Art. 15; 16 Abs. 1 Nr. 2 und 7 sowie Art. 18 Abs. 1 des Vertrages zwischen der Bundesrepublik Deutschland und der Schweizerischen Eidgenossenschaft über die grenzüberschreitende polizeiliche und justitielle Zusammenarbeit (schweizerisch-deutscher Polizeivertrag) vom 27.04.1999, ratifiziert durch Gesetz vom 25.09.2001, BGBl. II, S. 946.

d) Die Anwendung auf den Bundesstaat

Eine Anerkennungsregelung für den wirkungsbezogenen transnationalen Verwaltungsakt sieht *Ruffert*[441] auf Bundesländerebene nicht gegeben. Für den Vollzug der Bundesgesetze durch die Länder verweist er auf das Postulat einer bundesstaatlich gebotenen gleichmäßigen Gesetzesausführung, die von der auf bundesweiten Vollzug angelegten Geltungskraft der Bundesgesetze getragen wird.[442] Für den Bereich des landeseigenen Vollzuges von Landesgesetzen bleibe es im Grundsatz bei der territorialen Beschränkung der gliedstaatlichen Verwaltungszuständigkeiten auch im Bezug auf die Rechtswirkungen.[443] Diesem angesichts der kleinräumigen Verhältnisse in der Bundesrepublik unbefriedigenden Ergebnis könne aber durch Vereinbarungen zwischen den Ländern und sonstigen Formen der Zusammenarbeit im Zuge des kooperativen Föderalismus abgeholfen werden.[444]

Transnationale Verwaltungsakte im Bundesstaat in der Variante der Überregionalität kraft Adressatenbezugs treten nach *Ruffert* unter Hinweis auf die bundesweit aufgefächerten örtlichen Verwaltungszuständigkeiten nicht auf.[445] Für den behördenbezogenen Verwaltungsakt geht er davon aus, dass die Überschreitung von Landesgrenzen nach dem Vorbild des Musterentwurfes eines einheitlichen Polizeigesetzes erfasst wird.[446]

Zuzustimmen ist *Rufferts* Ausführungen zum wirkungsbezogenen transnationalen Verwaltungsakt. Entgegen *Ruffert* kommt aber ein adressatenbezogener transnationaler Verwaltungsakt in Betracht, wenn es um den Geltungsbereich und Vollzug von Landesgesetzen geht. Anders als beim Vollzug von Bundesgesetzen durch Landesbehörden steht Maßnahmen, die sich allein nach Landesrecht richten, das Territorialitätsprinzip entgegen.[447]

---

441 Vgl. *Ruffert*, Die Verwaltung 31 (2001), 453 (470).

442 Vgl. *Ruffert*, Die Verwaltung 31 (2001), 453 (471). Für die bundesweite Geltung von Landesverwaltungsakten, wenn diese Bundesgesetze ausführen siehe auch *Seibert*, 1989, S. 274 f.; *Henneke*, in: Knack (Hrsg.), § 35 VwVfG, Rn. 8; *Lerche*, in: Maunz/Dürig, Art. 83 GG, Rn. 49 f.

443 *Ruffert*, Die Verwaltung 31 (2001), 453 (471) unter Hinweis auf BVerfGE 11, 6 (19); *Lerche*, in: Maunz/Dürig, Art. 83 GG, Rn. 49.

444 *Ruffert*, Die Verwaltung 31 (2001), 453 (471) unter Hinweis auf *Seibert*, 1989, S. 278 und *Püttner/Rux*, in: Achterberg/Püttner/Würtenberger (Hrsg.), Band I, § 14, Rn. 148 mit dem Beispiel der Anerkennung von Zeugnissen.

445 Vgl. *Ruffert*, Die Verwaltung 31 (2001), 453 (470).

446 Vgl. *Ruffert*, Die Verwaltung 31 (2001), 453 (470).

447 Vgl. *Ule*, JZ 1961, 622 (623); *Isensee*, in: HStR IV, § 98, Rn. 32 f.; aA *Henneke*, in: Knack (Hrsg.), § 35 VwVfG, Rn. 8; *Seibert*, 1989, S. 288, der zu dem Ergebnis kommt, dass Landesverwaltungsakte, die auf Landesrecht basieren, von anderen Ländern als bindend anzuerkennen sind, sofern die rechtlichen Voraussetzungen für den Erlass des Verwaltungsaktes in den betreffenden Ländern gleichwertig sind.

Auch sind für behördenbezogene transnationale Verwaltungsakte die §§ 52; 53 VEME PolG nur bedingt als Rechtsgrundlage geeignet. Zwar ermächtigen sie die Polizeibehörden zum Erlass von Verwaltungsakten gegenüber anderen Bundesbürgern. Nicht aber vermögen sie, die dadurch Betroffenen ihren materiell-rechtlichen polizeilichen Normen zu unterwerfen.

In den Rechtsinstituten der „Nachbarhilfe“ und der „Nacheile“ kommt der Rechtsgedanke zum Ausdruck, dass die Aufgabe der Gefahrenabwehr der strengen Beachtung der Zuständigkeiten vorgeht.[448] Grenzt die verbandsmäßige Zuständigkeit die Kompetenzen der Behörden verschiedener Träger öffentlicher Verwaltung von einander ab, so darf die Aufgabe der Gefahrenabwehr nicht darunter leiden. Die §§ 52; 53 VEME PolG lassen daher Amtshandlungen von Polizeivollzugsbeamten außerhalb des Zuständigkeitsbereiches ihres Landes zu. § 53 Abs. 1 VEME PolG bestimmt, dass

> *„Die Polizeibeamten des Landes ... dürfen im Zuständigkeitsbereich eines anderen Landes oder des Bundes nur in den Fällen des § 52 Abs. 1, Satz 1 und des Artikels 91 Abs. 2 des Grundgesetzes und nur dann tätig werden, wenn das jeweilige Landesrecht oder Bundesrecht es vorsieht.“*

§ 52 Abs. 1, Satz 1 VEME PolG sieht exterritoriale Amtshandlungen vor auf Anforderung oder mit Zustimmung der zuständigen Behörde (Nr.1), in den Fällen der Art. 35 Abs. 2 und 3 und Art. 91 Abs. 1 GG (Nr.2), zur Abwehr einer gegenwärtigen Gefahr, (...) wenn die zuständige Behörde die erforderlichen Maßnahmen nicht rechtzeitig treffen kann (Nr.3), zur Erfüllung polizeilicher Aufgaben bei Transporten (Nr.4), zur Verfolgung von Straftaten und Ordnungswidrigkeiten und zur Gefahrenabwehr in den durch Verwaltungsabkommen mit anderen Ländern geregelten Fällen (Nr.5).

Daran zeigt sich, dass die §§ 52 und 53 VEME PolG nicht geeignet sind, (eigenes) Polizeirecht über die jeweiligen Ländergrenzen hinweg zu verwirklichen. § 52 VEME PolG setzt entweder eine Anforderung oder Zustimmung der zuständigen Behörde oder ein Verwaltungsabkommen zwischen den Ländern voraus, um ein länderübergreifendes Tätigwerden zu legitimieren. Zulässig ist ein grenzüberschreitendes Handeln ansonsten nur in Notfällen und

---

448 Vgl. *Drews/Wacke/Vogel/Martens*, 1986, S. 106; das Rechtsinstitut der Nachbarhilfe ermächtigt jedoch nur die innerhalb eines Bundeslandes örtlich unzuständige Behörde bei Gefahr in Verzug einzuschreiten.

wenn der zuständigen Behörde ein rechtzeitiges Reagieren nicht möglich ist.[449] Deutlich wird die Ungeeignetheit zudem an § 53 Abs. 2 VEME PolG, nach dem das Handeln der an sich nicht zuständigen Behörde dem Einsatzland zugerechnet wird. Folge ist, dass die Polizeibeamten, die nach § 52 Abs. 1 VEME PolG zulässigerweise in einem anderen Bundesland tätig werden, die gleichen Befugnisse (und Pflichten) haben wie dessen eigene Polizeibeamten. Für ihre dort vorgenommenen Amtshandlungen ist daher nicht ihr Heimatrecht maßgebend, sondern das Polizeigesetz und das sonstige Recht des Einsatzlandes.[450]

Die Anordnung der präventiven Telekommunikationsüberwachung als adressatenbezogener transnationaler Verwaltungsakt kommt für die Fälle in Betracht, bei denen Diensteanbieter und/oder Betroffener ihren Sitz/Wohnort in einem anderen Bundesland haben. Für den Einsatz des IMSI-Catchers ist der behördenbezogene Verwaltungsakt heranzuziehen. Über die Rechtsfigur eines transnationalen Verwaltungsakts lässt sich die Anwendung von Landesrecht über die Ländergrenzen hinaus aber nur begründen, wenn entsprechende Absprachen und Vereinbarungen zwischen den Ländern getroffen werden. Denn auch beim transnationalen Verwaltungsakt bedarf die Transnationalität des Rechtsaktes einer verfahrens- oder materiellrechtlichen Grundlage.[451]

Zu diesem Ergebnis kommt auch *R.P. Schenke*[452] für die Frage, ob eine Landespolizeibehörde ein Auskunftsersuchen an einen landesfremden Anbieter stellen kann und inwieweit Auskünfte auch über landesexterne Teilnehmer eingeholt werden können. Die mögliche Qualifizierung der Kommunikationsüberwachung als transnationalen Verwaltungsakt hilft damit für eine länderübergreifende Anwendung nicht weiter.

---

449 § 52 Abs. 1, Satz 1 Nr. 3 VEME PolG beruht auf dem Gedanken der Notzuständigkeit und ermöglicht den Polizeibeamten eines anderen Landes das Einschreiten nur, wenn die zuständige (Landes-)Stelle die erforderlichen polizeilichen Maßnahmen nicht rechtzeitig treffen kann, vgl. *Belz/Mußmann*, § 78 PolG BW, Rn. 4.

450 So für § 78 Abs. 2 PolG BW *Belz/Mußman*, § 78 Rn. 12.

451 So *Ruffert*, Die Verwaltung 31 (2001), 453 (469). Die Pflicht zur Anerkennung der Regelungen eines transnationalen Verwaltungsakts beruhen auf Bestimmungen von in nationales Recht umgesetzten Richtlinien oder unmittelbar auf einer EG-Verordnung, vgl. *Kopp/Ramsauer*, § 35 VwVfG, Rn. 8c; siehe auch *Neßler*, 1994, S. 13 ff. und *Sydow*, 2004, S. 139. Dem von *Sydow* entwickelten *Einzelvollzugsmodell* und dem *Direktvollzugsmodell* kommen hier keine Bedeutung zu, da das *Einzelvollzugsmodell* auf einen Vollzug mit Wirkung allein auf das Hoheitsgebiet des vollziehenden Staates abstellt (S. 127) und das *Direktvollzugsmodell* die Vollziehung von Verwaltungsentscheidungen europäischer Behörden zum Gegenstand hat, die keiner Umsetzung durch die Mitgliedstaaten bedarf (S. 216 f.).

452 Vgl. *R.P. Schenke*, AöR 125 (2000), 1 (17 f.).

III. Die Durchsetzung von Landesgesetzen in anderen Bundesländern

Bundesländer als Bestandteile eines föderativen Bundesstaates können nicht völlig isoliert von einander stehen. Die föderative Praxis der Bundesrepublik lässt daher schlichte Hoheitstätigkeit über die Ländergrenzen hinweg zu, wenn für das länderübergreifende Handeln ein sachgerechter Anknüpfungspunkt vorliegt und das Handeln des einen Landes die Hoheitstätigkeit des anderen nicht stört, auf dessen Gebiet es sich auswirkt.[453]

Die Verbandskompetenz als Voraussetzung für eine auf Landesrecht basierenden Grundverfügung ist gegeben, wenn der Maßnahmeadressat der Staatsgewalt des Landes unterworfen ist. Diese Gewaltunterworfenheit muss dabei nicht immer an den personellen Status des Adressaten als Gebietsansässigen anknüpfen, sondern kann sich auch nach anderen Kriterien, etwa nach dem Prinzip der belegenen Sache, richten.[454]

Unzulässig ist dagegen, dass ein Land auf dem Gebiet eines anderen ohne dessen Zustimmung Vollstreckungsakte oder sonstige Befehls- und Zwangsmaßnahmen trifft, um seinen Gesetzen eigenmächtig auf fremdem Territorium Geltung zu verschaffen.[455] Solche Verwaltungsvollstreckungsmaßnahmen auf fremdem Landesgebiet sind nichtig.[456] Die Vollstreckung ist vom Wohnsitzland des Betroffenen durchzuführen.[457]

Ordnungsverfügungen können zwar gegen landesexterne Störer erlassen werden. Voraussetzung ist aber, dass sie der Staatsgewalt des betroffenen Landes unterworfen sind, weil entsprechende Anknüpfungspunkte durch den Aufenthaltsort der Person oder den Belegenheit-

---

453 Vgl. *Isensee*, in: HStR IV, § 98, Rn. 39.

454 Vgl. *Oldiges*, DÖV 1989, 873 (878). Auch *Ruffert*, Die Verwaltung 31 (2001), 453 (463) sieht vergleichbare Verfügungen mit „Auslandsbezug“ nicht als transnationale Verwaltungsakte an, da diese in völkerrechtskonformer Ausübung der Gebietshoheit ergehen. Gegen den in einem anderen Bundesland wohnenden Grundstückseigentümer kann daher eine Ordnungsverfügung, die ihm die Beseitigung von Gefahren auferlegt, erlassen werden, vgl. *Oldiges*, DÖV 1989, 873 (878). Die postalische Zustellung eines Verwaltungsaktes in ein anderes Bundesland ist in der Regel zulässig, vgl. *Isensee*, in: HStR IV, § 98, Rn. 39. Auch kann ein Platzverweis gegenüber einem Störer ergehen, der in einem andern Bundesland wohnt.

455 Vgl. *Isensee*, in: HStR IV, § 98, Rn. 39; *Hilf*, NVwZ 1987, 537 (543).

456 Vgl. BGH NJW 1970, 1841 (1843).

457 Ist die Behörde zu Zwangsvollstreckungsmaßnahmen nicht befugt, so fällt hierunter lediglich die Anwendung der Zwangsmittel; vorausgehende Maßnahmen wie die Androhung und Festsetzung eines Zwangsmittels sowie die erforderlichen Zustellungen darf die Behörde jedoch selbst treffen, vgl. *Lemke*, 1997, S. 131 f. für die örtlich unzuständige Behörde; aA für den Fall der fehlenden Verbandskompetenz wohl BVerwGE 79, 339 ff.; vgl. auch BGH NJW 1970, 1841 (1843); *Schneider*, § 4 LVwVG, Anm. 6.

sort einer Sache gegeben sind. Die Maßnahme ist dabei stets inlandsbezogen.[458] Die Durchsetzung dieser hoheitlichen Maßnahme kann in einem anderen Bundesland aber nur im Wege der Amtshilfe erfolgen.[459]

Als Lösung für die Problematik der länderübergreifenden Sachverhalte bei Telekommunikationsüberwachungen kann die bundesländerübergreifende Geltung bestimmter Verfügungen nicht dienen. Denn bei der Überwachung der Telekommunikation ist zwischen insgesamt drei Verhältnissen oder Beziehungen zu unterscheiden:

Einmal zwischen Polizei und Telekommunikationsanbieter. Zur Überwachungsermöglichung und Auskunftserteilung ergeht ein Verwaltungsakt der Ordnungsbehörde gegenüber dem Diensteanbieter. Zwischen Polizei und Betroffenem[460] ergeht dagegen gerade keine Ordnungsverfügung. Bei der heimlichen Beobachtung, beim verdeckten Einsatz technischer Mittel und beim Einsatz verdeckter Ermittler ist die Polizei gezielt ohne Wissen des Betroffenen tätig. Ein Verwaltungsakt kann hier schon mangels Bekanntgabe nicht vorliegen. Die Rechtsfigur einer stillschweigenden Duldungsverfügung ist deshalb verfehlt.[461] Vielmehr liegt hier ein regelungsersetzender Realakt vor.[462] Das dritte Verhältnis besteht zwischen Diensteanbieter und Betroffenem, welches rein privatrechtlichter Natur ist und für die Problematik der „Grenzüberschreitung“ keine Relevanz hat.

Es handelt sich bei der Telekommunikationsüberwachung nicht um eine hoheitliche Maßnahme deren Geltungsbereich sich innerhalb der Landesgrenzen hält und lediglich in einem anderen Bundesland vollstreckt werden soll, sondern vielmehr um eine Maßnahme, deren Geltungsbereich sich über die Landesgrenzen erstreckt. Zwar zielen die Anordnung gegenüber den Telekommunikationsunternehmen und die daraus resultierende Überwachungsmöglichkeit oder Information über die Kommunikation des Betroffenen darauf ab, die Möglichkeit einer inlandsbezogenen Maßnahme zu eröffnen. Denn aufgrund der Erkenntnisse aus der Kommunikationsüberwachung sollen Gefahrenabwehrmaßnahmen im Inland getroffen wer-

---

458 Der Platzverweis-Störer hat also einen bestimmten inländischen Bereich zu meiden und der Grundstückseigentümer hat eine Maßnahme an einem inländischen Grundstück vorzunehmen.

459 Vgl. BGH NJW 1970, 1841(1843); *Isensee*, in: HStR IV, § 98, Rn. 40; *Oldiges*, DÖV 1989, 873 (879); *Hilf*, NVwZ 1987, 537 (543).

460 Adressat der Datenerhebung ist die befragte Person; Betroffener derjenige, um dessen Daten es sich handelt, vgl. *Würtenberger/Heckmann*, 2005, Rn. 562. Siehe auch die Legaldefinition in § 3 Abs. 1 BDSG.

461 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 686; *Deutsch*, 1992, S. 279 f.

462 Vgl. BVerwG, NJW 1997, 2534; *Würtenberger/Heckmann*, 2005, Rn. 686.

den.[463] Die Anordnung gegenüber dem Diensteanbieter und die daraus folgende Kommunikationsüberwachung des Betroffenen kann sich aber je nach Unternehmenssitz oder Wohnort in anderen Bundesländern realisieren.

IV. Die Verpflichtung der Telekommunikationsdienstleistungsunternehmen

Die Zugriffsmöglichkeit auch auf landesexterne Telekommunikationsdienstleistungsunternehmen resultiert direkt aus dem TKG. Die §§ 111; 112 Abs. 2 Nr. 2, Abs. 4, Satz 1; 113 Abs. 1 TKG beinhalten Ansprüche für (Landes-)Gefahrenabwehrbehörden, ohne Einschränkungen bezüglich des Unternehmenssitzes oder des Wohnsitzes des Betroffenen. Erforderlich ist nur, dass die Auskünfte zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind.[464] Dies ist der Fall, wenn die Auskünfte zur Gefahrenabwehr im jeweiligen Bundesland benötigt werden.[465] Das Auskunftsverlangen kann daher nicht vom jeweiligen Unternehmenssitz abhängig gemacht werden.

Auch die Auskunftserteilung und die Überwachungsermöglichung können durch Landesgesetz verlangt werden, soweit die übrigen Voraussetzungen des § 88 Abs. 3, Satz 3 TKG erfüllt sind. Eine Beschränkung auf landesinterne Anbieter ist hier ebenfalls nicht angezeigt, da das TKG als Bundesgesetz den Zugriff auf alle Anbieter ermöglicht.[466] Hinzutritt, dass ein landesspezifischer Bezug gegeben ist, da das betroffene Telekommunikationsunternehmen seine Dienste im Inland anbietet[467] und Erkenntnisse zur Gefahrenabwehr im jeweiligen Bundesland gewonnen werden sollen. Auch werden dadurch die anderen Bundesländer nicht beeinträchtigt, weil deren Zugriffsmöglichkeiten erhalten bleibt.[468]

---

463 Polizeiliche Datenerhebung und –verarbeitung stehen in einem engen Verhältnis zur Gefahrenvorsorge, denn die (polizeiliche) Information ist Grundlage und Voraussetzung für jede polizeiliche Tätigkeit, vgl. *Würtenberger/Heckmann*, 2005, Rn. 538.

464 Vgl. § 112 Abs. 2 TKG.

465 Vgl. *Löwnau-Igbal*, in: Scheurle/Mayen (Hrsg.), § 90 TKG, Rn. 14.

466 Vgl. die Formulierungen in § 88 Abs. 2 und § 110 Abs. 6, Satz 1 TKG: „Jeder Betreiber ist verpflichtet...".

467 Vgl. dazu LT-Drucks. Bayern 15/2096, S. 29.

468 Nach § 6 Abs. 4 TKÜV muss der Verpflichtete dafür Sorge tragen, dass die Überwachung für mehrere Bedarfsträger gleichzeitig realisiert werden kann. Sollte das fremde Bundesland also für seine eigene Gefahrenabwehr ebenfalls eine Überwachung des betroffenen Telefonanschlusses durchführen wollen, so würde diese hoheitliche Maßnahme nicht durch die Überwachung eines anderen Hoheitsträgers beeinträchtigt, siehe dazu *I.M. Pernice*, DuD 2002, 207 (209).

Setzt § 88 Abs. 3, Satz 3 TKG ein Gesetz voraus, aufgrund dessen die Überwachung der Telekommunikation verlangt werden kann, so ist damit keine Aussage über den betroffenen Personenkreis getroffen.[469] Wer als Betroffener der Überwachung unterfällt, ergibt sich aus den Anordnungsgesetzen.[470] Aufgrund der landesgesetzlichen Regelungen ist die Überwachung eines Störers dann unabhängig davon möglich, wo er sich aufhält oder sich sein Kommunikationsanschluss befindet, wenn den Landesnormen, die die Telekommunikationsüberwachung regeln, bundesweite Geltung zukommen.[471]

V. Die bundesweite Geltung von Landesgesetzen

Bislang hat sich die Rechtsprechung selten mit der Problematik „länderübergreifender Sachverhalte“ beziehungsweise dem Geltungsbereich von Landesgesetzen beschäftigt.[472]

1. Die Entscheidung des BVerwG zur bundesweiten Zeugenpflicht vor Landesuntersuchungsausschüssen

Von Bedeutung ist die Entscheidung des BVerwG über das Bestehen einer bundesweiten Zeugenpflicht vor Landesuntersuchungsausschüssen.[473] Dieser Entscheidung lag der Sachverhalt zugrunde, dass der 10. Parlamentarische Untersuchungsausschuss des Niedersächsischen Landtags einen in Baden-Württemberg lebenden Zeugen vernehmen wollte. Dieser blieb den Ladungen zu den Ausschusssitzungen fern, worauf der Untersuchungsausschuss ihm die durch sein Ausbleiben verursachten Kosten auferlegte und gleichzeitig ein Ord-

---

469 Bei den §§ 112; 113 TKG ergibt sich dies aus der Eigenschaft der Betroffenen als Kunden des jeweiligen Anbieters. Ob der Auskunftsfordernde dabei über den betroffenen Kunden tatsächlich Auskunft verlangen kann, wird von der Regulierungsbehörde grundsätzlich nicht überprüft, § 112 Abs. 4, Sätze 2 und 3 TKG.

470 Die Möglichkeit einer Überwachung landesexterner Betroffener erwähnt auch nicht die bayerische Gesetzesbegründung.

471 Würde das Telekommunikationsunternehmen die Überwachung der Telekommunikation ermöglichen, obwohl der Betroffene nicht unter den Geltungsbereich des Anordnungsgesetzes fällt, können Ansprüche gegen den Diensteanbieter bestehen. Denkbar sind dabei Unterlassungs- und auch Schadensersatzansprüche; vgl. *Trute* in: Trute/Spoerr/Bosch, § 85 TKG, Rn. 29 ff; *Zerres* in Scheurle/Mayen (Hrsg.), § 85 TKG, Rn. 47. Ansprüche des Betroffenen ergeben sich zudem aus § 44 Abs. 1 TKG. Schadensersatzansprüche dürften aber ausscheiden, solange das Gesetz den formalen Anforderungen des § 88 Abs. 3, Satz 3 TKG entspricht, da es dann an einem entsprechenden Verschulden des Telekommunikationsunternehmens fehlen dürfte, denn die Zulässigkeit der Anordnungmaßnahmen hat der Betreiber nicht zu überprüfen; so *Meyer-Goßner*, § 100 b StPO, Rn. 5 für die Überwachung nach § 100 a StPO.

472 Vgl. BVerfG NVwZ 1994, 54 ff.; BVerfGE 11, 6 ff.; BVerwGE 22, 229 ff.; E 79, 339 ff.; OVG Lüneburg DVBl. 1986, 476 ff.; VG Hannover NJW 1988, 1928 ff.

473 BVerwGE 79, 339 ff.

nungsgeld, ersatzweise Ordnungshaft, festsetzte. Als der Zeuge wiederum nicht erschien, beschloss der Untersuchungsausschuss dessen Vorführung.[474]

Das daraufhin angerufene Verwaltungsgericht Hannover hat den Beschluss des Untersuchungsausschusses aufgehoben, soweit Ordnungsgeld und Ersatzordnungshaft gegen den Zeugen festgesetzt waren, und im Übrigen die Klage abgewiesen.[475] Das Gericht hat die Aussagepflicht des Zeugen vor dem niedersächsischen Untersuchungsausschuss bejaht, da eine sachlich begründete Anknüpfung vorhanden sei, wenn das niedersächsische Verfassungsrecht eine Zeugnispflicht an der Kenntnis von Tatsachen festmache, die für eine Untersuchung wesentlich seien. Durchzusetzen sei eine solche landesrechtlich begründete Aussagepflicht in anderen Bundesländern allerdings nur im Wege der Amts- und Rechtshilfe. Geltung und Vollzug seien zu trennen.[476]

Das Oberverwaltungsgericht Lüneburg hat der daraufhin eingelegten Berufung des Klägers stattgegeben,[477] da Art. 11 Abs. 4, Satz 1 Nds.Verf.[478] und die Vorschriften über den Strafprozess Zeugenpflichten nur gegenüber solchen Personen begründen könnten, die der niedersächsischen Landesstaatsgewalt, dem räumlichen Machtbereich des Landes Niedersachsen unterworfen seien.[479]

Nach Ansicht des Berufungsgerichts wird das innere Verhältnis des Bundesstaates nach dem Recht des Grundgesetzes ausschließlich durch das geltende Bundesverfassungsrecht bestimmt[480], wobei bei Beziehungen der Bundesländer untereinander die Grundsätze des Völkerrechts zur Ermittlung des Inhalts des Bundesverfassungsrechts in diesem Zusammenhang heranzuziehen seien.[481] Zu beachten sei dabei vor allem der Unterschied zwischen extra-

---

474 Vgl. OVG Lüneburg DVBl. 1986, 476.
475 Vgl. Urteil des VG Hannover vom 24.10.1985, AZ: 6 A 130/85.
476 Vgl. VG Hannover Urteil vom 24.10.1985, AZ: 6 A 130/85, S. 14 f., *Hilf*, NVwZ 1987, 537 (542).
477 OVG Lüneburg DVBl. 1986, 476.
478 Art. 11 Abs.4, Satz 1 Nds.Verf. (vorläufige) lautete: „Auf die Erhebungen der Ausschüsse und der von ihnen ersuchten Behörden finden die Vorschriften über den Strafprozess Anwendung.“ Die vorläufige Verfassung vom 13.04.1951 ist aufgrund der Niedersächsischen Verfassung vom 19.05.1993 außer Kraft getreten.
479 Vgl. OLG Lüneburg, DVBl. 1986, 476 (477).
480 Vgl. OLG Lüneburg, DVBl. 1986, 476 (477) unter Hinweis auf BVerfGE 34, 216 (231).
481 Vgl. OLG Lüneburg, DVBl. 1986, 476 (477).

territorialem Recht[482] und der territorialen Rechtserstreckung durch die Erweiterung des räumlichen Geltungsbereichs.

Die Frage, ob Zeugenpflichten für alle Bundesbürger gegenüber Untersuchungsausschüssen eines Landtags bestehen, sei eine Frage territorialer Erstreckung niedersächsischen Rechts. Eine entsprechende landesrechtliche Regelung bedürfe daher eines Rechtstitels, der durch einen Staatsvertrag geschaffen werden könne.[483]

Die Revision führte zur Wiederherstellung des erstinstanzlichen Urteils durch das BverwG mit der Begründung, dass ein Bundesland in seiner Gesetzgebungshoheit zwar grundsätzlich auf sein eigenes Gebiet beschränkt sei,[484] sich die Bundesländer aber über die Landesgrenzen hinweg als Einheit behandeln lassen müssten und dies mutatis mutandis auch für die Bundesbürger gelte.[485] Dieser aus dem bundesstaatlichen Charakter der Bundesrepublik Deutschland in der spezifischen Ausprägung des Grundgesetzes fließende Grundsatz komme nicht nur in Art. 33 Abs. 1 GG zum Ausdruck, sondern dieser Grundsatz schlage sich weiter in Art. 35 Abs. 1 GG nieder.[486] Die Beschränkungen der Landesstaatsgewalt auf das Landesgebiet könne dem Grundgesetz nicht ohne weiteres entnommen werden.[487] Denn es gebe keine Vorschrift im Grundgesetz, nach der die Staatsgewalt eines Landes nur in seinem Gebiet ausgeübt werden könne und bei einer Ausdehnung der Zuständigkeit auf das ganze Bundesgebiet nur der Bund zuständig wäre.[488] Eine generelle Beschränkung könne insbesondere dann nicht angenommen werden, wenn es, wie im zu entscheidenden Fall, nicht darum gehe, die Geltung eines Landesgesetzes – in einer die Staatsgewalt der anderen Bundesländer beeinträchtigenden Weise – über die Landesgrenzen hinaus zu erstrecken, sondern lediglich um die Möglichkeit, das auf den Landesbereich beschränkte Gesetz wirksam zu vollziehen.[489] Über die Tätigkeit von Untersuchungsausschüssen hinaus lasse sich generell sagen, dass der

---

482 Dabei regelt der Gesetzgeber Sachverhalte mit Auslandsberührung und wendet nationale Rechtsvorschriften im Inland in Bezug auf Tatbestände an, die sich zwar im Ausland ereignet haben, aber einen Inlandsbezug aufweisen und deswegen Rechtsfolgen im Inland zeitigen sollen, vgl. OVG Lüneburg DVBl. 1986, 476 (477 f.); siehe auch *Geiger*, 2002, § 52 I.

483 Vgl. OLG Lüneburg, DVBl. 1986, 476 (478).

484 Vgl. BVerwGE 79, 339 (341).

485 Vgl. BVerwGE 79, 339 (342) unter Hinweis auf BVerfGE 33, 303 (358).

486 Vgl. BVerwGE 79, 339 (342).

487 Vgl. BVerwGE 79, 339 (342) unter Hinweis auf BVerwGE 22, 299.

488 Vgl. BVerwGE 22, 299 (307).

489 Vgl. BVerwGE 79, 339 (342); *Hilf*, NVwZ 1987, 537 (543); *Arloth*, NJW 1987, 808 (810).

im Landesbereich wurzelnde Regelungsgegenstand für Vollzug und Verwirklichung Auswirkungen, die die Landesgrenzen überschreiten, durchaus entfalten kann.[490]

Das Urteil des BVerwG zur bundesweiten Zeugenpflicht vor Landesuntersuchungsausschüssen ist nur bedingt geeignet, die Erstreckung von Landesrecht über die Ländergrenzen hinaus zu begründen. Denn bei der Zeugenpflicht von Bundesbürgern vor Landesuntersuchungsausschüssen ging es nicht um die *Erstreckung* von Landesrecht, sondern um dessen *Vollstreckung*. Lediglich in einem Nebensatz hat das BVerwG zu erkennen gegeben, dass eine Erstreckung möglich ist, wenn die Staatsgewalt anderer (Bundes-)Länder nicht beeinträchtigt wird und der Regelungsgegenstand im Landesbereich wurzelt.[491]

2. Die präventive Telekommunikationsüberwachung als extra-territoriales Recht?

Handelt es sich bei extra-territorialem Recht um die Anwendung von nationalen Rechtsvorschriften im Inland in Bezug auf Tatbestände, die sich zwar im Ausland ereignet haben, aber einen Inlandsbezug aufweisen und deswegen Rechtsfolgen im Inland zeitigen sollen,[492] so zeigt sich, dass diese Merkmale nicht auf den Fall der präventiven Telekommunikationsüberwachung passen.

Zwar sollen durch die Überwachung der Telekommunikation, die in einem anderen Bundesland stattfindet, Erkenntnisse gesammelt werden, die dann zu einer Gefahrenabwehr im Inland führen. Dabei ist jedoch die unter III. dargestellte Differenzierung zu beachten:

Rechtsfolgen der Anordnung sind zunächst die Überwachungsermöglichung sowie die Auskunftserteilung durch die Telekommunikationsunternehmen. Die daraus gewonnenen Informationen bilden die Grundlage, um weitere Anordnungen in Bezug auf eine Gefahrenbeseitigung treffen zu können, die dann zur Gefahrenabwehr im Inland führt. Abzustellen ist hier auf die Zugriffsmöglichkeiten auf die Kommunikation in einem anderen Bundesland. Diese Maßnahmen führen zu Rechtsfolgen mit Bezug auf die Hoheitsgebiete anderer Bundesländer,

---

490 Vgl. BVerwGE 79, 339 (343).

491 Vgl. BVerwGE 79, 339 (342, 343).

492 Vgl. OVG Lüneburg, DVBl. 1986, S. 476 (477 f.). So besteuert die Bundesrepublik die auf ihrem Gebiet ansässigen Personen mit ihrem Welteinkommen. Das bedeutet, dass eine Steuerpflicht im Inland auch besteht, wenn sich der Steuertatbestand im Ausland verwirklicht hat, vgl. *Geiger*, 2002, § 52 II.

wenn die Diensteanbieter ihren Sitz und/oder die Betroffenen ihren Kommunikationsanschluss in diesem Bundesland haben.

Die präventive Telekommunikationsüberwachung ist nicht als extra-territoriales Recht zu qualifizieren, da keine inländischen Sachverhalte mit Auslandsberührung geregelt werden. Vielmehr handelt es sich bei diesen Regelungen um die territoriale Erstreckung des jeweiligen Polizeigesetzes über die Landesgrenzen hinweg.[493]

3. Die Voraussetzungen der bundesweiten Geltung

Geprüft wird im Folgenden, ob die Voraussetzungen für die bundesweite Geltung einer landesgesetzlich geregelten Telekommunikationsüberwachung bei den hier untersuchten Polizeigesetzen vorliegen.

a) Regelungsgegenstand

Regelungsgegenstand der präventiv-polizeilichen Telefonüberwachung ist die effektive Gefahrenabwehr im Inland, welcher damit einen spezifischen landesrechtlichen Bezug aufweist.[494] Die mit der Telekommunikationsüberwachung bezweckte Gefahrenabwehr bezieht sich nicht auf eine Abwehr von Gefahren in anderen Bundesländern.

b) Keine Beeinträchtigung fremder Hoheitsgewalt

Haben sich andere Bundesländer entschieden, eine Kommunikationsüberwachung zu präventiven Zwecken nicht zuzulassen, fragt sich, ob eine Beeinträchtigung ihrer Hoheitsgewalt darin liegt, dass eine Überwachung ihrer Einwohner dennoch stattfinden kann.

---

493 Zwischen der exterritorialen Wirkung von Hoheitsakten und einem transnationalen VA besteht keine Identität. Exterritoriale Wirkung von Hoheitsakten bedeutet die Berechtigung der Staaten zur Regelung von Sachverhalten außerhalb ihres Hoheitsgebiets ohne Zustimmung betroffener Staaten und die völkerrechtlichen Grenzen dieser Berechtigung, vgl. *Geiger,* 2002, § 52 I; *Ruffert*, Die Verwaltung 34 (2001), 453 (455). Kennzeichnend für den transnationalen VA ist, dass seine Wirkungen nicht auf das Staatsgebiet der erlassenden Behörde beschränkt sind, sondern dieses überschreiten. Extraterritorialität und Transnationalität sind dabei keine Eigenschaften von Verwaltungsakten, die einander widersprechen, sondern Charakteristika grenzüberschreitenden hoheitlichen Handelns, die jeweils aus einer bestimmten Perspektive in den Vordergrund treten, vgl. *Ruffert*, Die Verwaltung 34 (2001), 453 (455).

494 So jedenfalls LT-Drucks. Nds. 15/240: „Das Niedersächsische Gefahrenabwehrgesetz soll mit dem Ziel geändert werden, der Polizei und den Gefahrenabwehrbehörden ein verbessertes Instrumentarium zur Verfügung zu stellen, um die Sicherheit der Bürger und Bürgerinnen in Niedersachsen gewährleisten zu können."

aa) Die Bundestreue

Wie bereits erwähnt, können die einzelnen Bundesländer aufgrund ihrer Stellung als Gliedstaaten der Bundesrepublik Deutschland nicht isoliert von einander betrachtet werden. So hat das BVerfG bereits in seinem ersten Entscheidungsband klar gestellt, dass der Grundsatz „bundesfreundlichen Verhaltens" alle an dem verfassungsrechtlichen Bündnis Beteiligten bindet und daher sowohl im Verhältnis des Bundes zu den Ländern als auch im Verhältnis zu den Ländern untereinander Geltung beansprucht und zwar jeweils gegenseitig und mit dem Ziel des Zusammenwirkens, der Verständigung, der Rücksichtnahme, der Wahrung der wohlverstandenen Belange der Beteiligten sowie der Festigung des „Bündnisses".[495] In seinem „Fernsehurteil" hat das BVerfG die Formel aufgestellt: „Im deutschen Bundesstaat wird das gesamte verfassungsrechtliche Verhältnis zwischen dem Gesamtstaat und seinen Gliedern sowie das verfassungsrechtliche Verhältnis zwischen den Gliedern durch den ungeschriebenen Verfassungsgrundsatz von der wechselseitigen Pflicht des Bundes und der Länder zu bundesfreundlichem Verhalten beherrscht".[496]

Die Bundestreue kann als eine normative Ableitung und gleichzeitig als bereichsspezifische Ausprägung des allgemeinen Rechtsprinzips von Treu und Glauben betrachtet werden.[497] Aus dieser Perspektive konkretisiert sie das abstrakte Normenprogramm von Treu und Glauben entsprechend dem zwischen Bund und Ländern bestehenden „eigentümlichen Grundverhältnis"[498] unter den Vorgaben der grundgesetzlichen Ordnung.[499]

---

495 Vgl. BVerfGE 1, 299 (315); siehe auch *Bauer*, in: Dreier (Hrsg.), Art.20 GG (Bundesstaat), Rn. 39, *Sommermann*, in: v.Mangoldt/Klein/Starck (Hrsg.), Art. 20 Abs. 1 GG, Rn. 37; *Stern*, Staatsrecht, Band I, S. 699. Das BVerfG begreift die Bundestreue gleichsam aus sich selbst heraus als einen „das gesamte verfassungsrechtliche Verhältnis zwischen dem Gesamtstaat und seinen Gliedern sowie das verfassungsrechtliche Verhältnis zwischen den Gliedern beherrschenden Grundsatz", vgl. BVerfGE 12, 205 (254). Zu den von der Literatur entwickelten bundesstaatlichen Ordnungsmodellen, vgl. *Bauer*, 1992, S. 129 ff.

496 Vgl. BVerfGE 12, 205 (254).

497 Vgl. *Lorz*, 2001, S. 26; *Bauer*, in: Dreier (Hrsg.), Art. 20 GG (Bundeststaat), Rn. 39; vgl. *ders.*, 1992, S. 243. Nach *Bauer*, 1992, scheiden die Zusammenschau von Einzelaspekten, S. 235 ff., Gewohnheitsrecht, S. 237 ff. und rechtsstaatliche Grundsätze, S. 239 ff. als Rechtsgrundlagen aus. Bei Treu und Glauben handelt es sich zwar um einen allgemeinen Rechtsgrundsatz, der im Zivilrecht einen besonderen Ausdruck im geschriebenen Recht gefunden hat, als ungeschriebenes Recht aber in der gesamten Rechtsordnung Geltung beanspruchen kann, vgl. *Bauer*, 1992, S. 245; *Sachs*, in: Sachs (Hrsg.), Art. 20 GG, Rn. 68. Das BVerfG hat den Grundsatz der Bundestreue „aus dem Wesen des Bundesstaates entwickelt" (vgl. E 8, 122/138), er „entspringt dem eigentümlichen Grundverhältnis von Gesamtstaaten und Gliedstaaten im Bundesstaat" (vgl. E 31 314/354) und dem „bundesstaatlichen Prinzip" (E 34, 9/20).

498 Vgl. BVerfGE 31, 314 (354).

499 *Lorz*, 2001, S. 27. So vor allem die Sicht von *Bauer*, 1992, S. 252 f.; vgl. auch *Isensee*, in: HStR IV, § 98, Rn. 157 ff.

Das damit weitgezogene und überdies der Weiterentwicklung zugängliche Normenprogramm der Bundestreue wird für seine Handhabung und Handhabbarkeit in der Rechtspraxis[500] dadurch konkretisiert, dass zwischen der Bundestreue im allgemeinen und deren Einzelausprägungen unterschieden wird.[501] Während die Bundestreue im allgemeinen den Bund und die Länder in permanenter bundesstaatlicher Verbindung zu einer Schicksalsgemeinschaft zusammen schließt[502], ergeben sich aus den Einzelausprägungen als besondere Rechtsverhältnisse Rechte und Pflichten, die auf Verfassung, Gesetz oder auch Vertrag beruhen.[503]

Fasst man die in der verfassungsgerichtlichen Rechtsprechung bislang gefundenen Konkretisierungsergebnisse der Bundestreue zusammen, so ergibt sich zunächst eine Typologie spezifischer Pflichten, die das BVerfG dem Prinzip der Bundestreue entnimmt:[504]

(1) Die pflichtenbegründende Funktion

Es ist dies zunächst die Pflicht zu gegenseitiger Hilfeleistung, Rücksichtnahme und Verständigungsbereitschaft. Die Bundestreue beinhaltet damit vornehmlich den Grundgedanken der solidarischen Verbundenheit von Bund und Ländern.[505]

Da der Bund und die Länder zu einer Schicksalsgemeinschaft verbunden sind, die nur funktionsfähig ist, wenn sich die Beteiligten über Ereignisse und Vorhaben, die für die jeweils anderen von Belang sind, frühzeitig wechselseitig in Kenntnis setzen und sich gemeinsam beraten, lässt sich aus der bundesstaatlichen Ordnung eine Verpflichtung zur Information und Konsultation ableiten.[506] Beispiele für diese Informationspflichten sind etwa die Verpflich-

---

500 Vgl. bspw. BVerfGE 21, 312 (326).

501 Vgl. *Bauer*, 1992, S. 147. So im Ergebnis auch *Lorz*, 2001, S. 29, der ausführt, dass die Bundestreue in der Regel immer nur im Rahmen eines konkreten verfassungsrechtlichen Verhältnisses zur Wirksamkeit gelangt.

502 Vgl. BVerfGE 72, 330 (419) „politische Schicksalsgemeinschaft des Bundesstaates".

503 Vgl. *Bauer*, 1992, S. 305 ff; *Stern*, Staatsrecht, Band I, S. 702.

504 Vgl. *Lorz*, 2001, S. 31 ff; *Isensee*, in: HStR IV, § 98, Rn. 158 ff. und *Stern*, Staatsrecht, Band I, S. 702 unterscheiden zwischen Handlungs- und Unterlassungspflichten. Siehe dazu auch *Bauer*, 1992, S. 327 ff., der zunächst zwischen dem sachlichen Anwendungsbereich der Bundestreue, ihrer Typologie und den sonstigen allgemeinen Anwendungsmodalitäten unterscheidet. Bei den typischen Erscheinungsformen werden im Wesentlichen drei Funktionen unterschieden: die pflichtenbegründende Funktion, die rechtsbeschränkende Funktion und die Funktion, ergänzende Regelungen für das Vertragsrecht bereit zu stellen, vgl. *Bauer*, 1992, S. 334.

505 Vgl. *Bauer*, 1992, S. 343; *Lorz*, 2001, S. 31. Beispiele hierfür sind der horizontale und vertikale Finanzausgleich, siehe z.B. BVerfGE 72, 330 ff., die Rechts- und Amtshilfe sowie Unterstützungsleistungen bei Katastrophenfällen nach Art. 35 GG.

506 Vgl. *Bauer*, 1992, S. 346; *Sachs*, in: Sachs (Hrsg.), Art. 20 GG, Rn. 71.

tungen des Bundes zur Unterrichtung der Länder im Zusammenhang mit dem Abschluss völkerrechtlicher Verträge, die wesentliche Interessen des Bundes berühren.[507] Im Verhältnis der Länder untereinander bestehen Informations-, aber auch Warn- und Hinweispflichten u.a. dann, wenn „die Auswirkungen einer gesetzlichen Regelung nicht auf den Raum des (eigenen) Landes begrenzt sind".[508]

Weiter ist das allgemeine Gebot zur Abstimmung und Zusammenarbeit in der Bundestreue angelegt. Wesentliche Konkretisierungen daraus sind Verpflichtungen zur Abstimmung und Zusammenarbeit, die zur Deckung des Koordinations- und Kooperationsbedarfs in der bundesstaatlichen Ordnung des Grundgesetzes beitragen. Diese Abstimmung und Zusammenarbeit beinhaltet exemplarisch ein positives Zusammenwirken der Beteiligten, vorherige Zustimmungseinholung und Kompromißbereitschaft.[509] Als Beispiel kann die grenzüberschreitende Regionalplanung dienen, bei der die notwendigen Maßnahmen in gegenseitigem Einverständnis mit den anderen beteiligten Ländern zu treffen sind.[510] Jedoch verlangt der Grundsatz des bundesfreundlichen Verhaltens keinesfalls eine allgemeine Vorabstimmung bei Einführung neuer Regelungen[511] oder einen völlig unitaristischen Gesetzesvollzug.[512]

Des Weiteren ergeben sich aus der Bundestreue Anforderungen für das Prozedere und den Umgangsstil zwischen dem Bund und den Ländern. Der Bund darf bei Verhandlungen, an denen alle Länder interessiert sind, nicht ein Verfahren einschlagen, das einzelne Länder ausschließt oder sonst benachteiligt.[513] Daneben dürfen die Länder nicht durch willkürlich-obstruktives Verhalten in Verhandlungen gemeinsam zu treffende Entscheidungen blockieren oder ihre Kooperation ausschließlich parteipolitischen Zielen dienstbar machen und durch entsprechend motivierte Sonderbündnisse bei Angelegenheiten von überregionaler Bedeutung ein betroffenes Land in eine Außenseiterrolle abdrängen.[514]

---

507 Vgl. Nr. 4 lit. a des Lindauer Abkommens vom 14.11.1957 (Textabdruck bei *I. Pernice*, in: Dreier (Hrsg.), Art. 32 GG, Rn. 48), wonach bei solchen Verträgen „die Länder möglichst frühzeitig über den beabsichtigten Abschluss derartiger Verträge unterrichtet werden".

508 Vgl. BVerfGE 4, 115 (140); *Lorz*, 2001, S. 28; *Felix*, 1998, S. 367; *Bauer*, 1992, S. 348; *Steinberger*, NJW 1987, 2345 (2348).

509 Vgl. *Bauer*, S. 347 ff.; *Lorz*, 2001, S. 31 ff.; vgl. BVerfGE 73, 118 (196 f.); kritisch *Schmitt Glaeser/Degenhart*, AfP 17 (1986), S.173 ff. *Rudolf/Jutzi*, ZRP 1987, S. 2 ff.

510 Vgl. § 4 Abs. 4, § 5 Abs. 3 Satz 3 ROG.

511 Vgl. BVerfGE 32, 199 (219 f.); E 45, 400 (421); *Stern*, Staatsrecht, Band I, S. 703.

512 Vgl. BVerfGE 76, 1 (77 f.).

513 Vgl. BVerfGE 12, 205 (206 LS 9, 255); E 81, 310 (337 f.); *Stern*, Staatsrecht, Band I, S. 703.

514 Vgl. *Bauer*, 1992, S. 353, 354; vgl. *Isensee*, in: HStR IV, § 98, Rn. 144.

Zu den weiteren Verhaltenspflichten zählen u.a. die Schutzpflichten des Bundes zugunsten der Länder gegenüber auswärtigen Staaten und supranationalen Institutionen der Europäischen Gemeinschaften.[515]

(2) Die rechtsbeschränkende Funktion

Der Grundsatz bundesfreundlichen Verhaltens verpflichtet Bund und Länder aber auch bei der Inanspruchnahme ihrer Rechte die gebotene Rücksicht auf die Belange der anderen Mitglieder der bundesstaatlichen Rechtsverhältnisse zu nehmen und nicht egoistisch auf die einseitige Durchsetzung eigener Rechtspositionen zu pochen.[516] Diese rechtsbeschränkenden Konkretisierungen[517] der Bundestreue beinhalten vor allem das Rechtsmißbrauchsverbot und das Verbot widersprüchlichen Verhaltens. Rechtsfolge der rechtsbeschränkenden Tatbestände ist die zumindest zeitweilige unzulässige Rechtsausübung.[518]

Das Rechtsmißbrauchsverbot verhindert, dass Bund und Länder kraft der ihnen eingeräumten Befugnisse rücksichtslos ihre eigenen Vorstellungen verwirklichen und nur ihren eigenen Interessen folgen, indem es jede Rechtsausübung unter den immanenten Vorbehalt der Berücksichtigung der Belange der anderen Beteiligten des jeweiligen bundesstaatlichen Rechtsverhältnisses stellt.[519]

In Anlehnung an anderweitige Beschäftigungen mit dem Verbot mißbräuchlicher Rechtsausübung[520] wird dieser Ausnahmetatbestand für das Bundesstaatsrecht dahingehend präzisiert, dass die Ausübung eines Rechts unzulässig sein kann, wenn der Rechtsinhaber keine berechtigten Interessen verfolgt oder überwiegende Belange der anderen Beteiligten entgegenstehen und die Rechtsausübung zu einer gravierenden Störung der bundesstaatlichen Ordnung führen würde.[521]

---

515 Vgl. *Bauer*, 1992, S. 354.

516 Vgl. BVerfGE 34, 216 (232); BVerwGE 50, 137 (148).

517 In den rechtsbeschränkenden Konkretisierungen wird von *Karpen/v.Rönn*, JZ 1990, 579 (584): die größte Bedeutung des Grundsatzes der Bundestreue gesehen. So auch *Stern*, Staatsrecht, Band I, S. 703.

518 Vgl. *Bauer*, 1992, S. 356; *ders.*, in: Dreier (Hrsg.), Art. 20 GG (Bundeststaat), Rn. 43; *Sachs*, in: Sachs (Hrsg.) Art. 20 GG, Rn. 70.

519 Vgl. BVerfGE 34, 216 (232); *Bauer*, 1992, S. 356; *Isensee*, in: HStR IV, § 98, Rn. 157 f.

520 Siehe zum Zivilrecht etwa *Mansel*, in: Jauernig (Hrsg.), § 242 BGB, Rn. 32 ff.

521 Vgl. *Bauer*, 1992, S. 357. Beispiele sind Rechtsausübungen die zu einer „Erschütterung des gesamten Finanzgefüges von Bund und Ländern führen“, vgl. BVerfGE 4, 115 (140).

Auch kann die Rechtsausübung unzulässig sein, wenn sich der Rechtsinhaber mit ihr in Widerspruch zu seinem eigenen Vorverhalten setzt.[522]

(3) Die Funktion, ergänzende Regelungen für das Vertragsrecht bereit zu stellen

Die Bundestreue wird seit langem auch mit dem Komplex „Verträge im Bundesstaat" in Verbindung gebracht und dabei als Ansatzpunkt zur Gewinnung ergänzender Regeln für das intraföderative Vertragsrechts verwendet.[523] Außerdem entnimmt man dem Grundsatz bundesfreundlichen Verhaltens die Einschränkung des Satzes „Pacta sunt servanda" durch die „clausula rebus sic stantibus", die unter bestimmten Voraussetzungen eine Vertragsanpassung an grundlegend veränderte Verhältnisse ermöglicht.[524]

bb) Der Anwendungsbereich der Bundestreue

Der sachliche Anwendungsbereich der Bundestreue gilt zunächst für jede Maßnahme des Bundes und der Länder.[525] Besondere Bedeutung kommt jedoch der Gesetzgebung zu. Dabei beeinflusst die Bundestreue nicht nur das „Wie", also die Art und Weise der Gesetzgebung, sondern auch das „Ob".[526]

Als sonstige allgemeine Anwendungsmodalitäten der Bundestreue sind neben der Voraussetzung eines konkreten Rechtsverhältnisses[527] noch die Verschuldensunabhängigkeit[528] und der Ausschluss des Einwandes „tu quoque"[529] zu nennen.

---

522 Vgl. hierzu aus der zivilrechtlichen Literatur etwa *Mansel*, in: Jauernig (Hrsg.), § 242 BGB, Rn. 48 ff.; *Bauer*, 1992, S. 358.

523 *Bauer*, 1992, S. 359.

524 Vgl. BVerfGE 34, 216 (232); E 42, 345 (358 f.); BVerwGE 50, 137 (145); *Sachs*, in: Sachs (Hrsg.), Art. 20 GG, Rn. 72; *Isensee*, in: HStR IV, § 98, Rn. 157.

525 Vgl. BVerfGE 8, 122 (131).

526 Vgl. dazu BVerfGE 34, 9 (29) zur zeitlich parallelen Gesetzgebungsarbeit von Bund und Land im Regelungsbereich des Besoldungswesens; *Stern*, Staatsrecht, Band I, S. 703.

527 Vgl. *Isensee*, in: HStR IV, § 98, Rn. 157; *Sommermann*, in: v.Mangoldt/Klein/Strack (Hrsg.), Art.20 Abs. 1 GG, Rn. 37; *Stern*, Staatsrecht, Band I, S. 702. .Es ist umstritten, ob bereits ein konkretes Rechtsverhältnis vorliegen muss, auf das die bundesstaatlichen Treuepflichten Anwendung finden oder ob dem Grundsatz bundesfreundlichen Verhaltens selbst eine selbständig pflichtenbegründende Funktion zukommt, *Bauer*, 1992, S. 335, 336. So wohl aber auch BVerfGE 21, 312 (326). An die Voraussetzungen für ein konkretes Rechtsverhältnis dürften aber ohnehin keine hohen Anforderungen zu stellen sein. So heißt es z.B. allgemein in BVerfGE 12, 205 (255): „Wo immer der Bund sich in einer Frage des Verfassungslebens, an der alle Länder interessiert oder beteiligt sind, um eine verfassungsrechtlich relevante Vereinbarung bemüht, verbietet ihm jene Pflicht zu bundesfreundlichem Verhalten ...".

528 Vgl. BVerfGE 8, 122 (140). *Sachs*, in: Sachs (Hrsg.), Art. 20 GG, Rn. 69; *Stern*, Staatsrecht, Band I, S. 702.

cc) Die Folgen eines Verstoßes

Der Verstoß gegen die Bundestreue kann nicht nur durch das Land geltend gemacht werden, welches sich in seinen Rechten beeinträchtigt sieht. Vielmehr kann bei einem wegen Verletzung des Grundsatzes bundesfreundlichen Verhaltens nichtigen Gesetzes ein durch dieses Gesetz in seinen grundrechtlich geschützten Rechtspositionen betroffener Bürger den Verfassungsverstoß über die Freiheitsgrundrechte geltend machen.[530]

Zu beachten ist dabei allerdings, dass eine Gesetzgebung nur bei Überschreiten äußerster Grenzen als verfassungswidrig bewertet werden kann[531]: Zwar setzt die Feststellung der Verletzung der Pflicht zu bundesfreundlichem Verhalten nicht den Nachweis einer „Treulosigkeit“ oder der Böswilligkeit voraus [532]; doch kann ein Gesetz wegen Verletzung der aus dem Grundsatz der Bundestreue abzuleitenden Schranken nur dann als verfassungswidrig verworfen werden, wenn der jeweilige Gesetzgeber seine gesetzgeberische Freiheit „offenbar mißbraucht“ hat.[533]

Von besonderer Bedeutung ist dabei, dass ein „Mißbrauch“ gesetzgeberischer Freiräume nur schwer feststellbar sein dürfte, wenn die Zielsetzung andere Normenkomplexe beeinträchtigenden Regelungen nicht allein auf dem „Egoismus“ des jeweiligen Gesetzgebers beruhen[534], sondern ihrerseits wiederum durch legitime gesetzgeberische Ziele gerechtfertigt sind.[535]

---

529 Auch „kann sich kein Teil seiner Pflicht zu bundesfreundlichem Verhalten mit der Behauptung oder dem Nachweis entziehen, dass auch der andere Teil seiner Pflicht zu bundesfreundlichem Verhalten nicht nachgekommen sei; die Verletzung der Pflicht durch den einen Teil entbindet den anderen nicht von der Beachtung dieser selben Pflicht, vgl. BVerfGE 8, 122 (140); *Sommermann*, in: v.Mangoldt/Klein/Starck, Art. 20 Abs. 1 GG, Rn. 38; *Stern*, Staatsrecht, Band I, S.702.

530 Vgl. *Bauer*, 1992, S. 312; ebenso *W.-R. Schenke*, 1977, S. 139 mit Fn. 226 zum Parallelproblem bei der Verfassungsorgantreue. Zur Überprüfung von (gerügten oder für erörterungswürdig erachteten etwaigen) Verletzungen der Bundestreue im Rahmen von Verfassungsbeschwerden nach Art. 93 Abs. 1 Nr. 4 a GG vgl. BVerfGE 26, 116 (137); E 34, 165 (194 f.); E 45, 400 (421); E 76, 1 (77).

531 Vgl. Bauer, 1992, S. 356 ff.

532 Die Feststellung der Treuepflichtverletzung setzt weder den Nachweis der Treulosigkeit noch der Böswilligkeit voraus; sie impliziert „überhaupt keinen Vorwurf“, so BVerfGE 8, 122 (140); *Sachs*, in: Sachs (Hrsg.), Art. 20 GG, Rn. 69.

533 Vgl. Bauer, 1992, S. 357 unter Hinweis auf Entscheidungen des BVerfG in denen es eine „unvertretbare Schädigung oder Beeinträchtigung“ (E 34, 9/44), eine „schwerwiegende Beeinträchtigung elementarer Interessen“ (E 34, 216/232) oder eine „mißbräuchliche Interessenwahrnehmung“ (E 61, 149/205) fordert.

534 Vgl. BVerfGE 43, 291 (348).

535 In diesem Kontext ist zu beachten, dass schon die Verfassung miteinander konfligierende Zwecke verfolgt und dementsprechend einander beeinträchtigende Gesetze eine geradezu zwangsläufige Entscheidung sind; vgl. *Felix*, 1998, S. 367. Siehe dazu auch Bauer, 1992, S. 357.

dd) Die präventive Telekommunikationsüberwachung als Verstoß gegen die Bundestreue?

Ein Verstoß gegen den Grundsatz des bundesfreundlichen Verhaltens durch eine länderübergreifende Telekommunikationsüberwachung kommt unter mehreren Aspekten in Betracht.

Zu einen ist ein Land angehalten ein anderes Bundesland zu informieren und zu unterrichten, wenn „die Auswirkungen einer gesetzlichen Regelung nicht auf den Raum des (eigenen) Landes begrenzt sind“.[536] Zum anderen kann das Land in diesem Fall zur Zusammenarbeit und Kooperation verpflichtet sein, da es sich um grenzüberschreitende Maßnahmen handelt.[537]

Anders als beim Beispiel der Raumplanung[538] zieht die Telekommunikationsüberwachung allerdings nicht die Konsequenz nach sich, dass abhängig vom Vorgehen des einen Landes eine präventive Telekommunikationsüberwachung durch das andere Land tatsächliche oder rechtliche Einschränkungen erfahren würde. Ist das eine Land bei der Verwirklichung seiner (Raum-)Pläne durch die bereits ausgeführten Vorhaben des anderen Landes gehindert, trifft dies bei der Telekommunikationsüberwachung nicht zu. Maßnahmen sind unabhängig von einander möglich.[539] Eine Zusammenarbeit und Kooperation mag zwar wünschenswert sein, (verfassungsrechtlich) zwingend ist sie nicht.

Allerdings ist das jeweilige Land angehalten, das (Nachbar-)Bundesland zu informieren, auf das sich seine Telekommunikationsüberwachung erstrecken kann. Unterlässt es dies, dürfte die getroffene Regelung dennoch nicht nichtig sein. Ein „offenbarer Mißbrauch“[540] gesetzgeberischer Kompetenz ist nicht zu erkennen, zumal das „betroffene“ Land keine Einschränkungen territorialer Art erfährt und es ihm unbenommen bleibt, selbst eine Telekommunikationsüberwachung zu Gefahrenabwehrzwecken zu normieren.

---

536 Vgl. BVerfGE 4, 115 (140); *Lorz*, 2001, S. 28; *Felix*, 1998, S. 367; *Bauer*, 1992, S. 348; *Steinberger*, NJW 1987, 2345 (2348).

537 Vgl. § 4 Abs. 4; § 5 Abs. 3, Satz 3 ROG.

538 Vgl. dieses Kapitel unter VI. 3. b) aa) (1).

539 Sollte das betroffene Bundesland am überwachten Telekommunikationsanschluss Überwachungsmaßnahmen durchführen wollen, so ist ihm das ohne weiteres möglich, vgl. § 6 Abs. 4 TKÜ.

540 Vgl. Fn. 533.

Vielmehr ist zu bedenken, ob das Land, das sich gegen die Gefahrenabwehrmaßnahme der Telekommunikationsüberwachung eines anderen Landes zu Wehr setzt, nicht rechtsmißbräuchlich handelt. Folge wäre, dass das betroffene Land die Kommunikationsüberwachung zu dulden hätte.[541] Ein rechtsmißbräuchliches Handeln kann dann vorliegen, wenn der Rechtsinhaber keine berechtigten Interessen verfolgt oder überwiegende Belange der anderen Beteiligten entgegenstehen und die Rechtsausübung zu einer gravierenden Störung der bundesstaatlichen Ordnung führen würde.[542]

Selbstverständlich kann jedes Land für sich entscheiden, welche Gefahrenabwehrmaßnahmen auf seinem Hoheitsgebiet zur Anwendung gebracht werden. Nicht entschieden ist damit aber, welche Maßnahmen gegenüber einem potenziellen Störer ergriffen werden können, der nicht für eine Gefahrenlage im eigenen, sondern für eine Gefahrenlage in einem anderen Bundesland verantwortlich ist.

Die präventive Telekommunikationsüberwachung lediglich auf das eigene Bundesland zu erstrecken, würde dieser Maßnahme in einer Vielzahl von Fällen die Wirksamkeit nehmen. Charakteristisch für die Telekommunikationsüberwachung in der heutigen Zeit ist, dass sie überwiegend nicht mehr ortsgebunden ist. Die mittels (Handy-)Kommunikation aufgebauten Netzwerke der potenziellen Störer und die damit einhergehenden Gefahren bekämpfen zu können, ist u.a. Hintergrund der neuen gesetzlichen Regelungen.[543]

Würde das Bundesland darauf bestehen, dass auf seinem Gebiet keine Telekommunikation stattfindet, würde dies insofern zu einer empfindlichen Störung der bundesstaatlichen Ordnung führen, als ein Land dann effektive Gefahrenabwehrmaßnahmen eines anderen verhindern könnte, obwohl es dadurch keinerlei (territoriale) Einschränkung erfährt. Denn auch durch die Verfahrensregelungen für die Überwachungsanordnung wird nicht in fremde Ho-

---

541 Vgl. *Bauer*, 1992, S. 357: „ ... die Ausübung eines Rechts unzulässig sein kann, wenn der Rechtsinhaber keine berechtigten Interessen verfolgt oder überwiegende Belange der anderen Beteiligten entgegenstehen...“. Siehe auch BVerfGE 1, 299 (316 f.) zur Unbeachtlichkeit eines sachfremden Widerspruchs und *Stern*, Staatsrecht, Band I, S. 703 unter Hinweis auf BVerfGE 21, 312 (326): „Man darf also teils einen bestimmten Gebrauch von Kompetenzen nicht machen, teils muss man in bestimmter Weise vorgehen.“

542 Vgl. BVerfGE 4, 115 (140); *Bauer*, 1992, S. 357.

543 Vgl. LT-Drucks. Th. 3/2128, S. 8; LT-Drucks. Nds. 15/240, S. 16, LT-Drucks. Bayern15/2096, S. 2.

heitsrechte eingegriffen. Zuständig für die Anordnung sind die Amtsgerichte, in deren Bezirk die antragstellende Polizeibehörde ihren Sitz hat.[544]

Das „Überwacher-Bundesland“ wäre beschränkt auf die Überwachung von Kommunikation, die lediglich im eigenen Bundesland stattfindet. Ein solch eingeschränkter Aktionsradius kann kaum dazu beitragen, die Organisierte Kriminalität und den internationalen Terrorismus und damit Gefahren für den Bürger wirksam zu bekämpfen.[545]

c) Die subjektiven Rechte Privater

Subjektive Rechte Privater stehen der bundesweiten Geltung ebenfalls nicht entgegen. Insofern werden keine vertrauensschaffenden Rechtspositionen verletzt. Ist eine Person für eine potenzielle Gefahr in einem Bundesland verantwortlich, so kann die zuständige Behörde nach Maßgabe des jeweiligen Landesrechts einschreiten. Dass die dafür geeignete Maßnahme Wirkung über die Landesgrenzen hinweg entfaltet, vermag Rechte des Betroffenen nicht zu verletzten, ein Verlust demokratischer Selbstbestimmung ist nicht gegeben.[546] Die demokratische Legitimation des Normgebers besteht grundsätzlich für sein territoriales Hoheitsgebiet. Gegen den Verursacher einer Gefahr innerhalb dieses Gebiets darf eingeschritten werden. Dass dabei die (ermessensgerecht) gewählte Maßnahme auch Wirkung über die Landesgrenze hinaus entfaltet, vermag nach der hier vertretenen Ansicht an der demokratischen Legitimation des Normgebers nichts zu ändern. Eine Vertrauensposition dergestalt, dass der Behörde eine effektive Gefahrenabwehr verwehrt ist, nur weil sich der Störer außerhalb der Landesgrenzen aufhält, ist nicht gegeben. Ein derartiger „Täterschutz“ ist nicht angezeigt.[547]

4. Fazit

Den landesgesetzlichen Ermächtigungsgrundlagen kommt bundesweite Geltung zu, da ihr Regelungsgegenstand einen spezifischen landesrechtlichen Bezug aufweist und fremde Hoheitsrechte nicht beeinträchtigt werden. Die neu eingeführten Maßnahmen ermöglichen daher

---

544 § 34 a Abs. 2, Satz 4 ThPAG, § 33 a Abs. 3, Satz 1 NSOG, Art. 34 c Abs. 1 iVm Art. 34 Abs. 4, Satz 2 PAG, § 31 Abs. 4, Satz 5 POG und § 15 a Abs. 4, Satz 2 HSOG. Anders ist dies beispielsweise bei der Wohnraumüberwachung. Für die Anordnung von Wohnraumüberwachungen ist das Amtsgericht zuständig, in dessen Bezirk die Wohnung liegt, vgl. § 26 Abs. 1 ThPAG und § 39 Abs. 1, Satz 2 HSOG.

545 Vgl. die Ausführungen auf Seite 75 und 76.

546 So aber *R.P. Schenke*, AöR 125, 1 (17).

547 Zum Themenkreis, ob Datenschutz gleich Täterschutz bedeutet, siehe *Hassemer/Starzacher*, 1993

der Polizei Kommunikationsanschlüsse in anderen Bundesländern und Mobilfunkanschlüsse nicht landesansässiger Bundesbürger zu überwachen. Die Erhebung der Telekommunikationsdaten bzw. die Überwachung der Telekommunikation erfolgt durch den Zugriff über inländische Diensteanbieter[548], der sich der Polizei über die Regelungen des Telekommunikationsgesetzes eröffnet. Solange der Betroffene seine Kommunikation über diese Dienstanbieter abwickelt, ist die Überwachung unabhängig von seinem Aufenthaltsort zulässig.[549]

VI. Die Überwachung mittels IMSI-Catcher

Der Einsatz des IMSI-Catchers ist den Landespolizeibehörden nur durch die jeweiligen Landesgesetze eröffnet. Eine Ermächtigung im TKG ist nicht vorhanden. Der Einsatz des IMSI-Catchers setzt eine räumliche Nähe zur überwachenden Person voraus.[550] Da der räumliche Hoheitsbereich anderer Bundesländer nicht verletzt werden darf, ist sein Einsatz grundsätzlich nur auf dem eigenen Staatsgebiet möglich.[551] Sein Einsatz auf fremdem Hoheitsterritorium durch landeseigene Polizeibehörden kann nicht durch Landesgesetz geregelt werden. Erforderlich wäre dafür eine entsprechende Vereinbarung der Bundesländer.

---

548 § 34 a Abs. 4, Satz 1 ThPAG iVm § 2 Abs. 1, Satz 3 und 4 G-10-Gesetz; § 33 a Abs. 7 und § 33 c Nds.SOG; Art. 34 b Abs. 1 und 2 PAG; § 31 Abs. 6 POG; § 15 a Abs. 1 HSOG.

549 Siehe dazu die Ausführungen in diesem Kapitel unter IV.

550 In die simulierte Funkzelle eines IMSI-Catchers loggen sich Handys im Umkreis von 100 – 300 m ein, vgl. das Kapitel „Der Zugriff auf die Telekommunikationsdaten“ unter IV.

551 Vgl. BVerfGE 11, 6 (19); *Oldiges*, DÖV 1989, 873 (878 f.); *Ule*, JZ 1961, 622 (623); *Isensee*, in: HStR IV, § 98, Rn. 33.

Kapitel 5: Grundrechtliche Anforderungen

Durch die Überwachung des Telekommunikationsverkehrs erhalten die Polizeibehörden Kenntnis über eine Vielzahl verschiedener Daten. Die Normen, die diese Maßnahme der Datenerhebung ermöglichen, müssen der verfassungsmäßigen Ordnung entsprechen und sind daher an den Schranken der durch die Überwachung betroffenen Grundrechte des Grundgesetzes zu messen.

Schranken der Polizeigewalt bilden jedoch nicht nur die Grundrechte des Grundgesetzes, sondern auch die Europäischen Grund- und Menschenrechte, die auf unterschiedlichen Ebenen und mit unterschiedlichen Rechtswirkungen normiert sind.[552]

So verbrieft Art. 8 Abs. 1 der Europäischen Menschenrechtskonvention (EMRK)[553] das Recht jeder Person auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz. Einen Eingriff in dieses Recht stellt die staatliche Telefonüberwachung dar.[554] Die Gewährleistung steht jedoch unter Vorbehalt, denn Art. 8 Abs. 2 EMRK gestattet auf gesetzlicher Grundlage die in einer demokratischen Gesellschaft notwendigen Eingriffe in die Rechte aus Abs. 1 „für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer“. Da der EMRK zwar kein Verfassungsrang[555], jedoch der Rang eines einfachen Bundesgesetzes zukommt,[556] kann die EMRK als Maßstab für polizeiliche Einzelmaßnahmen herangezogen werden und hat gegenüber den landesrechtlichen Polizeigesetzen Vorrang.[557]

---

552 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 65.

553 Die Bundesrepublik Deutschland ratifizierte die am 03. September 1953 in Kraft getretene Konvention bereits am 05.12.1952 und gehört damit gemeinsam mit Norwegen, Schweden, Belgien, Großbritannien, Irland und Luxemburg zu den Mitgliedsstaaten der ersten Stunde, vgl. *Grabenwarter*, 2005, § 1, Rn. 3.

554 Vgl. EGMR EuGRZ 1979, 279 (284); ÖJZ 1999, 115 (116); NJW 2007, 1433 (1434); *Meyer-Ladewig*, Art. 8 EMRK, Rn. 10.

555 Vgl. BVerfGE 10, 271 (274); 64, 135 (157); 74, 102 (128), wonach Prüfungsmaßstab im Rahmen einer Verfassungsbeschwerde allein die Grundrechte des Grundgesetzes sind.

556 Art. 59 Abs. 2 GG.

557 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 66. Nach Art. 46 EMRK sind die Vertragsstaaten verpflichtet, in allen Rechtssachen, in denen sie Partei sind, das endgültige Urteil des Gerichtshofs zu befolgen. Wird eine Konventionsverletzung festgestellt, begründet dies für den beklagten Staat die Verpflichtung, die Konventionsverletzung abzustellen und Ersatz für die Folgen zu leisten. Zur Beendigung der Verletzung sind die Mitgliedsstaaten verpflichtet, diejenigen Maßnahmen zu ergreifen, die notwendig sind, um die Verletzung abzustellen. vgl. *Meyer-Ladewig*, Art. 46 EMRK, Rn. 2; *Grabenwarter*, 2005, § 16, Rn. 3. Die Pflicht zur Beseitigung der Konventionsverletzung kann zunächst Gerichte und vor allem das Verfassungsgericht treffen, vgl. *Grabenwarter*, 2005, § 16 Rn. 4; siehe auch *Meyer-Ladewig*, § 46 EMRK,

Auch den europarechtlichen Anforderungen haben die neuen gesetzlichen Regelungen Rechnung zu tragen. Zugunsten des europäischen Gemeinschaftsrechts besteht nach Ansicht des Europäischen Gerichtshofs (EuGH) ein uneingeschränkter Anwendungsvorrang gegenüber dem nationalen Recht.[558] Insbesondere dieser Anwendungsvorrang bedingt die Notwendigkeit der Gewährleistung eines gemeinschaftsweiten Grundrechtsstandards.[559] Das primäre und sekundäre Gemeinschaftsrecht enthalten jedoch (noch) keinen ausformulierten Grundrechtskatalog,[560] sondern gewährleisten explizit nur eine begrenzte Anzahl von Grundrechten.[561] Der im Dezember 2000 proklamierten EU-Grundrechtscharta[562], die in Art. 7 ein Recht jeder Person auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation gewährleistet,[563] kommt bislang keine Rechtsqualität zu. Zwar wurde die EU-Grundrechtscharta in den Verfassungsvertrag der Europäischen Union aufgenommen[564] und soll nun aufgrund der Ablehnung des Verfassungsvertrages in mehreren Mitgliedstaaten durch einen Verweis im Reformvertrag[565] rechtsverbindlich werden.[566] Voraussetzung dafür ist jedoch die Ratifizierung durch alle Mitgliedstaaten, die (noch) nicht erfolgt ist.[567]

Rn. 4 ff. Der Gesetzgeber ist zur Umsetzung verpflichtet, wenn eine konventionskonforme Interpretation nicht möglich ist, vgl. *Grabenwarter*, 2005, § 16 Rn. 5; *Meyer-Ladewig*, Art. 46 EMRK, Rn. 23 und 35.

558 Grundlegend EuGHE 1964, 1251; ausführlich dazu *G. Hirsch*, NJW 2000, 1817. Das BVerfG dagegen erkennt diesen Anwendungsvorrang nur gegenüber dem nationalen einfachen Recht uneingeschränkt an, vgl. BVerfGE 31, 145 (174). In Bezug auf das nationale Verfassungsrecht geht das BVerfG nur von einem Anwendungsvorrang aus, solange ein wirksamer Grundrechtsschutz durch den EuGH gewährleistet ist; BVerfGE 37, 271 – Solange I – Entscheidung und BVerfGE 73, 339 – Solange II – Entscheidung. Vgl. dazu ausführlich *Streinz*, 2005, Rn. 224 ff.

559 Vgl. *Weber*, NJW 2000, 537 (542), *I. Pernice*, NJW 1990, 2409 (2412); *Streinz*, 2005, Rn. 753.

560 Zum Vorhaben der Europäischen Union einen eigenen geschriebenen Grundrechtskatalog zu entwickeln vgl. *Streinz*, 2005, Rn. 755 ff.

561 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 69 mit dem Beispiel des Verbots der Diskriminierung aus Gründen der Staatsangehörigkeit in Art. 12 Abs. 1 EGV.

562 Abl. EG 2000, Nr. C 364, S. 1 ff; dazu *Magiera*, DÖV 2000, 1017. Einen Überblick über die verschiedenen Grundrechtsgewährleistungen bietet *Grabenwarter*, DVBl. 2001, 1 ff.

563 Die Rechte des Art. 7 der Grundrechtscharta entsprechen den Rechten, die durch Art. 8 EMRK gewährleistet sind. Um der technischen Entwicklung Rechnung zu tragen, wurde lediglich der Begriff „Korrespondenz“ durch „Kommunikation“ ersetzt, *Rengeling/Szczekalla*, 2004, Rn. 655. Nach Art. 52 Abs. 3 der Grundrechtscharta haben die in der Charta aufgeführten Rechte eine dem jeweiligen Artikel der EMRK entsprechende Bedeutung und Tragweite, vgl. dazu auch *Kingreen*, in Calliess/Ruffert (Hrsg.), GrCh, Art. 7, Rn. 2 ff.. Die möglichen Einschränkungen dieses Artikels sind daher diejenigen, die sich aus der EMRK ergeben, *Rengeling/Szczekalla*, 2004, Rn. 656; vgl. auch *Grabenwarter*, DVBl. 2001, 1 (4).

564 *Oppermann*, 2005, § 6 Rn. 39. Siehe auch *Würtenberger/Heckmann*, 2005, Rn. 69.

565 Vgl. Entwurf eines Vertrages zur Änderung des Vertrages über die Europäische Union und des Vertrages zur Gründung der Europäischen Gemeinschaften (Refomvertragsentwurf) vom 23.07.2007, Dok.Nr. CIG 1/07.

566 Vgl. Art. 1 des Reformvertragsentwurfs, der die Änderungen bzgl. der Grundrechtscharta in Art. 6 Nr. 1 des Verfassungsvertrages enthält.

567 Die Ratifizierung soll bis 01.01.2009 erfolgen, vgl. Schlußbestimmungen des Reformvertragsentwurfs.

Daher stützt sich die Begründung der Grundrechte (momentan) auf außerhalb des Gemeinschaftsrechts liegende Erkenntnisquellen.[568] Dies sind die Grundsätze des Gemeinschaftsrechts und der Gemeinschaftsverträge[569], die gemeinsame Verfassungsüberlieferung der Mitgliedstaaten[570] und die völkerrechtlichen Menschenrechtsgewährleistungen[571].

Da der EuGH die EMRK zur Ermittlung der einzelnen Gewährleistungen heranzieht, werden die dortigen Gewährleistungen als Mindeststandard für den gemeinschaftsrechtlichen Grundrechtsschutz angesehen.[572] Zieht der EuGH zudem die nationalen Grundrechte als Gewährleistungsgehalt heran, so dürfte ein Verstoß gegen Gemeinschaftsrecht ausgeschlossen sein, wenn die neuen polizeigesetzlichen Regelungen in Einklang mit dem Grundgesetz und der EMRK stehen.[573] Insofern kann auf eine Überprüfung, ob diese Regelungen auch mit den europäischen Grundrechten in Einklang stehen, verzichtet werden.[574]

Ist eine staatliche Maßnahme in mehreren Gesetzen vorgesehen, liegt es nahe deren (Eingriffs-)Voraussetzungen miteinander zu vergleichen. Hinter der Formel der „Einheit der Rechtsordnung“[575] steht dabei die Vorstellung, dass die Teile einer Rechtsordnung – also die verschiedenen Rechtsgebiete – nicht beziehungslos neben einander stehen, sondern eine harmonische Einheit bilden.

Wie bereits in Kapitel 2 unter I. und II. dargestellt, ist die staatliche Telekommunikationsüberwachung neben den nunmehr eingeführten landesgesetzlichen Regelungen bereits in §§ 100 a StPO, dem G-10-Gesetz, den Gesetzen der Nachrichtendienste und den §§ 23 a ff.

---

568 Art. 6 Abs. 2 EUV.

569 Vgl. EuGHE 1985, 538 (550).

570 Vgl. EuGHE 1974, 491 (507); 1989, 2609 (2639).

571 Vgl. EuGHE 1979, 3727 (3745); 1986, 1663 (1682).

572 Vgl. *Streinz*, 2005, Rn. 761.

573 Die Gemeinschaftsrechte binden die Mitgliedsstaaten nur, wenn und soweit der konkrete Fall dem Anwendungsbereich des Gemeinschaftsrechts unterliegt, vgl. *Streinz*, 2005, Rn. 768. Siehe zum Grundrechtsschutz durch den EuGH, den EGMR und die nationalen Gerichte *Schwarze*, NJW 2005, 3459 ff.

574 Der EuGH hatte bislang noch keinen Anlass, Inhalt und Umfang des gemeinschaftsrechtlichen Grundrechtsschutzes des Brief-, Post- und Fernmeldegeheimnisses zu präzisieren; vgl. *Kingreen*, in: Calliess/Ruffert (Hrsg.), 2002, EUV, Art. 6, Rn. 102. Zu Art. 7 Grundrechtscharta vgl. *Kingreen*, in Calliess/Ruffert (Hrsg.), GrCh, Art. 7, Rn. 2 ff.

575 Vgl. zur Verwendung der „Einheitsformel“ in der Geschichte des juristischen Denkens von 1797 bis 1935, *Baldus*, 1995.

ZFdG enthalten. Auch finden sich in den Landespolizeigesetzen bereits Ermächtigungsgrundlagen für die Standortbestimmung.[576]

Gefordert wird, dass die verschiedenen Teilrechtsgebiete keine einander widersprechenden Lösungen hervorbringen, sondern Widersprüche zwischen den einzelnen Teilrechtsordnungen im Hinblick auf die Wahrung der Einheit der Rechtsordnung zu vermeiden sind.[577]

Auch das BVerfG hat ausgeführt: „Das Rechtsstaatsprinzip und die bundesstaatliche Kompetenzordnung verpflichten alle rechtssetzenden Organe, ihre Regelungen jeweils so aufeinander abzustimmen, dass den Normadressaten nicht gegenläufige Vorschriften erreichen, die Rechtsordnung also nicht aufgrund unterschiedlicher Anordnungen widersprüchlich wird.“[578]

Das Postulat der Einheit bzw. Widerspruchsfreiheit der Rechtsordnung[579] richtet sich gegen Widersprüche innerhalb einer Rechtsordnung, die sich nicht mit Hilfe der allgemeinen Kollisionsregeln lösen lassen.[580] Das Problem liegt darin, dass entweder mehrere Regelungen an den gleichen Tatbestand unterschiedliche und sich wechselseitige Rechtsfolgen anknüpfen (Normwiderspruch) oder mehrere Regelungen, die einen vergleichbaren Sachverhalt betreffen, deshalb widersprüchlich sind, weil ihnen unterschiedliche Wertungen zugrunde liegen (Wertungswiderspruch).[581] Eine einheitliche Rechtsordnung liegt vor, soweit es sich wie

---

576 Art. 33 Abs. 1 Nr. 1 und 2, Abs. 3 PAG; § 34 Abs. 1 und 2 ThPAG; §§ 34, 35 Nds.SOG; § 28 Abs. 1 und 2 Nr. 1 und 5 POG; § 15 Abs. 1 Nr.1, Abs. 2 HSOG.

577 Vgl. *Felix*, 1998, S. 142 f.

578 BVerfGE 98, 83 (97). Zur Kritik in der Literatur vgl. *Kloepfer/Bröcker*, DÖV 2001, 1 ff., die das Gebot der widerspruchsfreien Normgebung lediglich als spezielle Kompetenzausübungsschranke ansehen und *Brüning*, NVwZ 2002, 33 ff., nach dessen Ansicht sich die Verallgemeinerung des Gebots der Widerspruchsfreiheit zu einem rechtsstaatlichen Gebot verbietet, da dessen Schwammigkeit und Konturlosigkeit alle Möglichkeiten eröffnet.

579 Das BVerfG hat nicht ein (positives) Gebot der Stimmigkeit der Rechtsordnung postuliert, sondern es bei dem Negativ-Kriterium der Widerspruchsfreiheit belassen, vgl. *Kloepfer/Bröcker*, DÖV 2001, 1 (8). Zur Verwendung der Einheit der Rechtsordnung als begründungstragende Argumentationsfigur vgl. *Felix*, 1998, S. 5; *Baldus*, 1995, S. 13; *Michel*, JuS 1961, 274 (275 f.). In der Regel wurden aus der „Einheit der Rechtsordnung“ einfach Folgerungen abgeleitet, ohne zu hinterfragen, worum es sich bei der Argumentationsfigur überhaupt handelt, vgl. z.B. *Paulick*, DStR 1975, S. 564 (572); LG Köln ZMR 1989, S. 96 (97).

580 Als Kollisionsregeln gelten dabei die Grundsätze „lex superior derogat legi inferiori“, „lex posterior derogat legi priori“ und „lex specialis derogat legi generali“, vgl. *Felix*, 1998, S. 154; *Kloepfer/Bröcker*, DÖV 2001, 1 (9 f.). Heranzuziehen sind aber auch die Kompetenzordnung des Grundgesetzes, die Möglichkeit der Gesetzesauslegung sowie der Grundsatz des bundesfreundlichen Verhaltens, vgl. *Kloepfer/Bröcker*, DÖV 2001, 1 (3 ff.); *Zippelius/Würtenberger*, 2005, § 12 III 3.

581 Vgl. *Zippelius/Würtenberger*, 2005, § 12 III 3; *Felix*, 1998, S. 243 f.; *Engisch*, 2005, S. 209 ff.

beim Bundesrecht um einen Normenkomplex handelt, der auf ein und dieselbe Autorität zurückgeht.[582] Gleiches gilt jedoch auch bei Konflikten zwischen Bundes- und Landesrecht. [583]

Zu (Wertungs-)Widersprüchen zwischen Bundes- und Landesrecht kann es normalerweise nicht kommen, da das Grundgesetz die Gesetzgebungskompetenzenverteilung eindeutig vorgenommen hat.[584] Daher ist von sich widersprechenden Normen regelmäßig eine Norm kompetenzwidrig und damit schon ohne Rücksicht auf den Wertungswiderspruch nichtig.[585] Ein Wertungswiderspruch ist ausnahmsweise dann möglich, wenn derselbe Lebenssachverhalt unter verschiedenen Aspekten geregelt wird und einmal der Bund und einmal das Land die entsprechende Gesetzgebungskompetenz hat.[586]

Derartige Wertungswidersprüche lassen sich nicht vollständig anhand der Regeln über den Vorrang des Bundesrechts oder die Kompetenzordnung lösen. Für ihre Auflösung hat das BVerfG den rechtsstaatlichen, aber auch im Bundesstaatsprinzip wurzelnden Grundsatz der

---

582 Vgl. *Felix*, 1998, S. 147.

583 *Felix*, 1998, S. 149. Denn die zwischen Bund und Ländern geteilten staatlichen Kompetenzen sind es, die letztlich die „volle deutsche Staatsgewalt“ und die hinter der gemeinsamen Rechtsordnung stehenden Autorität ausmachen. Die Rechtsordnungen der Länder sind in die Rechtsordnungen des Bundes gleichsam eingebettet und bilden gemeinsam eine einheitliche Rechtsordnung, nämlich die der Bundesrepublik Deutschland, die verfassungsrechtlich vom Bund und den Ländern „als ein Ganzes“ gebildet wird, vgl. BVerfGE 6, 309 (340).

584 Zu widersprüchlichen Regelungen auf einer Gesetzgebungsebene kann es kommen, wenn eine rechtliche Regelung nicht in das System der übrigen rechtlichen Regelungen passt. Hier verpflichtet der aus Art. 3 Abs. 1 GG und dem Rechtsstaatsprinzip hergeleitete Grundsatz der Systemgerechtigkeit bzw. der Folgerichtigkeit, dass sich gesetzgeberische Entscheidungen in den Kontext der Verfassung aber auch des sonst geltenden Rechts logisch und teleologisch widerspruchsfrei einfügen, vgl. *Zippelius/Würtenberger*, 2005, § 23 II 1 f) unter Hinweis auf BVerfGE 60, 16 (40) und BVerfGE 104, 74 (87). Nach *Felix*, 1998, S. 289, soll Art. 3 Abs. 1 GG keine Bedeutung für die Widerspruchsfreiheit der Rechtsordnung haben, da das verfassungsrechtliche Gleichbehandlungsgebot nicht die Gleichbehandlung eines identischen Sachverhalts in unterschiedlichen Teilrechtsgebieten gebiete.

585 Vgl. Art. 72 Abs. 1 und 31 GG.

586 Vgl. *Zippelius/Würtenberger*, 2005, § 12 III 3. Wertungswidersprüche zwischen den Landespolizeigesetzen, dem G-10-Gesetz den Nachrichtendienstgesetzen und dem ZfdG dürften damit ausscheiden. Zum einen ermächtigen diese nicht den Polizeivollzugsdienst zur Telekommunikationsüberwachung und zum anderen verfolgen das G-10-Gesetz und die Nachrichtendienstgesetze mit dem Staatsschutz andere Ziele als die Polizeigesetze. Das ZFdG konzentriert sich auf die Verhinderung von Straftaten nach dem AWG und die Gefahrenabwehr, wenn ohne Genehmigung oder Entscheidung nach der Verordnung (EG) Nr. 1334/2000 oder nach den §§ 5 c oder 5 d der Außenwirtschaftverordnung die Ausfuhr bestimmter Güter vorbereitet wird. Etwas anderes kann bei sog. doppelfunktionalen Maßnahmen gelten, deren Rechtmäßigkeit sich sowohl nach den Polizeigesetzen als auch der StPO richten kann. Keine einheitliche Rechtsordnung liegt zwischen den verschiedenen Landesgesetzen vor, da diese Normen auf verschiedene Gesetzgeber zurückgehen. Sollte ein Widerspruch darin liegen, dass ein Land eine Telekommunikationsüberwachung nicht zulassen will, im Rahmen der länderübergreifenden Sachverhalte aber eine Überwachung seiner Bürger möglich ist, berührt dies den Grundsatz der Bundestreue und ist an dessen Maßstäben zu prüfen; vgl. dazu Kapitel „Länderübergreifende Sachverhalte“, V. 3. b). So im Ergebnis auch *Felix*, 1998, S. 364 ff.

Widerspruchsfreiheit der Rechtsordnung (fort-)entwickelt.[587] Welche der widersprüchlichen Regelungen zu weichen hat, ist aus der Verteilung der Gesetzgebungskompetenzen und mit Rücksicht auf das Prinzip des bundesfreundlichen Verhaltens zu entwickeln.[588]

Im Rahmen der Überprüfung der Verfassungsmäßigkeit der landespolizeigesetzlichen Regelungen wird daher auch auf die Widerspruchsfreiheit in Bezug auf die bereits bestehenden Regelungen der Telekommunikationsüberwachung eingegangen.[589]

Die Untersuchung der Landespolizeigesetze erfolgt dergestalt, dass zunächst die neu eingeführten Regelungen anhand ihrer Eingriffsvoraussetzungen und Verfahrensanforderungen dargestellt werden. Dann wird herausgearbeitet, welche Anforderungen das Grundgesetz und EMRK an Art. 10 Abs. 1 GG einschränkende Gesetze stellen. Im Anschluss daran wird überprüft, ob die landespolizeigesetzlichen Regelungen diesen Anforderungen gerecht werden. Schließlich erfolgt ein Vergleich mit den in der StPO vorhandenen Vorschriften zur Telekommunikationsüberwachung und den Regelungen in den Polizeigesetzen zur Standortbestimmung.

I. Die Regelungen der präventiv-polizeilichen Telekommunikationsüberwachung in den Polizeigesetzen[590]

Die Polizeigesetze sehen verschiedene Eingriffsvoraussetzungen für die präventiv-polizeiliche Telekommunikationsüberwachung vor. Differenziert wird nach den unterschiedlichen „Methoden“ der Telekommunikationsüberwachung, also Auskunftserteilung, Inhaltsüberwachung und dem Einsatz des IMSI-Catchers sowie nach den jeweils betroffenen Personen.

---

587 Vgl. BVerfGE 98, 83 (97 f.); *Zippelius/Würtenberger*, 2005, § 12 III 3. Nach *Felix*, 1998, S. 401 findet die Argumentationsfigur „Einheit der Rechtsordnung“ im geltenden Verfassungsrecht dagegen keine Stütze. Vielmehr sei die Widerspruchslosigkeit als rechtsstaatliches Gebot der Normenklarheit im weiteren Sinne anzuerkennen; sie verpflichtet den Gesetzgeber zur Vermeidung inhaltlicher Widersprüche nicht nur innerhalb eines konkreten Gesetzeswerkes, sondern über die Gesamtrechtsordnung hinweg. Auch könnten Widersprüche innerhalb der Rechtsordnung über die Bundestreue oder im Rahmen der Verhältnismäßigkeitsprüfung gelöst werden, vgl. *Felix*, 1998, S. 242, 364 und 383. So wohl auch *Schulze-Fielitz*, in: Dreier (Hrsg.), Art. 20 GG (Rechtsstaat), Rn. 141, da das Gebot der Klarheit des Rechts gebietet, dass Gesetze verständlich, widerspruchsfrei und praktikabel sein müssen.

588 Vgl. *Zippelius/Würtenberger*, 2005, § 12 III 3.

589 Ob dabei überhaupt Widersprüche vor dem Hintergrund der verschiedenen Gesetzeszwecke und Mittel zu finden sind, wird in diesem Kapitel unter IV. erörtert.

590 Eine Übersicht über die verschiedenen Anordnungsvoraussetzungen gibt die Tabelle im Anhang.

Die Verfahrensanforderungen, die die fünf Polizeigesetze an die Anordnung einer präventiven Telekommunikationsüberwachung stellen, sind dagegen nahezu identisch. Vorgesehen ist jeweils die Anordnung durch den Richter, das Verfahren richtet sich nach dem FGG.[591]

1. Die Eingriffsvoraussetzungen nach Art. 34 a – c PAG

Nach Art. 34 a Abs. 1 Satz 1 PAG kann die Polizei durch die Überwachung und Aufzeichnung der Telekommunikation personenbezogene Daten erheben

- über die für eine Gefahr Verantwortlichen, 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 (Nr. 1),
- über Personen, wenn konkrete Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass sie eine schwerwiegende Straftat begehen werden (Nr. 2) und
- über Personen, soweit bestimmte Tatsachen die begründete Annahme rechtfertigen, dass sie für Personen nach Nr. 1 oder 2 bestimmte oder von diesen herrührende Mitteilungen entgegennehmen[592] oder weitergeben (Nr. 3 a) oder die unter Nr. 1 und 2 genannten Personen ihre Kommunikationseinrichtungen benutzen werden (Nr. 3 b).

Gemäß Art. 34 a Abs. 2, Satz 1 und Art. 34 a Abs. 4, Satz 1 PAG kann die Polizei unter den Voraussetzungen des Art. 34 a Abs. 1 PAG auch einen IMSI-Catcher einsetzen, sowie die Kommunikationsverbindungen der dort genannten Personen unterbrechen oder verhindern.[593]

---

591 Die Voraussetzungen entsprechen damit im Wesentlichen denen der präventiven Wohnraumüberwachung.

592 Für diese Alternative ist erforderlich, dass keine Zeugnisverweigerungsrechte nach §§ 53, 53 a StPO für die betroffene Person gegeben sind.

593 An spezialgesetzlichen Befugnisnormen für die Unterbrechung oder Verhinderung von Kommunikationsverbindungen hat es bislang gefehlt. Durch die Befugnis der Polizei – nicht der Telekommunikationsunternehmen – zur Unterbrechung der Kommunikation, soll diese sicherheitsrechtliche Lücke geschlossen werden, vgl. LT-Drucks. Bayern 15/2096, S. 58. Nach Ansicht von *Schmidbauer*, in: Schmidbauer/Steiner/Roese, Art. 11 PAG, Rn. 177 ff. konnte die Unterbrechung der technischen Kommunikation aber auf die polizeiliche Generalklausel des Art. 11 Abs. 1 und 2 PAG gestützt werden. Darin sei kein Verstoß gegen das Zitiergebot zu sehen, da Art. 10 GG hinsichtlich seines Inhalts jede Art von Fernmelderecht vor Eingriffen der öffentlichen Gewalt schütze, das Grundrecht aber keinen Anspruch auf Anschluss an ein Fernmeldenetz gewähre. Dieser Ansicht ist schon deswegen kritisch zu begegnen, da die Unterbrechung regelmäßig dazu führen wird und führen soll, dass bestimmte Inhalte und Informationen nicht ausgetauscht werden.

Eine Datenerhebung mittels IMSI-Catcher über die gefährdete Person ist vorgesehen in Art. 34 a Abs. 3 PAG.

Nach Art. 34 b Abs. 2 PAG kann die Polizei Diensteanbieter zur Auskunftserteilung über die Daten der Betroffenen verpflichten. Die Übermittlung von Daten über Telekommunikationsverbindungen, die zu diesen Personen hergestellt worden sind (Zielwahlsuche)[594], darf nur angeordnet werden, wenn die Erforschung des Sachverhalts oder die Ermittlung ihres Aufenthaltsorts auf andere Weise aussichtslos oder wesentlich erschwert wäre.[595] Zwar umfasst die Auskunft über die Verbindungsdaten auch die Ruf- oder Kennnummer des Anrufenden[596], doch lässt sich damit nur dann eine bestimmte Person ermitteln, wenn bekannt ist, wann exakt die Kommunikation stattgefunden hat.[597] Die übrigen hier untersuchten Polizeigesetze sehen eine Zielwahlsuche nicht vor.

a) Gefahrenabwehr

Das PAG fordert das Vorliegen einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person.[598] Danach muss eine Gefahr gegeben sein, die mit hinreichender Wahrscheinlichkeit für wichtige Rechtsgüter droht. Eine einfache Körperverletzung reicht nicht aus, um die Maßnahme zu rechtfertigen, ungeachtet der zeitlichen Nähe der Rechtsgutsverletzung.[599] Für die Abwehr von Sachgefahren[600] wird eine gemeine Gefahr gefordert. Diese liegt vor, wenn für eine unbestimmte Vielzahl von Personen oder für erhebliche Sachwerte ein Schaden droht.[601] Besteht eine Gefahr für Leben oder Gesundheit einer Person, so ist auch deren Überwachung mög-

---

594 Bei der Zielwahlsuche werden die Verbindungsdaten anderer Anschlüsse (potenzieller Anrufer) nach Anrufen zum Beschuldigten oder Nachrichtenmittler gefiltert, vgl. *Nack*, in: KK, § 100 g StPO, Rn. 7.

595 Art. 34 b Abs. 2, Satz 2 PAG.

596 Vgl. § 100 g Abs. 3 Nr. 1 StPO; § 7 Nr. 3 TKÜV.

597 Vgl. dazu den Beschluss des LG Kaiserslautern vom 13.08.2004 in NJW 2005, 443 f. Das Auskunftsersuchen kann bei einer Zielwahlsuche beispielsweise auf die Verbindungsdaten von Gesprächen gerichtet sein, die aus dem Ausland eingehen. U.a. dieses Auskunftsverlangen lag der Entscheidung des BVerfG in NJW 2003, 1787 ff. zugrunde.

598 Durch das Merkmal „dringende Gefahr“ will der Gesetzgeber die Beachtung des Verhältnismäßigkeitsgrundsatzes zusätzlich betonen und eine Begrenzung gewährleisten, soweit mangels einer schwerwiegenden Straftat, die verhütet bzw. unterbunden werden soll, keine weiteren einschränkenden Merkmale für die konkrete Gefahr für die jeweiligen Rechtsgüter vorhanden sind, vgl. LT-Drucks. Bayern 15/4097, S. 3. Der ursprüngliche Gesetzentwurf sah noch eine „einfache Gefahrenlage“ vor, vgl. LT-Drucks. Bayern 15/2096, S. 15.

599 Vgl. LT-Drucks. Bayern 15/4097, S. 3.

600 Das PAG lässt als einziges der hier untersuchten Polizeigesetz eine Überwachung bei einer Sachgefahr zu.

601 Vgl. *Schmidbauer*, in: Schmidbauer/Steiner/Roese, Art. 11 PAG, Rn. 55.

lich.[602] Kommunikationsverbindungen Dritter dürfen unterbrochen werden, wenn eine gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person nicht durch andere Mittel abgewendet werden kann.[603]

b) Straftatenverhütung

Die schwerwiegenden Straftaten, bei denen ein Begehungsverdacht die Anordnung einer Telekommunikationsüberwachung ermöglicht, werden in § 30 Abs. 5, Satz 1 PAG abschließend aufgezählt. Es soll sich dabei um hinreichend gewichtige Delikte handeln, die den Bereich mittlerer Kriminalität überschreiten oder zumindest an dessen Obergrenze liegen und daher geeignet sind, im Interesse der Verhinderung einer Straftat einen Eingriff in die Fernmeldefreiheit zu rechtfertigen.[604]

Straftaten nach § 30 Abs. 5, Satz 1 PAG sind solche des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaats oder des Landesverrats und der Gefährdung der äußeren Sicherheit, Straftaten gegen die öffentliche Ordnung, gegen die sexuelle Selbstbestimmung, gegen das Leben und die persönliche Freiheit, gemeingefährliche Straftaten, Verbrechen gegen die Menschlichkeit und Kriegsverbrechen, Straftaten nach dem Waffengesetz und dem Kriegswaffenkontrollgesetz sowie Straftaten nach dem Betäubungsmittelgesetz. Eine Telekommunikationsüberwachung kommt dann in Betracht, wenn konkrete Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass eine Person diese Straftaten begehen wird.[605] Erforderlich ist, dass aufgrund bestimmter Tatsachen ein konkreter, in der Entwicklung befindlicher Vorgang aufgrund bestimmter Tatsachen festgestellt werden kann, der für sich geeignet ist, die Annahme zu rechtfertigen, dass eine Person eine schwerwiegende Straftat begehen wird. Kon-

---

602 Art. 34 a Abs. 3, Satz 1 Nr. 1 PAG.

603 Als Beispiel führt die Gesetzesbegründung Entführungen an, bei denen die Kommunikation des Geiselnehmers mit Komplizen außerhalb des Tatorts über die Mobiltelefone Dritter erfolgt, vgl. LT-Drucks. Bayern 15/2096, S. 58.

604 Vgl. LT-Drucks. Bayern 15/2096, S. 52. Mit § 30 Abs. 5, Satz 1 PAG wurden die Straftaten ins PAG aufgenommen, zu deren Verhinderung nach Meinung des Gesetzgebers Grundrechtseingriffe insbesondere in Art. 10 und Art. 13 GG zulässig sind, vgl. LT-Drucks. Bayern 15/2096, S. 31. Vgl. zu den Änderungen aufgrund des BVerfG-Urteils zum „Großen Lauschangriff“ LT-Drucks. Bayern 15/4097, S. 2.

605 Im Zuge des BVerfG-Urteils zum Nds.SOG hat der bayerische Gesetzgeber die Eingriffsvoraussetzungen verdeutlicht, vgl. LT-Drucks. Bayern 15/4097, S. 4.

krete Vorbereitungshandlung ist jede die schwerwiegende Straftat objektiv fördernde Tätigkeit. Dazu sind insbesondere konkrete Planungstätigkeiten zu rechnen.[606]

Die Gesetzesbegründung statuiert, dass im konkreten Einzelfall unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit gemäß Art. 4 PAG und der Einschränkung, die hinsichtlich der Tatsachengrundlage und der Begründetheit der Gefahrprognose gesetzlich vorgesehen sind, eine Abwägung zu treffen ist. Dabei soll zu berücksichtigen sein, dass das Gewicht des durch die Strafnorm geschützten Rechtsguts und die Anforderung an die Wahrscheinlichkeit des Eintritts der Rechtsgutsverletzung in einem umgekehrten Verhältnis stehen. Bei überragend wichtigen Gütern genügen geringere Anhaltspunkte, während bei einem weniger bedeutsamen Rechtsgut höhere Anforderungen an die Begründetheit der Annahme, dass die Straftat verwirklicht wird, zu stellen sind.[607]

c) Adressaten/Kontakt- und Begleitpersonen

Für die Telekommunikationsüberwachung übernimmt das PAG nicht den Begriff der „Kontakt- und Begleitpersonen“ in Art. 33 Abs. 3 Nr. 2 PAG[608]. Adressaten der Maßnahmen nach Art. 34 a und Art. 34 b PAG können neben Störern und potenziellen Straftätern Personen sein, die für diese Mitteilungen entgegennehmen oder weitergeben oder deren Kommunikationseinrichtungen der potenzielle Straftäter benutzt.[609] Vom Wortlaut der Norm ist auch umfasst, dass der Störer die Kommunikationseinrichtung ohne Kenntnis der betroffenen Person benutzt bzw. bei seiner „Botentätigkeit“ „gutgläubig“ ist.

Andere Personen können keine Maßnahmeadressaten nach Art. 34 a Abs. 1 PAG sein und dürfen daher nur dann von der Maßnahme betroffen werden, wenn dies unvermeidbar ist.[610]

---

606 Vgl. LT-Drucks. 15/4097, S. 4. Das BVerfG hat in seinem Urteil zum Nds.SOG ausgeführt, dass die Anforderungen an das Gewicht des Schutzgutes und die Gefährlichkeit der erwarteten Verletzungshandlung steigen, wenn nicht einmal an Planungs- oder sonstige Vorbereitungshandlungen angeknüpft wird, vgl. BVerfGE 113, 349 (386 f.).

607 Vgl. LT-Drucks. Bayern 15/2096, S. 52.

608 Nach Art. 33 Abs. 3 Nr. 2 PAG sind Kontakt- oder Begleitpersonen von Datenerhebungsmaßnahmen Betroffene, die mit Straftatverdächtigen nach Kenntnis der Polizei in Verbindung stehen, ohne dass ihre Beteiligung an strafbaren Handlungen zu diesem Zeitpunkt für die Polizei erkennbar ist.

609 Art. 34 a Abs. 1 Nr. 2 b) und c) PAG.

610 Weil sie Kommunikationspartner des Adressaten sind, vgl. LT-Drucks. Bayern 15/2096. S. 52 f. Eine Überwachung der gefährdeten Person ist im Fall des Art. 34 a Abs. 3, Satz 1 PAG möglich.

d) Sonstige Voraussetzungen

Das PAG enthält differenzierte Vorschriften über die Befristung der Telekommunikationsüberwachung in Art. 34c Abs. 3, Satz 4 PAG. So richtet sich die Dauer der Befristung nach der Schwere des Eingriffs und reicht von drei Tagen[611] über zwei Wochen[612] bis zu einem Monat.[613] Eine Verlängerung ist um jeweils nicht mehr als den genannten Zeitraum möglich.[614] Die Maßnahme ist unverzüglich zu beenden, wenn die Anordnungsvoraussetzungen nicht mehr fortbestehen; die Beendigung ist auch dem Richter mitzuteilen.[615]

Das PAG trifft keine Aussage über den rückwirkenden Zeitraum, innerhalb dessen Auskunft über Telekommunikationsdaten erlangt werden kann. Es gilt daher der Zeitraum von 6 Monaten für den die Telekommunikationsunternehmen die Daten zulässigerweise speichern dürfen bzw. müssen.[616]

Als Ausprägung des Verhältnismäßigkeitsgrundsatzes bestimmt Art. 34 a Abs. 1, Satz 2 PAG, dass Datenerhebungen nach Art. 34 a Abs. 1 PAG nur durchgeführt werden dürfen, wenn die Erfüllung einer polizeilichen Aufgabe auf andere Weise aussichtslos oder wesentlich erschwert wäre.[617]

2. Die Verfahrensanforderungen

Das PAG sieht durch einen Verweis in Art. 34 c Abs. 1 PAG auf die Vorschrift des Art. 34 Abs. 4, Sätze 1 und 2 PAG vor, dass die Telekommunikationsüberwachungsmaßnahmen nur durch einen Richter angeordnet werden dürfen.[618] Anderes gilt bei Gefahr im Verzug; dabei

---

611 In den Fällen des Art. 34 a Abs. 4, Satz 2 PAG, welcher die Kommunikationsunterbrechung Dritter regelt.

612 Im Fall des Art. 34 a Abs. 4, Satz 1 PAG, welcher die Kommunikationsunterbrechung der in Art. 34 a Abs. 1 PAG genannten Personen regelt.

613 Die zulässige Anordnungsdauer orientiert sich für die übrigen Überwachungsmaßnahmen an der Regelung für die Wohnraumüberwachung. Die Fristen für die Telekommunikationsunterbrechung und -verhinderung sind vor dem Hintergrund des Übermaßverbotes kürzer, vgl. LT-Drucks. Bayern 15/2096, S. 62.

614 Art. 34 c Abs. 3, Satz 5 PAG.

615 Art. 34 c Abs. 3, Satz 6 PAG.

616 Vgl. § 97 Abs. 3, Satz 3 TKG und § 113 a Abs. 1 TKG.

617 Damit ist die Erhebung von Inhaltsdaten gegenüber anderen Maßnahmen, mit Ausnahme der Wohnraumüberwachung, die den schwereren Grundrechtseingriff darstellt, subsidiär, so LT-Drucks. Bayern 15/2096, S. 53. Der Subsidiaritätsgrundsatz ist weiter verankert in Art. 34 a Abs. 1, Satz 3; Absatz 4, Satz 2 und Art. 34 b Abs. 2, Satz 2 PAG.

618 Die richterliche Entscheidung wurde in Anbetracht der hohen Bedeutung des Fernmeldegeheimnisses vorgesehen, vgl. LT-Drucks. Bayern 15/2096, S. 61.

genügt die Anordnung durch die in Art. 33 Abs. 5, Satz 1 PAG genannten Dienststellenleiter. Die Bestätigung durch den Richter ist aber unverzüglich nachzuholen.[619] Zuständig für die Anordnung ist das Amtsgericht, in dessen Bezirk die beantragende Polizeidienststelle ihren Sitz hat.[620]

Für Maßnahmen nach Art. 34 a Abs. 3 PAG, die ausschließlich dazu dienen, den Aufenthaltsort einer dort genannten Person zu ermitteln, gilt die Besonderheit, dass sie auch durch die Dienststellenleiter der in Art. 4 Abs. 2, Satz 1 Nr. 1 bis 3 BayPOG genannten Dienststellen[621] oder das Landeskriminalamt angeordnet werden können. Diese können die Anordnungsbefugnis auf besondere Beauftragte übertragen.[622] Einen Richtervorbehalt sieht der bayerische Gesetzgeber in diesen Fällen nicht als geboten an, da die Maßnahmen regelmäßig besonders eilbedürftig seien und im Interesse des Betroffenen liegen würden.[623]

Die Anordnungen sind schriftlich zu erlassen und zu begründen.[624] Die Anordnung muss Namen und Anschrift des Betroffenen, gegen den sich die Maßnahme richtet sowie die Rufnummer oder eine andere Kennung des Telekommunikationsanschlusses oder des Endgerätes enthalten. In der Anordnung müssen zudem Art, Umfang und Dauer der Maßnahme genau bestimmt sein.[625] Im Falle einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person genügt eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation.[626] Als Beispiel genannt wird in der Gesetzesbegründung die Unterbrechung des Mobilfunkverkehrs bei einer Geiselnahme, um eine mögliche Kommunikation zwischen dem unbekannten Täter und seinen Komplizen zu verhindern.[627]

---

619 Die Anordnung bleibt solange wirksam, bis die richterliche Entscheidung vorliegt. Sie ist jedoch vom Anordnenden schon vorher selbst aufzuheben, wenn sich herausstellt, dass der zugrunde liegende Verdacht unbegründet ist, so *Honnacker/Beinhofer*, Art. 34 PAG, Rn. 7, für die Wohnraumüberwachung.

620 Für das Verfahren gelten die Vorschriften des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend, Art. 34 c Abs. 1; Art. 34 Abs. 4, Satz 2; Art. 24 Abs. 1, Satz 3 PAG.

621 Art. 4 Abs. 2 BayPOG lautet: Die Landespolizei gliedert sich in (Nr. 1) Präsidien, die dem Staatsministerium des Inneren unmittelbar nachgeordnet sind, (Nr. 2) Direktionen, (Nr. 3) Inspektionen und (Nr. 4) soweit erforderlich Stationen.

622 Art. 34 c Abs. 2 PAG.

623 Vgl. LT-Drucks. Bayern 15/2096, S. 61. Die Datenerhebung liegt regelmäßig im Interesse der betroffenen Person, da in diesen Fällen eine Gefahr für Leben oder Gesundheit der betroffenen Person besteht.

624 Die Schriftlichkeit soll neben der Beweiswirkung eine Warnfunktion haben, vgl. LT-Drucks. Bayern 15/2096, S.62.

625 Art. 34 c Abs. 3, Satz 3 PAG.

626 Art. 34 c Abs. 3, Satz 2, 2. HS PAG.

627 Vgl. LT-Drucks. Bayern 15/2096, S.62.

3. Die Regelungen in den übrigen Polizeigesetzen

a) Gefahrenabwehr

Die Anforderungen an die Gefahrenlage sind in den jeweiligen Polizeigesetzen unterschiedlich ausgestaltet. So ist die Anordnung der präventiven Telekommunikationsüberwachung in Niedersachsen, Rheinland-Pfalz und Hessen nur zulässig bei Vorliegen einer gegenwärtigen Gefahr.[628] Das Nds.SOG und das HSOG sehen dabei als zu schützende Rechtsgüter den Leib, das Leben und die Freiheit einer Person vor[629], während § 31 POG eine weitere Beschränkung auf die Schutzgüter Leib und Leben einer Person vornimmt. Diese Einschränkung hat auch das Nds.SOG vorgenommen, soweit es um den Einsatz des IMSI-Catchers geht. In Rheinland-Pfalz und Hessen ist der Einsatz des IMSI-Catchers unter den gleichen Voraussetzungen vorgesehen wie die Auskunftserteilung und Inhaltsüberwachung.

§ 34 a Abs. 1 Nr. 2 ThPAG hält dagegen eine (einfache) Gefahrenlage für den Bestand oder die Sicherheit des Bundes oder eines Landes[630] oder für Leben, Gesundheit oder Freiheit einer Person[631] für ausreichend, um eine präventive Telekommunikationsüberwachung durchführen zu können.[632]

---

628 Der Begriff der gegenwärtigen Gefahr ist legaldefiniert in § 2 Nr. 1 b) Nds.SOG. Danach bedeutet eine gegenwärtige Gefahrenlage eine Gefahr, bei der die Einwirkung des schädigenden Ereignisses bereits begonnen hat oder bei der diese Einwirkung unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzender Wahrscheinlichkeit bevorsteht.

629 Nach § 2 Nr. 1 d) Nds.SOG droht eine Gefahr für Leib und Leben bei einer nicht nur leichten Körperverletzung oder dem Tod.

630 Eine Gefährdung des Bestandes oder der Sicherheit des Bundes oder eines Landes liegt dann vor, wenn die Freiheit des Bundes oder Landes von fremder Herrschaft aufgehoben, ihre staatliche Einheit beseitigt, ein zu ihnen gehörendes Gebiet abgetrennt oder Bund, Länder oder deren Einrichtungen in ihrer Funktionsfähigkeit erheblich beeinträchtigt werden, vgl. *Ebert/Honnacker/Seel*, § 34 a ThPAG, Rn. 30.

631 Unter dem Begriff der „Gefahr für Leib und Leben“ wird nicht jede drohende Körperverletzung verstanden, sondern nur schwere Verletzungen, vgl. *Ebert/Honnacker/Seel*, § 2 ThPAG, Rn. 19 e). Diesem Begriff ist die Formulierung „Gefahr für Leben und Gesundheit“ gleichzustellen.

632 Zur Telekommunikationsüberwachung im ThPAG vgl. *P.M. Huber*, ThürVBl. 2005, 1 (3 f.).

b) Straftatenverhütung[633]

§ 34 Abs. 1 Nr. 1 ThPAG verweist nicht auf den Straftatenkatalog in § 31 Abs. 5 ThPAG, sondern auf den des § 100 a StPO[634], wogegen § 33 a Nds.SOG 2005 Bezug nimmt auf seinen „eigenen" Straftatenkatalog in § 2 Nr. 10 Nds.SOG 2005. Die in § 2 Nr.10 Nds.SOG 2005 aufgeführten Straftaten betreffen Delikte gegen den Staat und die öffentliche Ordnung, die sexuelle Selbstbestimmung, Geld- und Wertzeichenfälschungen, Straftaten gegen die persönliche Freiheit und durch den Verweis auf § 138 StGB auch Raubdelikte und gemeingefährliche Straftaten. Der Organisationsaspekt wird hervorgehoben durch die banden- oder gewerbsmäßig begangen Vergehen.[635]

Durch die Formulierung in § 2 Nr. 10 b) Nds.SOG 2005„ein nach dem geschützten Rechtsgut und Strafandrohung vergleichbares Vergehen" ist der Katalog nicht abschließend. Welche Straftaten den genannten Vergehen vergleichbar sind, ist schwer einzugrenzen. Zum einen sind die durch diese Strafvorschriften geschützten Rechtsgüter höchst unterschiedlich und vielgestaltig. Zum anderen reicht der für die Delikte vorgesehene Strafrahmen von der Geldstrafe bis zu fünf oder im Einzelfall gar zehn Jahren Freiheitsstrafe.[636]

---

633 Mit Urteil vom 27.07.2005 hat das BVerfG § 33 a Abs. 1 Nr. 2 und Nr. 3 Nds.SOG für mit dem Grundgesetz unvereinbar und nichtig erklärt, vgl. BVerfGE 113, 349 ff. Durch Art. 2 des Gesetzes zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung vom 25.11.2007, Nds.GVBl. 2007, S. 654, wurden neben weiteren Änderungen die Regelungen des § 33 a Abs. 1 Nr. 2 und 3 Nds.SOG gestrichen. Die folgenden Ausführungen zu diesen Vorschriften dienen dennoch zur Verdeutlichung der Voraussetzungen, die von Verfassung wegen bei einer präventiven Telekommunikationsüberwachung zur Straftatenverhütung zu beachten sind. Vgl. zur Änderung des Nds.SOG infolge des BVerfG-Urteils den Entwurf eines Gesetzes zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung, LT-Drucks. Nds. 15/3810, S.29 ff.

634 Mit dem Merkmal „wenn Tatsachen die Annahme rechtfertigen" kommt nach der Gesetzesbegründung zum Ausdruck, dass die Datenerhebung sich nicht auf bloße Spekulationen oder Vermutungen gründet, sondern sich auf tatsächliche Begebenheiten stützt, die jederzeit nachvollzogen werden können. Der Polizei müssen konkrete und nachprüfbare Tatsachen vorliegen, die nach der Lebenserfahrung oder kriminalistischer Erfahrung bei vernünftiger Würdigung den Schluss zulassen, dass der Störer eine Katalogtat nach § 34 a Abs. 1 Nr. 1 ThPAG begehen wird, vgl. LT-Drucks. Th. 3/2128, S. 35; *Ebert/Honnacker/Seel*, § 34 a ThPAG, Rn. 29.

635 § 2 Nr. 10 c) Nds.SOG 2005. Dadurch trägt der niedersächsische Gesetzgeber seinen eigenen Vorgaben Rechnung, durch die präventive Kommunikationsüberwachung kriminellen Organisationen entgegentreten zu können, vgl. LT-Drucks. Nds. 15/240, S. 8.

636 Als Auslegungshilfe ist heranzuziehen, dass durch die Vergehen von erheblicher Bedeutung die Datenerhebung nach den §§ 33 a bis 37 Nds.SOG 2005 eröffnet wird, weshalb nur Delikte, die im Bereich zumindest mittelschwerer, anderweitig nicht aufklärbarer, insbesondere organisierter Kriminalität angesiedelt sind, in Betracht kommen, vgl. *Unger/Siefken*, in: Böhrenz/Unger/Siefken, § 2 Nds.SOG, Anm. 17. Die Strafandrohung soll dann vergleichbar sein, wenn der Strafrahmen eine Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe vorsieht, vgl. *Unger/Siefken*, in: Böhrenz/Unger/Siefken, § 2 Nds.SOG, AB 2.10.

In Rheinland-Pfalz und Hessen ist die Telekommunikationsüberwachung zu Zwecken der Straftatenverhütung nicht vorgesehen. Der rheinland-pfälzische Gesetzgeber geht dennoch davon aus, dass die Ermächtigungsgrundlage des § 31 POG auch der vorbeugenden Verbrechensbekämpfung dient,[637] da bei der Beseitigung von Gefahrenlagen auch mögliche Straftaten gegen Leib und Leben verhindert werden.[638]

Im Gegensatz dazu hebt die hessische Gesetzesbegründung ausdrücklich hervor, dass es eine Überwachung zur Bekämpfung von Straftaten im Vorfeld einer konkreten Gefahr nicht geben soll.[639] In Hessen soll die Telekommunikationsüberwachung lediglich der Abwehr unmittelbar bevorstehender Gefahren für bestimmte hochwertige Rechtsgüter dienen.[640]

c) Adressaten/Kontakt- und Begleitpersonen

Neben den potentiellen Störern und Straftätern ist in Thüringen nur noch die Überwachung von Kontakt- und Begleitpersonen zulässig. Die Legaldefinition ist in § 34 Abs. 3 Nr. 3 ThPAG enthalten.[641] Die Datenerhebung über Kontakt- und Begleitpersonen ist auf die Ge-

---

637 Vgl. Plenarprotokoll Landtag RhPf. 16/44, S. 4404.

638 Dies bestätigt das Landgericht Kaiserslautern in seinem Beschluss vom 13.08.2004, NJW 2004, 443, welches die Beschwerde gegen eine richterliche Anordnung zur Telekommunikationsüberwachung zurückgewiesen hat. Dem Gericht hat sich nach der vorliegenden Sachlage der Schluss aufgedrängt, dass ein Banküberfall geplant war. Darin hat das Landgericht eine konkrete Gefahr für Leib und Leben der Kunden und Bediensteten gesehen, da Überfälle auf Banken oder Sparkassen fast immer von bewaffneten Tätern durchgeführt werden, die dabei nicht zurückschrecken, zur Durchsetzung ihrer Forderungen anwesende Kunden oder Bedienstete des Kreditinstituts mit der Verletzung von Leib und Leben zu bedrohen.

639 Vgl. LT-Drucks. Hessen 16/2352, S. 18 f. Die Gesetzesbegründung verweist ausdrücklich auf die Regelungen in Thüringen und Niedersachsen, die der hessische Gesetzgeber für zu weitreichend hält.

640 Als Beispiele werden genannt die Feststellung des Aufenthaltsortes einer suizidgefährdeten Person und die Androhung einer Entführung oder Geiselnahme. Hierfür sieht der hessische Gesetzgeber ein unabweisbares Bedürfnis gegeben, da ein Suizid nicht unter den Katalog des § 100 a StPO fällt und die bloße Androhung noch keine Versuchstat darstellt; vgl. LT-Drucks. Hessen 16/2352, S. 19.

641 Die Legaldefinition ist durch das Änderungsgesetz im Hinblick auf die verfassungsgerichtliche Rechtsprechung präzisiert worden, vgl. LT-Drucks. Th. 3/2128, S. 10 unter Hinweis auf BayVerfGH BayVBl. 1995, 143 und SächsVerfGH NJW 1996, 1953 = DVBl. 1996, 1423. Der Wortlaut entspricht der vom Sächsischen Verfassungsgerichtshof in DVBl. 1996, 1423 (1424) LS. 7 formulierten verfassungskonformen Auslegung zum Begriff der „Kontakt- oder Begleitperson“. Durch die genaue Abfassung der Definition werden an die Qualität der Verbindung zur Zielperson höhere Anforderungen gestellt, so dass ein loser Kontakt zwischen der Zielperson und der Kontakt- bzw. Begleitperson als nicht mehr ausreichend angesehen werden kann, vgl. LT-Drucks. Th. 3/2128, S. 30; *Ebert/Honnacker/Seel*, § 34 ThPAG, Rn. 20. Als Kontakt- und Begleitpersonen sind nicht Personen anzusehen, zu denen der Störer lediglich eine flüchtige Beziehung unterhält, sondern solche, die in einem strafrechtsrelevantem Kontakt stehen und als so genannte Nachrichtenmittler auftreten, die Informationen für den Störer entgegennehmen oder weiterleiten, vgl. LT-Drucks. Th. 3/2128, S. 35; *Ebert/Honnacker/Seel*, § 34 a ThPAG, Rn. 31.

winnung von Hinweisen bezüglich der angenommenen Straftat beschränkt und muss zu deren vorbeugenden Bekämpfung zwingend erforderlich sein.[642]

Das Nds.SOG 2005 sieht neben dem Verhaltens- und Zustandsstörer, den potenziellen Straftätern sowie deren Kontakt- und Begleitpersonen, auch den Nichtstörer als Adressaten vor.[643] § 2 Nr. 11 Nds.SOG 2005 enthält die Legaldefinition der Begleit- und Kontaktpersonen.[644] Da Kontakt- und Begleitpersonen und der Nichtstörer nicht für eine Gefahr verantwortlich sind, kann eine Inanspruchnahme aufgrund der Schwere des Eingriffs nur in den Fällen des polizeilichen Notstands gemäß § 8 Nds.SOG „unerlässlich" sein.[645] Insoweit kommt nur die Erhebung solcher Daten in Betracht, die von Relevanz für den Kontakt und demnach unerlässlich für die Verhinderung der betreffenden Straftaten sind.[646]

Als einziges Polizeigesetz enthält § 31 Abs. 2, Satz 2 POG eine (zusätzliche) Regelung darüber, welche Kommunikationsanschlüsse überwacht werden dürfen. Dies sind Anschlüsse, die mit hoher Wahrscheinlichkeit vom Betroffenen selbst oder für eine Verbindungsaufnahme mit ihm genutzt werden. Die Regelung wurde vom Gesetzgeber aufgenommen, da im Bereich

---

642 Dies bedeutet zum einen, dass Daten Dritter, die keinen Bezug zu den angenommenen Straftaten aufweisen, unverzüglich zu löschen sind. Dies folgt aus § 40 Abs. 1 iVm § 45 Abs. 2, Satz 1 Nr. 1 ThPAG. Danach dürfen Daten nur gespeichert werden, wenn sie rechtmäßig erlangt worden sind. Ist dies nicht der Fall, sind sie zu löschen, vgl. *Ebert/Honnacker/Seel*, § 45 ThPAG, Rn. 3. Etwas anderes dürfte für die Verwertung von Zufallserkenntnissen nach § 34 a Abs. 6 ThPAG gelten. Zum anderen bedeutet es, dass der Zugriff auf den Nachrichtenmittler das zuletzt mögliche Mittel sein muss. Die zwingende Erforderlichkeit ist eine Ausformung der Subsidiaritätsklausel, welche sich aus der besonderen Nachrangigkeit der Heranziehung von Unbeteiligten, zu denen Kontakt- und Begleitpersonen gehören, rechtfertigt, so LT-Drucks. Th. 3/2128, S. 30.

643 § 6 Nds.SOG regelt den Verhaltensstörer, § 7 Nds.SOG den Zustandsstörer. § 8 Nds.SOG regelt die Voraussetzungen für Maßnahmen gegen Nichtstörer.

644 Danach sind Kontakt- und Begleitpersonen Personen, die mit dem potenziellen Straftäter in einer Weise in Verbindung stehen, die erwarten lässt, dass durch sie Hinweise über die angenommene Straftat gewonnen werden können. Dabei ist nicht erforderlich, dass die Kontakt- oder Begleitperson in die Pläne des potenziellen Täters eingeweiht ist, denn auch Erkenntnisse über eine arglose Kontakt- und Begleitperson können zur Verhütung einer Straftat geeignet sein. Vorausgesetzt sind aber konkrete Tatsachen für einen objektiven Tatbezug, insbesondere eine Verwicklung in den Hintergrund oder im Umfeld des Täters. Auch ein flüchtiger sozialer Kontakt kann für die Einordnung als Kontakt- oder Begleitperson ausreichen, vgl. *Unger/Siefken*, in: Böhrenz/Unger/Siefken, § 2 Nds.SOG, Anm. 19. Umfasst sein dürfte damit auch der Fall, dass der Anschluss ohne Kenntnis benutzt wird. Aufgrund des Urteils des BVerfG vom 27.07.2005, BVerGE 113, 349 ff., wurde die Vorschrift am Ende um folgenden Halbsatz ergänzt: "...weil Tatsachen die Annahme rechtfertigen, dass die Person insbesondere von der Planung oder der Vorbereitung der Straftat oder der Verwertung der Tatvorteile oder von einer einzelnen Vorbereitungshandlung Kenntnis hat oder daran wissentlich oder unwissentlich mitwirkt.", vgl. dazu LT-Drucks.Nds. 15/3810, S. 19.

645 Vgl. *Unger/Siefken*, in: Böhrenz/Unger/Siefken, §33 a Nds.SOG, Anm. 4.

646 Vgl. *Unger/Siefken*, in: Böhrenz/Unger/Siefken, §33 a Nds.SOG, Anm. 4. Über Kontakt- und Begleitpersonen dürfen insofern erheblich weniger Daten gespeichert werden, als über die primären Maßnahmenadressaten, vgl. LT-Drucks. Nds. 15/240, S. 18.

der Organisierten Kriminalität erfahrungsgemäß die Kommunikationsverbindungen (Mobiltelefone und Telefonkarten) häufig gewechselt werden.[647]

Wer Adressat der Telekommunikationsüberwachungsmaßnahmen in Hessen sein kann, ist nicht in § 15 a HSOG geregelt. Es sind daher die allgemeinen Vorschriften der §§ 6; 7 und 9 HSOG[648] heranzuziehen.[649]

d) Sonstige Voraussetzungen

Die Telekommunikationsüberwachungsmaßnahmen sind in Thüringen, Niedersachen, Rheinland-Pfalz und Hessen auf höchstens drei Monate zu befristen. Sie können um jeweils nicht mehr als drei Monate verlängert werden,[650] wobei das HSOG als einziges der untersuchten Polizeigesetze eine Obergrenze von zwölf Monaten enthält.[651] Die Auskunft über Verbindungsdaten[652] kann in Thüringen rückwirkend nur für den Zeitraum von zwei Monaten erfolgen[653], in Niedersachsen, Rheinland-Pfalz und Hessen für sechs Monate.[654] Dass die Maßnahmen unverzüglich abzubrechen sind, wenn die Anordnungsvoraussetzungen weggefallen sind, ist weder im ThPAG[655] oder Nds.SOG[656] und POG[657] noch im HSOG[658] ausdrücklich

---

647 Diese Regelung ist zu begrüßen, da mit der durch die Datenerhebung betroffenen Person nicht zwingend eine Aussage über den zu überwachenden Anschluss getroffen ist, vgl. LT-Drucks. RhPf. 14/2287, S. 48.

648 § 6 HSOG regelt den Verhaltensstörer, § 7 HSOG den Zustandsstörer und § 9 HSOG enthält die Voraussetzungen unter denen die Inanspruchnahme nicht verantwortlicher Personen zulässig ist.

649 So auch *W.-R. Schenke*, 2007, Rn. 197 c. Dazu *Graulich*, NVwZ 2005, 271 (273), der den Adressatenkreis des § 15 a HSOG als zu unbestimmt ansieht, da der Pflichtige nicht ausdrücklich genannt wird.

650 § 34 a Abs. 2, Sätze 9 und 10 ThPAG; § 33 a Abs. 4, Sätze 2 und 3 Nds.SOG; § 31 Abs. 5, Sätze 2 und 3 POG; § 15 a Abs. 4, Satz 4 HSOG.

651 § 15 Abs. 4, Satz 4 iVm § 15 Abs. 5, Satz 7 HSOG.

652 Eine rückwirkende Auskunft über Inhaltsdaten ist mangels (zulässiger) Speicherung nicht möglich.

653 § 34 a Abs. 1, Satz 2 ThPAG. Die Gesetzesbegründung sah noch 6 Monate vor, vgl. LT-Drucks. Th. 3/2128, S. 10.

654 Mangels anderweitiger Regelung ergibt sich dies aus § 97 Abs. 3, Satz 3 TKG.

655 Allerdings enthält § 34 a Abs. 3, Satz 2 ThPAG einen Verweis auf § 44 Abs. 3 ThPAG. Danach sind alle Daten zu löschen, wenn der Zweck der Maßnahme erreicht ist oder feststeht, dass er nicht erreicht werden kann. Da vor diesem Hintergrund eine weitere Überwachung kaum aufrechterhalten werden kann, kann § 34 a ThPAG nur so verstanden werden, dass die Telekommunikationsüberwachung unverzüglich abzubrechen ist, wenn die Voraussetzungen dafür nicht mehr vorliegen.

656 Lediglich aus § 38 Abs. 1, Satz 1 Nds.SOG ergibt sich, dass die Polizei rechtmäßig erhobene Daten nur speichern darf, wenn dies zu dem Zweck erforderlich ist, zu dem sie erhoben worden sind. Auch hat eine Löschung zu erfolgen, wenn die Daten zur Zweckerfüllung nicht mehr erforderlich sind, § 39 a Nds.SOG. Bei unzulässiger Speicherung sind Daten gemäß § 17 Abs. 2 Nr. 1 NDSG zu löschen. Das NDSG ist hier neben § 39 a Nds.SOG anwendbar, da diese Vorschrift eine Löschung u.a. nur bestimmt, wenn die Speicherung zur Zweckerreichung nicht (mehr) erforderlich ist, vgl. *Unger/Siefken*, in: Böhrenz/Unger/Siefken, § 39 a Nds.SOG, Anm. 4.

657 Gemäß § 31 Abs. 8 POG gilt, dass die durch die Telekommunikationsüberwachung erlangten Unterlagen unverzüglich zu vernichten sind, wenn sie nicht mehr erforderlich sind und die erlangten Daten bei einer unzulässigen Speicherung gemäß § 39 Abs. 2 Nr. 1 POG zu löschen sind.

geregelt. Lediglich für den Einsatz des IMSI-Catchers ist im POG vorgesehen, dass personenbezogene Daten Dritter, die zur Feststellung der Polizei nicht bekannter Telekommunikationsanschlüsse erhoben wurden, über den Datenabgleich zur Ermittlung der gesuchten Geräte- und Kartennummer hinaus nicht verwendet werden dürfen und nach Beendigung der Maßnahme unverzüglich zu löschen sind.[659]

Der Verhältnismäßigkeitsgrundsatz ist für die präventive Telekommunikationsüberwachung in allen Polizeigesetzen festgeschrieben. [660]

e) Verfahrensanforderungen

Richtervorbehalte sind in allen hier untersuchten Polizeigesetzen vorgesehen. Zuständig ist jeweils das Amtsgericht in dessen Bezirk die antragstellende Behörde ihren Sitz hat.[661] Das Verfahren richtet sich nach den Vorschriften der Freiwilligen Gerichtsbarkeit.[662] Bei Gefahr in Verzug und bei Form und Inhalt der richterlichen Anordnung sind jedoch unterschiedliche Regelungen vorgesehen.[663]

---

658 Nur aus den §§ 20 Abs. 3, Satz 1; 27 Abs. 2 Nr. 1 und Nr. 3, Abs. 3, Satz 1 und 3 HSOG ergibt sich, dass gespeicherte personenbezogene Daten zu löschen und die dazugehörigen Unterlagen zu vernichten sind, wenn die Datenspeicherung unzulässig ist oder die durch eine verdeckte Datenerhebung gewonnen Daten für den der Anordnung zugrunde liegenden Zweck nicht mehr erforderlich sind.

659 § 31 Abs. 3, Satz 2 POG.

660 § 34 a Abs. 1, Satz 3 ThPAG; §§ 33 a und b Nds.SOG; § 31 Abs. 1 und 2, Satz 4 POG; § 15 a Abs. 1 und 3 HSOG.

661 § 34 a Abs. 2 ThPAG; § 33 a Abs. 4 Nds.SOG; § 31 Abs. 5 POG; § 15 a Abs. 4 HSOG.

662 § 34 a Abs. 2 ThPAG; § 33 a Abs. 4, Satz 5 iVm § 19 Abs. 4, Satz 1 Nds.SOG; § 31 Abs. 5, Satz 5 iVm § 21 Abs. 1, Satz 3 POG; § 15 a Abs. 4, Satz 2 iVm § 39 Abs. 1 HSOG.

663 Soweit in Thüringen lediglich eine Auskunft über die näheren Umstände der Telekommunikation erforderlich ist, kann bei Gefahr im Verzug der Leiter des Landeskriminalamtes oder einer Polizeidirektion die Anordnung treffen, § 34 a Abs. 2, Satz 2 ThPAG. Zu den Anwendungsschwierigkeiten des Behördenvorbehalts vgl. LT-Drucks. Th. 4/249, S. 3 und ihrer Behebung durch eine Dienstanweisung des Innenministeriums, vgl. LT-Drucks. 4/972, S. 3 f. Die Anordnung des Behördenleiters tritt außer Kraft wenn sie nicht unverzüglich, spätestens jedoch binnen drei Tagen, durch den Richter bestätigt wird. Die Dreitagesfrist wird nach § 17 FGG berechnet und beginnt in dem Zeitpunkt zu laufen, wenn die behördliche Anordnung in den Kenntnisbereich des Erbringers der Telekommunikationsdienstleistung gerät, vgl. LT-Drucks. Th. 3/2128, S. 36. Die Anordnung ergeht in jedem Fall schriftlich. Sie muss Namen und Anschrift des Betroffenen, gegen den sie sich richtet oder die Rufnummer oder eine andere Kennung seines Telekommunikationsanschlusses oder seines Telekommunikationsgerätes enthalten. In ihr sind Art, Umfang und Dauer der Maßnahme zu bestimmen, vgl. § 34 a Abs. 2, Sätze 6 – 8 ThPAG.
In Niedersachsen sind in der Anordnung neben der Person, gegen die sich die Datenerhebung richtet, Art und Umfang der zu erhebenden Daten sowie die betroffenen Telekommunikationsanschlüsse zu bezeichnen; sie ist zudem zu begründen, vgl. § 33 a Abs. 4, Satz 4 Nds.SOG. Bei Gefahr im Verzug kann die Polizei die Anordnung treffen. Diese ist ebenfalls zu begründen, wie auch die Zulässigkeit der polizeilichen Anordnung selbst. Die Entscheidung trifft die Behördenleitung. Diese kann ihre Anordnungsbefugnis auf die Dienststellenleiter sowie Bedienstete des höheren Dienstes übertragen. Die richterliche Bestätigung der Anordnung ist unverzüglich zu beantragen, vgl. § 33 a Abs. 5, Satz 5 Nds.SOG. Die Anordnung der Polizei tritt außer Kraft, wenn die richterliche Bestätigung nicht innerhalb von 3 Tagen erfolgt, vgl. § 33

II. Die Anforderungen des Grundgesetzes und der EMRK

Das Grundgesetz und die EMRK sehen spezielle Anforderungen für die Einschränkung des Fernmeldegeheimnisses vor.

1. Art. 10 GG

a) Der Schutzbereich des Art. 10 GG

Die in Art. 10 GG gewährleisteten Grundrechte auf Wahrung des Brief-, Post- und Fernmeldegeheimnisses schützen die Vertraulichkeit individueller Kommunikation, wenn diese wegen der räumlichen Distanz zwischen den Beteiligten auf eine Übermittlung durch andere Stellen angewiesen ist[664] und deshalb dem Zugriff Dritter – insbesondere staatlicher Hoheitsträger – offen steht[665].

Das Fernmeldegeheimnis (moderner: Telekommunikationsgeheimnis[666]) schützt die Vertraulichkeit individueller Mitteilungen, die fernmeldetechnisch übertragen werden.[667] Es schützt in erster Linie vor der Kenntnisnahme und der Aufzeichnung des Kommunikationsinhalts.[668] Darüber hinaus erstreckt es sich aber auch auf den Kommunikationsvorgang, also die nähe-

---

a Abs. 5, Satz 6 Nds.SOG. Dient die Erhebung der Standortkennung lediglich der Ermittlung des Aufenthaltsorts der gefährdeten Person, so trifft die Polizei die Anordnung, vgl. § 33 a Abs. 6 Nds.SOG. Dies wird damit begründet, dass hierbei Eilfälle vorliegen, bei denen ein rechtzeitiges gerichtliches Einschalten nicht gelingen kann und zugleich der Grundrechtseingriff geringer ist als in den anderen Fällen; vgl. LT-Drucks. 15/3810, S. 31.
In Rheinland-Pfalz bestimmt § 31 Abs. 5, Satz 6 POG, dass bei Gefahr in Verzug die Maßnahme vorläufig durch die Behördenleitung oder einen von ihr besonders beauftragten Beamten des höheren Dienstes angeordnet werden kann und die richterliche Entscheidung unverzüglich nachzuholen ist. Nicht festgehalten ist, dass die Zulässigkeit einer polizeilichen Anordnung schriftlich zu begründen ist.
Nach § 15 a Abs. 4 HSOG bedürfen Maßnahmen der Telekommunikationsüberwachung bei Gefahr im Verzug nicht der richterlichen Anordnung. Bei Gefahr in Verzug können die Maßnahmen durch jeden Polizeivollzugsbeamten angeordnet werden. Anordnungen dieser Art bedürfen der richterlichen Bestätigung, die unverzüglich beantragt werden muss. Wird die Anordnung nicht binnen drei Tage bestätigt, tritt sie außer Kraft, vgl. *Meixner/Fredrich*, § 15 a HSOG, Rn. 4 und § 15 HSOG, Rn. 16. Ansonsten muss die schriftliche Anordnung Namen und Anschrift der Person, gegen die sie sich richtet oder die Rufnummer oder eine andere Kennung ihres Telekommunikationsanschlusses oder ihres Telekommunikationsgerätes enthalten. In ihr sind Dauer und Art der Maßnahme festzulegen, vgl. §§ 15 a Abs. 4, Satz 4; 15 Abs. 5, Satz 5 HSOG.

664 Vgl. BVerfGE 85, 386 (396); *Loewer*, in: v.Münch/Kunig (Hrsg.), Art. 10 GG, Rn. 12.

665 Vgl. *Hermes*, in: Dreier (Hrsg.), Art. 10 GG, Rn. 15; *Gusy*, JuS 1986, 89 (90 f.).

666 Vgl. *Loewer*, in: v.Münch/Kunig (Hrsg.), Art. 10 GG Rn. 18.

667 Vgl. BVerfGE 67, 157 (172); 85, 386 (396); *Hermes*, in: Dreier (Hrsg.), Art. 10 GG, Rn. 36.

668 Vgl. BVerfGE 85, 386 (396); *Hermes*, in: Dreier (Hrsg.), Art. 10 GG, Rn. 41.

ren Umstände, wie die beteiligten Personen und Anschlüsse, Datum, Dauer und Uhrzeit der fernmeldetechnischen Verbindungen.[669]

Ob die Standortfeststellung per IMSI-Catcher ebenfalls dem Schutzbereich des Art. 10 GG unterfällt, ist streitig. Das BVerfG hat dazu in seinem Nichtannahmebeschluss vom 22.08.2006 ausgeführt, dass die Feststellung des Aufenthaltsortes einer Person anhand der Positionsmeldung eingeschalteter Mobiltelefone nicht in den Schutzbereich des Art. 10 GG eingreife, sondern nur das Recht auf informationelle Selbstbestimmung tangiere.[670] Damit stellt es sich konträr zur bislang im Schrifttum und in der Fachgerichtsbarkeit vertretenen Auffassung.[671]

Das BVerfG stützt seine Entscheidung u.a. darauf, dass die näheren Umstände des Fernmeldevorgangs dem Fernmeldegeheimnis nur unterfallen würden, soweit diese Umstände überhaupt auf Kommunikationsinhalte beziehbar seien. Die Feststellung einer Geräte-oder Kartennummer bzw. des Standorts sei unabhängig von einem tatsächlich stattfindenden oder zumindest versuchten Kommunikationsvorgang zwischen Menschen.[672] Es fände lediglich ein „Kommunikationsaustausch“ zwischen Geräten statt. Dieser Kommunikations- bzw. Datenaustausch beziehe sich aber nicht auf Kommunikationsinhalte, sondern auf die Sicherung der Betriebsbereitschaft.[673]

Vom BVerfG wird jedoch verkannt, dass die Einbuchung eines Mobiltelefons in die nächstgelegene Basisstation eines Netzbetreibers Voraussetzung dafür ist, dass Telekommunikation überhaupt stattfinden kann. Damit wird die Kommunikationsbereitschaft des Handynutzers signalisiert.[674] Durch das Einloggen in das Netz eines Betreibers wird der Kommunikationsvorgang eingeleitet, der Teil des durch Art. 10 GG geschützten Geheimnisbereiches ist.[675] Mit der Garantie des Fernmeldegeheimnisses soll vermieden werden, dass Kommunikation

---

669 Vgl. aus jüngster Zeit BVerfGE 110, 33 (52 f.); BVerfGE 113, 349 (364 f.).

670 Vgl. BVerfG NJW 2007, 351 ff.

671 Vgl. BGH NJW 2001, 1587; VG Darmstadt NJW 2001, 2273 (2274); *Gusy*, in: v.Mangoldt/Klein/Starck, Art. 10 GG, Rn. 45; *Jarass*, in: Jarass/Pieroth, Art. 10 GG, Rn. 9; *Dix*, Kriminalistik 2004, 81 (83).

672 Vgl. BVerfG NJW 2007, 351 (353).

673 Vgl. BVerfG NJW 2007, 351 (353).

674 Vgl. *Nachbaur*, NJW 2007, 335 (337).

675 Für die Eröffnung des Schutzbereichs spricht nach *Saurer*, RDV 2007, 100 (102) auch die Parallel zu dem Instrument der sog. „stillen SMS“, bei der zur räumlichen Ortung ein Signal an eine bekannte Mobilfunknummer gesandt wird. Siehe auch BGH NJW 2001, 1587; VG Darmstadt NJW 2001, 2273 (2274).

unterbleibt, weil die Beteiligten eine Überwachung fürchten.[676] Wird die Mobilfunktelekommunikation zur Standortüberwachung benutzt, so besteht gerade die Gefahr, dass eine Kommunikation per Handy aus diesen Gründen unterbleibt.[677] Sollen die Beteiligten durch den Schutz des Art. 10 GG weitestgehend so gestellt werden, wie sie bei einer Kommunikation unter Anwesenden stünden[678], so muss auch die Standortdatenerfassung nach der hier vertretenen Auffassung dem Anwendungsbereich des Art. 10 GG unterfallen. Denn bei einer Kommunikation unter Anwesenden ist der Kommunikationsort Dritten regelmäßig nicht bekannt. Auch die Standortdaten unterfallen damit nach der hier vertretenen Auffassung dem Schutzbereich des Art. 10 GG.

Unerheblich ist, ob die Übertragung und Vermittlung der Telekommunikation durch private oder staatliche Betreiber erfolgt und ob diese Betreiberunternehmen öffentlich zugänglich sind oder nur einem begrenzten Teilnehmerkreis offen stehen.[679] Dem Schutz des Fernmeldegeheimnisses unterliegen deshalb auch Übermittlungsvorgänge in einem privat betriebenen Mobilfunknetz oder in einer haus- oder betriebsinternen Telefon- und Computeranlage.[680]

Nicht geschützt vom Fernmeldegeheimnis wird die Verlässlichkeit der Kommunikationswege. Das Unterbinden oder die Störung der Kommunikation unterfällt dem Schutzbereich des Art. 2 Abs. 1 GG.[681]

b) Der Eingriff in Art. 10 GG

In seiner Funktion als klassisches Abwehrrecht gegen den Staat schützt Art. 10 GG die Beteiligten des fernmeldetechnisch vermittelten Kommunikationsvorgangs vor hoheitlichen Eingriffen durch Strafverfolgungsorgane, Sicherheitsbehörden und andere gemäß Art. 1 Abs. 3 GG unmittelbar grundrechtsgebundene Hoheitsträger.[682]

---

676 Vgl. *Pagenkopf*, in: Sachs (Hrsg.), Art. 10 GG, Rn. 14; *Nachbaur*, NJW 2007, 335 (337); *Saurer*, RDV 2007, 100 (102).

677 Vgl. *Schenke*, AöR 125 (2000), 1 (20 f.); *Nachbaur*, NJW 2007, 335 (337); *Saurer*, RDV 2007, 100 (102).

678 Vgl. BVerfG NJW 2007, 351 (353).

679 Vgl. *Hermes*, in: Dreier (Hrsg.), Art. 10 GG Rn. 37; *Pagenkopf*, in: Sachs (Hrsg.), Art. 10 GG, Rn. 14 a; *Gröpl*, ZRP 1995, 13 (14).

680 Vgl. *Hermes*, in: Dreier (Hrsg.), Art. 10 GG Rn. 37; *Jarass*, in: Jarass/Pieroth, Art. 10 GG, Rn. 7.

681 Vgl. *Pagenkopf*, in: Sachs (Hrsg.), Art. 10 Rn. 52; *Hermes*, in: Dreier (Hrsg.), Art. 10 GG, Rn. 95.

682 Vgl. *Hermes*, in: Dreier (Hrsg.), Art. 10 GG, Rn. 47. Den Telekommunikationsunternehmen wird dieser Geheimnisschutz durch das TKG auferlegt.

Ein Eingriff in Art. 10 GG liegt vor, wenn staatliche Stellen sich ohne Zustimmung der Beteiligten[683] Kenntnis von dem Inhalt oder den Umständen eines Kommunikationsvorgangs verschaffen, die so erlangten Informationen speichern, verwerten oder weitergeben.[684]

Bei der Überwachung und Aufzeichnung der Telekommunikation sowie dem Auskunftsverlangen über Verbindungsdaten handelt es sich um den klassischen Fall des Eingriffs in das Fernmeldegeheimnis, der den Polizeibehörden durch die Regelungen der hier untersuchten Polizeigesetze eröffnet wird. Gleiches gilt für den Einsatz des IMSI-Catchers.

c) Die Rechtfertigung des Eingriffs

Eingriffe in Art. 10 GG sind zulässig, wenn sie auf Grund eines Gesetzes erfolgen. Dieser grundrechtliche Gesetzesvorbehalt ist in Art. 10 Abs. 2, Satz 1 GG enthalten, während die Staatsschutzklausel in Art. 10 Abs. 2, Satz 2 GG unter bestimmten Voraussetzungen eine Ausnahme von dem Grundsatz zulässt, dass dem Betroffenen ein Grundrechtseingriff offenbart werden muss und ihm hiergegen der Rechtsweg offen steht.

aa) Das Erfordernis eines Parlamentsgesetzes

Den Anforderungen des Art. 10 Abs. 1, Satz 1 GG, der bundes- oder landesgesetzliche Eingriffsermächtigungen zulässt, kann auch eine Rechtsverordnung oder Satzung genügen.[685] Allerdings führt der Vorbehalt des (Parlaments)Gesetzes regelmäßig dazu, dass die materiellen Eingriffsvoraussetzungen und grundlegenden Modalitäten durch den parlamentarischen Gesetzgeber entschieden werden müssen, so dass nur einige technische Details der näheren Regelung durch den Verordnungs- oder Satzungsgeber zugänglich sind.[686] Entsprechende Ermächtigungsnormen hat der Gesetzgeber im TKG geschaffen, auf deren Grundlage dann u.a. die Telekommunikationsüberwachungsverordnung ergangen ist.

---

683 Umstritten ist, ob die Zustimmung aller Kommunikationsteilnehmer erforderlich ist, so BVerfGE 85, 386 (398 f.); *Amelung/Pauli*, MDR 1980, 801 (803); *Jarass*, in: Jarass/Pieroth, Art. 10 GG, Rn. 13; *Gusy*, JuS 1986, 89 (94); aA BGH NJW 1994, 596 (597 ff.); *Loewer*, in: v.Münch/Kunig (Hrsg.), Art. 10 GG, Rn. 7.

684 Vgl. *Hermes*, in: Dreier (Hrsg.), Art. 10 GG, Rn. 50. Gleiches gilt, wenn die Telekommunikationsdaten zwischen Behörden weitergeben werden; vgl. dazu das Kapitel „Datenverarbeitung“ unter II. 1.b).

685 Vgl. *Schmitt Glaeser*, in: HStR VI, § 129, Rn. 74; *Jarass*, in: Jarass/Pieroth, Art.10 GG, Rn. 16.

686 Vgl. *Hermes*, in: Dreier (Hrsg.), Art. 10 GG, Rn. 58; *Loewer*, in: v.Münch/Kunig (Hrsg.), Art. 10 GG, Rn. 28.

In engem Zusammenhang mit dem Erfordernis einer klaren parlamentsgesetzlichen Ermächtigungsgrundlage steht das Zitiergebot des Art. 19 Abs. 1, Satz 2 GG. Dessen Warn- und Klarstellungsfunktion unterstützt den Zweck des Gesetzesvorbehalts, nämlich sicherzustellen, dass Notwendigkeit und Ausmaß von Eingriffen in die Grundrechte des Art. 10 Abs. 1 GG in öffentlicher parlamentarischer Debatte geklärt werden.[687] Das Zitiergebot hat jedoch in der bisherigen Rechtspraxis eine eher geringe Bedeutung entwickelt.[688] So gilt das Zitiergebot nach der Rechtsprechung des BVerfG nur für nachkonstitutionelle Gesetze.[689] Keine Geltung erlangt es auch bei Einschränkungen durch „allgemeine Gesetze“[690] oder durch „verfassungsimmanente Schranken“[691].[692] Begründet wird dies mit dem in Art. 19 Abs. 1 GG verwendeten Begriff der „Grundrechtseinschränkung“, wonach nur solche Grundrechte dem Zitiergebot unterliegen können, die aufgrund ausdrücklicher Ermächtigung vom Gesetzgeber eingeschränkt werden dürfen.[693] Über die restriktive Interpretation des Begriffs „Grundrechtseinschränkung“ hinaus, hat das BVerfG noch eine Reihe weitere Ausnahmen entwickelt, so für solche Gesetze, die bereits geltende Grundrechtsschranken unverändert oder mit geringen Abweichungen wiederholen.[694]

In der jüngsten Rechtsprechung ist allerdings ein Wandel eingetreten. So reicht es nach Ansicht des BVerfG für die Einhaltung des Zitiergebots nunmehr nicht aus, wenn das einschränkende Gesetz das einzuschränkende Grundrecht zwar zitiert, dieses Zitat aber nicht in Zusammenhang mit der einschränkenden Regelung aufgenommen wurde.[695] Durch das Zitat im Gesetzeswortlaut soll gesichert werden, dass der Gesetzgeber nur Eingriffe vornimmt, die ihm als solche bewusst sind und über deren Auswirkungen auf die betroffenen Grundrechte er sich Rechenschaft ablegt. Eine bereits enthaltene Nennung des eingeschränkten Grund-

---

687 Vgl. BVerfGE 85, 386 (403 f.).

688 Kritisch hierzu *P.M. Huber*, in: v.Mangoldt/Klein/Starck (Hrsg.), Art. 19 GG, Rn. 74 ff.; *Ipsen*, 2007, Rn. 191 ff.

689 So BVerfGE 2, 121 (122 f.) st.Rspr.

690 So die Einschränkungsmöglichkeit in Art. 5 Abs. 2 GG.

691 Anscheinend schrankenlos gewährleistete Grundrechte, wie z.B. Art. 5 Abs. 3 GG, finden ihre Grenzen im kollidierenden Verfassungsrecht, vgl. *Jarass*, in: Jarass/Pieroth, Art. 5 GG, Rn. 113 f.; *Bethge*, in: Sachs (Hrsg.), Art. 5 GG, Rn. 198.

692 Vgl. BVerfGE 28, 36 (47); E 33, 52 (77 f.) zu Art. 5 Abs. 2 GG und BVerfGE 83, 130 (154) zu Art. 5 Abs. 3 GG.

693 Vgl. BVerfGE 21, 92 (93), E 24, 367 (396 f.); E 64, 72 (79 f.); E 83, 130 (154). Zur Kritik siehe *P.M. Huber*, in: v.Mangoldt/Klein/Starck (Hrsg.), Art. 19 GG, Rn. 74 ff.; *Ipsen*, 2007, Rn. 191 ff.

694 Vgl. BVerfGE 5, 13 (16); E 15, 288 (293); E 35, 185 (189). Zur grundsätzlichen Kritik, dass der Gesetzgeber, der die frühere Grundrechtseinschränkung wiederholt, die Bestätigung nach denselben rechtlichen Maßstäben prüfen muss wie die Erstvornahme, vgl. *P.M. Huber*, in: v.Mangoldt/Klein/Starck (Hrsg.), Art. 19 GG, Rn. 74 ff.; *Stern*, Staatsrecht, Band III/2, S. 751 f.

695 Vgl. BVerfGE 113, 349 (366 f.); *Jarass*, in: Jarras/Pieroth, Art. 19 GG, Rn. 7.

rechts reicht dafür nicht aus. Auch ein bloßer Hinweis in der Gesetzesbegründung, der Gesetzgeber sei sich der Einschränkung des Grundrechts bewusst gewesen, genügt nicht.[696]

bb) Die Staatsschutzklausel des Art. 10 Abs. 2, Satz 2 GG

Art. 10 Abs. 2, Satz 2 GG[697] enthält keinen qualifizierten Gesetzesvorbehalt, sondern stellt im Gegenteil Eingriffe von sonstigen Rechtfertigungsanforderungen frei (so genannte Schrankenerweiterung oder Einschränkungsvorbehalt[698]).[699] In der Sache bestimmt die Staatsschutzklausel, dass Beeinträchtigungen des Art. 10 Abs. 1 GG, etwa das Abhören von Telefonen, den Betroffenen gegenüber dauerhaft geheim gehalten werden können und statt gerichtlichen Schutzes lediglich eine Überprüfung durch ein spezielles Kontrollorgan erfolgt. Voraussetzung ist unter anderem, dass der Ausschluss der Benachrichtigung wie des Rechtswegs im Hinblick auf diese Zwecke erforderlich ist.[700] Geheimhaltung und Ausschluss des Rechtswegs müssen verhältnismäßig sein. Daher ist eine Benachrichtigung geboten, sobald dies ohne Gefährdung des Zwecks der Beschränkung möglich ist.[701] Ist eine gerichtliche Verfahrenskontrolle nicht vorgesehen, ist erforderlich, dass ersatzweise eine Kontrolle durch unabhängige und an keine Weisungen gebundene staatliche Organe sichergestellt ist.[702] Die Kontrolle muss materiell und verfahrensmäßig der gerichtlichen Kontrolle gleichwertig sein. Sie muss den gesamten Prozess der Datenerfassung und –verwertung umfassen und ausreichend personell ausgestattet sein.[703]

cc) Der Bestimmtheitsgrundsatz

Die rechtsstaatlichen Bestimmtheitsanforderungen sind historisch gesehen insbesondere im Bereich der polizeilichen Gefahrenabwehr entwickelt und dort im Laufe der Zeit auf neue Erscheinungsformen gefahrenabwehrender Maßnahmen erstreckt worden.

---

696 Vgl. BVerfGE 113, 349 (366 f.); *Jarass*, in: Jarass/Pieroth, Art. 19 GG, Rn. 7.

697 Das BVerfG hält die Einschränkungen entgegen kritischen Stimmen aus der Literatur noch für verfassungsgemäß, so zuletzt BVerfGE 100, 313 (399).

698 So für Art. 17 a GG: *Jarass*, in: Jarass/Pieroth, Art. 17 a GG, Rn. 1.

699 Vgl. *Hermes*, in: Dreier (Hrsg.), Art. 10 GG Rn. 59; *Pieroth/Schlink*, 2007, Rn. 764.

700 Vgl. *Pagenkopf*, in: Sachs (Hrsg.), Art. 10 GG, Rn. 48.

701 Vgl. BVerfGE 30, 1 (31); *Pagenkopf*, in: Sachs (Hrsg.), Art. 10 GG, Rn. 48.

702 Vgl. BVerfGE 67, 157 (185); E 100, 313 (401).

703 BVerfGE 30, 1 (23 f.); E 100, 313 (361 f. und 401 f.).

Bei der Wahrnehmung der ihm durch Art. 10 Abs. 2 GG eingeräumten Einschränkungsmöglichkeiten ist der Gesetzgeber an die allgemeinen verfassungsrechtlichen Begrenzungen für Grundrechtseingriffe gebunden. Diese Begrenzungen sind im Hinblick auf den speziellen Gewährleistungsgehalt des Art. 10 GG zu konkretisieren, wobei auch hier die Besonderheit zum Tragen kommt, dass Art. 10 GG das Selbstbestimmungsrecht über Informationen gewährleistet und deshalb die Grundsätze heranzuziehen sind, die auch für das Grundrecht auf informationelle Selbstbestimmung gelten.[704]

Das BVerfG hat sich in jüngster Zeit mit seinem Urteil zum G-10-Gesetz[705], seinem Beschluss zum AWG[706] und seiner Entscheidung zum Nds.SOG 2005[707] mit der präventiven Telekommunikationsüberwachung auseinandergesetzt und dabei die verfassungsrechtlichen Anforderungen an die das Fernmeldegeheimnis einschränkenden Gesetze deutlich gemacht. Das Parlamentsgesetz muss die Voraussetzungen und den Umfang der Beschränkungen klar und erkennbar festlegen.[708] Dadurch soll sich der betroffene Bürger auf mögliche belastende Maßnahmen einstellen können, die gesetzesausführende Verwaltung für ihr Verhalten steuernde und begrenzende Handlungsmaßstäbe vorfinden und die Gerichte die Rechtskontrolle durchführen können.[709]

Die konkreten Anforderungen an die Klarheit und Bestimmtheit der Ermächtigung richten sich nach der Art und der Schwere des Eingriffs. Welchem Ziel dabei die Maßnahme dient, etwa der Gefahrenverhütung oder der Gefahrenabwehr, ist für die Beurteilung ihrer Schwere für den Betroffenen ohne Belang.[710] Je nach der zu erfüllenden Aufgabe findet der Gesetzgeber aber zur Rechtfertigung der Eingriffsvoraussetzungen und zu ihrer Umsetzung unterschiedliche Möglichkeiten vor. Bei der polizeilichen Gefahrenabwehr kann er an eine Gefahr, also an Tatsachen, aus denen das Bevorstehen eines schädigenden Ereignisses abzuleiten ist, anknüpfen, bei der Strafverfolgung an den Verdacht einer schon verwirklichten Straf-

---

704 Vgl. *Hermes*, in: Dreier (Hrsg.), Art. 10 GG, Rn. 62.
705 BVerfGE 100, 313 ff.
706 BVerfGE 110, 33 ff.: Das BVerfG hat die Ermächtigungen des § 39 Abs. 1 und 2 AWG zur Überwachung des Postverkehrs und der Telekommunikation im Bereich der Straftatenverhütung als nicht vereinbar mit Art. 10 GG angesehen.
707 BVerfGE 113, 349 ff.
708 Vgl. BVerfGE 100, 313 (360); E 110, 33 (53 f.); E 113, 349 (375).
709 Vgl. BVerfGE 113, 349 (376).
710 Vgl. BVerfGE 110, 33 (55).

tat.[711] Diese Anknüpfungsmöglichkeiten entfallen, soweit der Gesetzgeber die Aufgabe verfolgt, Straftaten zu verhüten oder Vorsorge für die Verfolgung zukünftig eventuell begangener Straftaten zu treffen. Das allein hindert aber nicht, in Wahrnehmung derartiger Aufgaben Eingriffe in das Grundrecht aus Art. 10 Abs. 1 GG zu ermöglichen. Der Bestimmtheitsgrundsatz setzt jedoch voraus, dass die jeweiligen Ermächtigungen handlungsbegrenzende Tatbestandsmerkmale enthalten, die einen Standard an Vorhersehbarkeit und Kontrollierbarkeit vergleichbar dem schaffen, der für die überkommenen Aufgaben der Gefahrenabwehr und der Strafverfolgung rechtsstaatlich geboten ist.[712]

Entsprechende Ermächtigungen dürfen für Zwecke der Straftatenverhütung an Tatsachen anknüpfen, die auf die Straftatenplanung schließen lassen. Dem Gesetzgeber ist es grundsätzlich erlaubt, zur Umschreibung des Anlasses und der weiteren Voraussetzungen der Straftatenverhütung unbestimmte Rechtsbegriffe zu benutzen.[713] Er hat daher die den Anlass bildenden Straftaten sowie die Anforderungen an die Verdachtstatsachen so bestimmt zu umschreiben, dass das Risiko einer Fehlprognose in dem Rahmen verbleibt, der auch für Maßnahmen der Strafverfolgung und der Gefahrenbekämpfung als verfassungsrechtlich hinnehmbar erscheint.[714]

Werden auslegungsbedürftige Begriffe verwendet, so stehen diese dem Bestimmtheitserfordernis nicht entgegen, solange die Auslegung unter Nutzung der juristischen Methodik zu bewältigen ist und die im konkreten Anwendungsfall verbleibende Ungewissheit nicht so weit geht, dass Vorhersehbarkeit und Justitiabilität des Verwaltungshandelns gefährdet sind.[715]

Das BVerfG hat festgestellt, dass der Begriff der Tatsache isoliert betrachtet hinreichend bestimmt ist. Denn er nimmt eine Abgrenzung zu bloßen Vermutungen und allgemeinen Verfahrensgrundsätzen vor, die für sich allein gerade nicht ausreichen. In Bezugnahme auf eine künftige Straftatenbegehung genügt dieses Tatbestandsmerkmal den Bestimmtheitsanforderungen aber nicht.[716] Die im Vorfeld künftiger Straftaten bestehenden Schwierigkeiten der

---

711 Vgl. BVerfGE 110, 33 (55); E 113, 349 (377).
712 Vgl. BverfGE 100, 313(376); E 110, 33 (55 f.); E 113, 349 (378).
713 Vgl. BVerfGE 110, 33 (56).
714 Vgl. BVerfGE 110, 33 (56).
715 Vgl. BVerfGE 110, 33 (56 f.).
716 Vgl. BVerfGE 113, 349 (378).

Abgrenzung eines harmlosen von dem in eine Straftatenbegehung mündendes Verhalten werden mit dem Begriff der Tatsache nicht durch einschränkende Tatbestandsmerkmale bewältigt.[717] Die Unbestimmtheit und das damit einhergehende Risiko der Fehlprognose werden auch nicht durch das Erfordernis der Straftaten von erheblicher Bedeutung vermindert. Dieses Tatbestandsmerkmal bietet keine Anknüpfungspunkte dafür, wann ein Verhalten auf die künftige Begehung solcher Straftaten hindeutet.[718]

dd) Der Grundsatz der Normenklarheit

Von der Bestimmtheit der einzelnen Rechtsnormen ist das Gebot der Klarheit des Rechts zu unterscheiden.[719] Der Gesetzesadressat muss danach den Inhalt der rechtlichen Regelungen auch ohne spezielle Kenntnisse mit hinreichender Sicherheit feststellen können.[720] Gesetze müssen widerspruchsfrei[721], verständlich[722] und praktikabel[723] sein, damit rechtliche Entscheidungen voraussehbar sind.

In seinem AWG-Beschluss ist das BVerfG zu dem Ergebnis gekommen, dass die im Außenwirtschaftsgesetz gewählte Regelungstechnik des § 39 Abs. 1 und 2 AWG mit ihren Verweisungen und Weiterverweisungen auf Strafrechtsnormen den Grundsätzen der Normenklarheit nicht genügt.[724] Zwar können Verweisungsketten in komplexen Regelungszusammenhängen gegenüber einer alternativen Umschreibung aller Eingriffsvoraussetzungen in der Eingriffsnorm selbst durchaus vorzugswürdig sein, da an Klarheit durch die Zusammenfassung in einer einzigen Norm nicht notwendig etwas gewonnen wird. Allerdings ist einfacher zu erkennen, welche Tatbestandsmerkmale erheblich sind.[725]

---

717 Vgl. BVerfGE 113, 349 (379).

718 Vgl. BVerfGE 113, 349 (379). Zwar kann ein für die Anordnung vorgesehener Richtervorbehalt die Bestimmtheitsdefizite ausgleichen, da grundsätzlich ausfüllungsbedürftige materielle Normen rechtsstaatlich eher tragbar sind, wenn durch ein formalisiertes, gerichtlich kontrolliertes Verfahren dafür gesorgt wird, dass die wesentlichen Entscheidungsfaktoren geprüft und auslegungsbedürftige Rechtsbegriffe angemessen angewandt werden. Voraussetzung ist aber, dass der Richter Anhaltspunkte, also einen Maßstab für die Prognoseentscheidung, im Gesetz vorfindet, vgl. BVerfGE 113, 349 (381). Nach Ansicht des BVerfG boten die angegriffenen Normen des Nds.SOG 2005 dem Richter ebenso wenig einen Maßstab für die Prognoseentscheidung wie der Polizei selbst.

719 Vgl. dazu *Schulze-Fielitz*, in: Dreier (Hrsg.), Art. 20 GG (Rechtsstaat), Rn. 141 ff.

720 Vgl. BVerfGE 5, 25 (31 f.); E 8, 274 (302); E 22, 330 (346); BAGE 38, 166 (174).

721 Vgl. BVerfGE 1, 14 (37); E 17, 306 (314); E 25, 216 (227).

722 Vgl. BVerfGE 14, 13 (16); E 17, 306 (314); E 47, 239 (247).

723 Vgl. BVerfGE 25, 216 (226 f.); E 78, 205 (212 f.).

724 Vgl. BVerfGE 110, 33 (57).

725 Vgl. BVerfGE 110, 33 (63).

ee) Das Verhältnismäßigkeitsprinzip

Eine herausragende Bedeutung als Grenze sowohl für den Gesetzgeber als auch für die Exekutive und die Rechtsprechung bei Auslegung und Anwendung gesetzlicher Vorschriften kommt dem Verhältnismäßigkeitsprinzip zu.[726] Daher dürfen die Einbußen an grundrechtlich geschützter Freiheit nicht in unangemessenem Verhältnis zu den Gemeinwohlzwecken stehen, denen die Grundrechtsbeschränkungen dienen.[727]

Der Gesetzgeber muss dabei zwischen Allgemein- und Individualinteressen einen angemessenen Ausgleich herbeiführen. Dabei ist auf grundrechtlicher Seite von Bedeutung, unter welchen Voraussetzungen welche und wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind. Kriterien sind hierfür die Gestaltung der Eingriffsschwellen, die Zahl der Betroffenen und die Intensität der Beeinträchtigungen. Dies hängt davon ab, ob die Gesprächsteilnehmer als Personen anonym bleiben, welche Gespräche und welche Inhalte erfasst werden können und welche Nachteile den Grundrechtsträgern aufgrund der Überwachungsmaßnahmen drohen. Auf Seiten des Gemeinwohlinteresses ist das Gewicht der Ziele und Belange maßgeblich, denen die Fernmeldeüberwachung dient. Es hängt unter anderem davon ab, wie groß die Gefahren sind, die mit Hilfe der Fernmeldeüberwachung erkannt werden sollen und wie wahrscheinlich ihr Eintritt ist.[728] Abzuwägen ist also, wie bedeutsam die Rechtsgüter sind, die mit Hilfe der Maßnahme geschützt werden sollen und wie wahrscheinlich der Eintritt einer Rechtsgutsverletzung ist.[729] Dies gilt auch für die Telekommunikationsüberwachung zur Verhinderung von Straftaten.[730]

Zur Wahrung des Verhältnismäßigkeitsgrundsatzes und der Verfassungsmäßigkeit ist der Eingriff angesichts der Sensibilität der durch die Grundrechtseingriffe erlangten Informationen auch von organisations- und verfahrensrechtlichen Sicherungen abhängig, wenn der Betroffene von dem Eingriff erst nachträglich oder überhaupt nicht Kenntnis erlangt.[731] Sowohl

---

726 Vgl. BVerfGE 65, 1 (44); E 67, 157 (173 ff.).

727 Vgl. BVerfGE 100, 313 (375 f.); E 113, 349 (382).

728 Vgl. BVerfGE 100, 313 (376).

729 Vgl. BVerfGE 113, 349 (382).

730 Im Rahmen der akustischen Wohnraumüberwachung ist das BVerfG davon ausgegangen, dass von einer besonderen Schwere einer Straftat im Sinne des Art. 13 Abs. 3 GG nur auszugehen ist, wenn sie der Gesetzgeber jedenfalls mit einer höheren Höchststrafe als fünf Jahre Freiheitsstrafe bewehrt hat, vgl. BVerfGE 109, 279 (347 f.).

731 Das BVerfG hat es in seinem BND-Urteil als verfassungsgemäß angesehen, dass eine Mitteilung in § 3 Abs. 8, Satz 1 G-10 nur eingeschränkt vorgeschrieben war. Art. 10 Abs. 2, Satz 2 iVm Art. 19 Abs. 4,

bei staatlichen Eingriffen als auch dort, wo der Staat die durch Art. 10 GG gewährleistete Vertraulichkeit zu schützen hat, sind regelmäßig organisatorische und verfahrensmäßige Vorkehrungen erforderlich, die die Einhaltung materieller Regelungen sichern. Dazu zählen die gesetzlich vorgesehenen Richtervorbehalte bei der Post- und Fernmeldeüberwachung, die, wenn nicht verfassungsrechtlich geboten, so doch jedenfalls nicht ohne Ersatz durch vergleichbare verfahrensrechtliche Vorkehrungen gestrichen werden können.[732] Ebenfalls gehören dazu die vom Bundesverfassungsgericht geforderten Kriterien, welche die Kontrolle durch die von der Volksvertretung bestellten Organe und Hilfsorgane gemäß Art. 10 Abs. 2, Satz 2 GG zu erfüllen haben.[733]

2. Art. 13 GG

a) Der Schutzbereich des Art. 13 GG

Das Grundrecht des Art. 13 GG steht in Zusammenhang mit der freien Entfaltung der Persönlichkeit und sichert die Privatheit der Wohnung als einen elementaren Lebensraum, die räumliche Sphäre, in der sich das Privatleben entfaltet.[734] Es konkretisiert das allgemeine Recht, in Ruhe gelassen zu werden und gewährleistet die Abschirmung der Privatsphäre in räumlicher Hinsicht.[735]

Satz 3 GG erlaube ein Absehen von der Mitteilung, wenn die Beschränkung des Fernmeldegeheimnisses dem Schutz der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes diene. Dies gelte jedoch nur mit der Maßgabe, dass eine nachträgliche Benachrichtigung stattfinden muss, sobald eine Gefährdung des Zwecks der Maßnahme und eine Gefährdung des Bestands oder der Sicherung des Bundes oder eines Landes ausgeschlossen werden könne. Beschränkungen, die der Früherkennung der Gefahr eines bewaffneten Angriffs dienen, seien danach verfassungsrechtlich unbedenklich. Für die mit dem Verbrechensbekämpfungsgesetz hinzugetretenen Gefahren würden diese Gesichtspunkte zwar nicht zutreffen. Insoweit greife jedoch Art. 10 Abs. 2 Satz 2 GG ein, der die Begrenzung zu anderen Zwecken zulässt. Geheimhaltungsgründe können darin bestehen, dass mit der Offenlegung von Erkenntnissen oder auch von eingesetzten Methoden, die im konkreten Fall noch geheim gehalten werden müssten, die Aufgabenwahrnehmung gefährdet werden würde, vgl. BVerfGE 100, 313 (397).

732 Vgl. *Hermes*, in: Dreier (Hrsg.), Art. 10 GG, Rn. 88 f.

733 Vgl. *Hermes*, in: Dreier (Hrsg.), Art. 10 GG, Rn. 88 f. Zur Wirksamkeit der Kontrolle gehört es, dass sich die Kontrolle auf alle Schritte des Prozesses der Fernmeldeüberwachung erstreckt. Kontrollbedürftig ist sowohl die Rechtmäßigkeit der Eingriffe als auch die Einhaltung der gesetzlichen Vorkehrungen zum Schutz des Fernmeldegeheimnisses, vgl. BVerfGE 100, 313 (362).

734 Vgl. BVerfGE 42, 212 (219); E 51, 97 (110); E 89, 1 (12); E 103, 142 (150); *Jarass*, in: Jarass/Pieroth, Art. 13 GG, Rn. 1.

735 Vgl. BVerfGE 32, 54 (72); E 65, 1 (40); E 97, 228 (265); *Jarass*, in: Jarass/Pieroth, Art. 13 GG, Rn. 1.

Als Wohnungen gelten alle Räume, die der allgemeinen Zugänglichkeit durch räumliche Abschottung entzogen und zur Stätte privaten Lebens und Wirkens gemacht sind.[736] Darunter fallen auch Arbeits-, Betriebs- und Geschäftsräume.[737] Träger des Grundrechts ist jeder unmittelbare Besitzer unabhängig von den Eigentumsverhältnissen.[738]

b) Der Eingriff in den Schutzbereich

Das Grundrecht des Art. 13 GG wird durch jede Verletzung der Privatheit der Wohnung durch staatliche Stellen beeinträchtigt. Diese Voraussetzung erfüllen Durchsuchungen sowie jedes sonstige Betreten der geschützten Räume.[739] Voraussetzung einer Durchsuchung ist das körperliche Betreten der Wohnung durch das Durchsuchungsorgan.[740] Eine Überwachung von Vorgängen in einer Wohnung von außen ohne körperliches Betreten stellt einen Eingriff dar, wenn dies mit Hilfe technischer Mittel geschieht.[741] Das Anbringen und der Gebrauch von Ton- und Bildaufzeichnungsgeräten, die das Geschehen in der überwachten Wohnung offen legen, bedeuten einen Eingriff in das Schutzgut des Art. 13 GG.[742] Technische Möglichkeiten, um die räumliche Abgrenzung einer Wohnung zu überwinden, sind Infrarotkameras, hochempfindliche Richtmikrophone und Abhörvorrichtungen.[743] Sie gestatten ein Eindringen – ähnlich dem körperlichen Betreten – in den räumlichen Individualbereich, ohne den Nutzungsberechtigten darauf aufmerksam zu machen. Die Ausspähung braucht nicht aus dem unmittelbaren Umfeld der Wohnung vorgenommen zu werden, auch eine Ausspähung aus weiter Ferne, etwa über Satellit, bedeutet einen Eingriff in Art. 13 GG.[744]

---

736 Vgl. BGHSt 44, 138 (140); *Jarass*, in: Jarass/Pieroth, Art. 13 GG, Rn. 2; *Papier*, in: Maunz/Dürig, Art. 13 GG, Rn. 11; *Gornig*, in: v.Mangoldt/Klein/Starck (Hrsg.), Art. 13 GG, Rn. 13.

737 Vgl. BVerfGE 44, 353 (371); 76, 83 (88); 96, 44 (51).

738 Vgl. *Kunig*, in: v.Münch/Kunig (Hrsg.), Art. 13 GG, Rn. 12; *Gornig*, in: v.Mangoldt/Klein/Starck (Hrsg.), Art. 13 GG, Rn. 29; *Jarass*, in: Jarass/Pieroth, Art. 13 GG, Rn. 6.

739 Vgl. BVerfG 65, 1 (40); *Jarass*, in Jarass/Pieroth, Art. 13 GG Rn. 7.

740 Vgl. *Jarass*, in Jarass/Pieroth, Art. 13 GG, Rn. 9 und 14.

741 Vgl. Art. 13 Abs. 3 - 5 GG.

742 Vgl. *Jarass*, in Jarass/Pieroth, Art. 13 GG, Rn. 7; *Gornig*, in: v.Mangoldt/Klein/Starck (Hrsg.), Art. 13 GG, Rn. 43.

743 Vgl. *Gornig*, in: v.Mangoldt/Klein/Starck (Hrsg.), Art. 13 GG, Rn. 44; *Jarass*, in Jarass/Pieroth, Art. 13 GG, Rn. 21 .

744 Vgl. *Gornig*, in: v.Mangoldt/Klein/Starck (Hrsg.), Art. 13 GG, Rn. 44; *Jarass*, in Jarass/Pieroth, Art. 13 GG Rn. 21; *Kunig*, in: v.Münch/Kunig (Hrsg.), Art. 13 GG, Rn. 17.

Eine Beobachtung von außen durch technische Mittel stellt aber nicht immer einen Eingriff dar. Erforderlich ist, dass die Datenerfassung unmittelbar das Wohngeschehen betrifft.[745] Eine Beobachtung von außen ohne technische Mittel, wie sie jedermann möglich ist, stellt in der Regel keinen Eingriff dar, weil damit die vom Grundrechtsinhaber vorgenommenen Abschirmungen nicht über das allgemeine mögliche Maß hinaus beeinträchtigt werden.[746]

Ob nun der Überwachung der Telekommunikation neben dem Eingriff in Art. 10 GG auch Eingriffsqualität gegenüber der Unverletzlichkeit der Wohnung zukommt, hängt zum einen von der Abgrenzung der beiden Schutzbereiche und zum anderen von der Feststellung ab, ob die mit der Telekommunikationsüberwachung verbundene Standortbestimmung einen Eingriff in die räumlich geschützte Privatsphäre mit Hilfe technischer Mittel bedeutet oder sich lediglich als eine Art. 13 GG nicht verletzende Observation darstellt.

aa) Abgrenzung Fernmeldegeheimnis – Unverletzlichkeit der Wohnung

Sowohl Art. 13 als auch Art. 10 GG gewährleisten den Schutz der privaten Lebensgestaltung. Von dem Schutz der Vertraulichkeit fernmeldetechnisch vermittelter Kommunikation lässt sich der Schutzbereich des Art. 13 GG danach abgrenzen, ob der Eingriff in die räumlich abgegrenzte Privatsphäre der Wohnung erfolgt oder ob in den von der Wohnung aus geführten fernmeldetechnischen Kommunikationsvorgang eingegriffen wird.[747] Genauer gesagt: eine Abgrenzung findet danach statt, ob die Durchbrechung des Geheimnisschutzes in der räumlichen Überwindung von Barrieren oder darin liegt, dass die fernmeldetechnische Übermittlung ausgenutzt wird.[748]

Wird die Überwachung eines Festnetzanschlusses innerhalb einer Wohnung angeordnet, so ist mit Beginn des Mithörens des Gesprächs auch bekannt, dass sich die betroffene Person innerhalb dieser Wohnung aufhält. Damit bei jeder Telekommunikationsüberwachung ebenfalls einen Eingriff in Art. 13 GG zu sehen, geht zu weit. Zum einen werden keine räumlichen Barrieren überwunden, sondern auf den Kommunikationsverkehr Zugriff genommen,

---

745 Vgl. *Kunig*, in: v.Münch/Kunig (Hrsg.), Art. 13 GG, Rn. 18. Vgl. zur längerfristigen Überwachung mittels Videokamera BGH StV 1998, 169 f.

746 Vgl. *Jarass*, in Jarass/Pieroth, Art. 13 GG, Rn. 8; *Ruthig*, JuS 1998, 506 (512).

747 Vgl. *Loewer*, in: v.Münch/Kunig (Hrsg.), Art. 10 GG, Rn. 55.

748 Vgl. *Hermes*, in: Dreier (Hrsg.), Art. 10 GG, Rn. 97; *Papier*, in: Maunz/Dürig, Art. 13, Rn. 149.

zum anderen werden dabei keine typischen Verhaltensweisen offen gelegt, die durch die räumliche Privatsphäre geschützt werden sollen.[749]

Bei der Überwachung eines mobilen Anschlusses ist dagegen eine differenzierte Betrachtung angezeigt. Wird die Standortkennung während eines Gesprächs übermittelt und hält sich der Betroffene dabei innerhalb einer Wohnung auf, so kann dabei nichts anderes gelten als bei der Überwachung eines Festnetzanschlusses. Ist das Mobilfunkgerät aber – ohne dass Kommunikation stattfindet – auf „Stand by" geschaltet und den Polizeibehörden dadurch die Standortbestimmung möglich und hält sich der Betroffene innerhalb seiner Wohnung auf, könnte eine Überwindung räumlicher Barrieren mit Hilfe technischer Mittel vorliegen.

Legt man die Abgrenzung zugrunde, dass Art. 13 GG dann als spezielles Grundrecht vorgeht, wenn räumliche Barrieren überwunden werden, Art. 10 GG aber einschlägig ist, wenn die fernmeldetechnische Übertragung ausgenutzt wird, ist keine andere Beurteilung geboten als im Fall des Kommunikationsvorgangs. Mit dem Einschalten des Handys ist die Kommunikationsbereitschaft des Anschlussinhabers offensichtlich. Auch der Datenempfang im „Stand by"-Betrieb unterfällt dem Schutzbereich des Art. 10 GG. Es wird der fernmeldetechnische Übermittlungsvorgang ausgenutzt, um vom „Aufenthaltsort Wohnung" erfahren zu können. Zwar kann der IMSI-Catcher begrifflich als technisches Mittel[750], das außerhalb von Wohnungen zum Einsatz kommt, eingeordnet werden. Doch setzt seine Funktionsweise stets voraus, dass sich das Mobilfunkgerät im Bereitschaftszustand befindet.[751] Eine Überwindung räumlicher Barrieren ohne die Anknüpfung an eine fernmeldetechnische Datenübermittlung ist dem IMSI-Catcher nicht möglich.

---

749 Bei der Überwachung mit Infrarotkamera können die Bewegungen innerhalb der Wohnung verfolgt werden; durch die Benutzung des Telefonanschlusses ist aber lediglich bekannt, dass sich die betroffene Person innerhalb der Wohnung aufhält. Bei der akustischen Überwachung werden Gespräche abgehört, die innerhalb der geschützten Räume verbleiben und nicht wie mittels Telefon nach außen transportiert werden sollen.

750 Nach *Mann/Müller*, ZRP 1995, 180 (181) handelt es sich bei dem Begriff des „technischen Mittels" um einen Sammelbegriff für von Menschen geschaffene Einrichtungen. Nach *Gornig*, in: v.Mangoldt/Klein/Starck (Hrsg.), Art. 13 GG Rn. 129, beschränkt sich der Begriff des technischen Mittels nicht auf die zur Zeit der Verfassungsänderung bekannten Mittel, sondern ist entwicklungsoffen.

751 Vgl. *Fox*, DuD 1997, 539; *ders.*, DuD 2002, 212(213).

bb) Wohnraumüberwachung oder Observation

In den hier untersuchten Polizeigesetzen der Länder sind die längerfristige Observation und die Standortbestimmung mit technischen Mitteln als besondere Mittel der Datenerhebung enthalten.[752] Die Datenerhebung aus Wohnungen zur Aufklärung von Vorgängen in einer Wohnung ist jeweils gesondert geregelt.[753]

Selbst wenn man den IMSI-Catcher als technisches Mittel qualifiziert, zeigt sich, dass die bloße Aufenthaltsbestimmung nicht das Grundrecht aus Art. 13 GG verletzt. Durch die punktuelle Bestimmung des Aufenthalts werden die private und höchstpersönliche Lebensgestaltung innerhalb der Wohnung nicht verletzt.[754] Durch die Bestimmung des Standorts mittels IMSI-Catcher wird der Aufenthalt innerhalb einer bestimmten Parzelle bekannt, nicht aber können Bewegungs- und Handlungsabläufe innerhalb der Wohnung beobachtet werden, wie dies mittels Infrarotkamera möglich ist. Der IMSI-Catcher erlaubt lediglich eine vergleichsweise genaue Feststellung der Position eines Handys, da er eine Funkzelle mit geringer Leistung und damit geringer Ausdehnung simuliert.[755] Es ist daher verfassungsrechtlich weder geboten, noch praktisch durchsetzbar, bei Standortbestimmungen Unterscheidungen bei den Anordnungsvoraussetzungen danach zu treffen, wo sich die zu beobachtende Person aufhält. Denn der Aufenthaltsort soll ja gerade erst durch die Standortbestimmung kenntlich gemacht werden. Nicht einzusehen ist, weshalb der Betroffene bei einer Kenntniserlangung der Behörden von seinem Aufenthaltsort besser geschützt sein soll, nur weil er sich zufällig in einer Wohnung aufhält. Die Wohnung in ihrer Eigenschaft als letzte Rückzugsmöglichkeit wird nicht verletzt, da Informationen über den bloßen Aufenthalt hinaus, nicht nach außen dringen. Da die Ortung mittels IMSI-Catcher nur funktioniert, wenn das Handy auf „stand by“ geschaltet ist, kann der IMSI-Catcher auch nicht ständig darüber Auskunft geben, ob sich die betreffende Person im Haus befindet.[756]

---

752 Vgl. § 34 Abs. 1 Nr. 1 ThPAG; § 35 Abs. 1 Nds.SOG; Art. 33 Abs. 1 Nr. 1 und 2, Abs. 3 PAG; § 28 Abs. 1 und Abs. 2 Nr. 1 und 5 POG; § 15 Abs. 1 Nr. 1, Abs. 2 HSOG.

753 Vgl. § 35 ThPAG; § 35 a Nds.SOG; Art. 34 PAG; § 29 POG; § 15 Abs. 1 und 4 HSOG.

754 Vgl. *Schwabe*, JZ 1993, 867 (871), der Art. 13 GG durch Durchsuchungen oder heimliche akustische und visuelle Mittel beeinträchtigt sieht, da dadurch Geheimnisse der Lebensführung zutage treten von der die Gesellschaft sonst niemals Kenntnis erhalten würde.

755 Vgl. *Fox*, DuD 2002, 212 (213 f.). Mit „vergleichsweise“ ist der Vergleich mit einer herkömmlichen Funkzelle gemeint, die einen Durchmesser von mehreren Kilometern haben kann.

756 Vgl. *Fox*, DuD 1997, 539; *ders.*, DuD 2002, 212(213).

Die ansatzweise vergleichbare Videoüberwachung eines Hauseingangs[757] fällt ebenfalls nicht unter Art. 13 GG, da nicht das Geschehen in der Wohnung selbst aufgezeichnet wird, sondern nur darüber Auskunft zu erlangen ist, ob die eigene Wohnung betreten oder verlassen wird.[758]

Der IMSI-Catcher ähnelt in seiner Wirkung dem Einsatz eines Peilsenders oder eines GPS.[759] Durch deren Einsatz wird in das Recht auf informationelle Selbstbestimmung eingegriffen[760], nicht aber die Lebensgestaltung innerhalb der häuslichen Privat- und Intimsphäre offengelegt. Im Gegensatz zum Peilsender kann auch nicht sichergestellt werden, ob tatsächlich der Betroffene erfasst ist, da dieser sein Handy auch verliehen oder zu Hause gelassen haben kann.

Die Standortbestimmung mittels IMSI-Catcher greift nach der hier vertretenen Auffassung daher nicht in Art. 13 GG ein.[761] Etwas anderes ergibt sich auch nicht aus den Polizeigesetzen. Zwar finden sich in den Gesetzesbegründungen Thüringens und Bayerns folgende Aussagen: „Unberührt bleiben die Eingriffsvoraussetzungen des § 35 ThPAG[762], soweit die Telekommunikationsüberwachung zur Standortbestimmung mit technischen Mitteln in oder aus Wohnungen eingesetzt wird“[763] und „Die Erforschung des Aufenthaltsortes ist bei Einhaltung der übrigen Voraussetzungen (des Art. 34 PAG[764]) ebenfalls zulässig“[765]. Von diesen Aussagen sind jedoch nicht Standortbestimmungen mittels IMSI-Catcher umfasst. Der thüringer Gesetzgeber sieht den Einsatz des IMSI-Catchers gar nicht vor. Daten über den Standort nicht ortsfester Telekommunikationsanlagen sind für ihn nur durch eine Funkzellenabfrage

---

757 Durch die Überwachung des Hauseingangs wird Kenntnis darüber erlangt, wer das Haus durch diesen Eingang betritt oder verlässt. Ob sich die Personen nicht auch eines anderen Ein- oder Ausgangs bedienen, bleibt offen. Durch die Ermittlung des „Handystandortes“ ist klar, wo sich das Handy befindet, eine zwingende Kenntnis des Aufenthaltsorts des Handybesitzers ist damit aber nicht verbunden.

758 Vgl. BGH NJW 1991, 2651 (2652).

759 Das BVerfG hat in seinem GPS-Urteil sinngemäß ausgeführt, dass es beim Einsatz des GPS um die Ortung und Aufenthaltsbestimmung mit technischen Mitteln geht. Dabei musste der Gesetzgeber aufgrund der Funktionsweise des GPS nicht davon ausgehen, dass dieses zu einem Ortungsinstrument besonderer Art und spezifischer Tiefe werden könnte, dessen Einsatz von Verfassungs wegen nur unter restriktiven Voraussetzungen gestattet werden darf, vgl. BVerfG NJW 2005, 1338 (1340).

760 Vgl. OLG Düsseldorf, NStZ 1998, 268 (269). So für die Videoüberwachung des Wohnungseingangs auch BGH NJW 1991, 2651.

761 AA *R.P. Schenke*, AöR 125 (2000), 1 (22), der Standortbestimmungen mittels IMSI-Catcher dem qualifizierten Gesetzesvorbehalt des Art. 13 Abs. 7 GG unterstellt.

762 Die Vorschrift des § 35 ThPAG enthält “Besondere Bestimmungen über den Einsatz technischer Mittel in Wohnungen”.

763 LT-Drucks. Th. 3/2128, S. 36.

764 Art. 34 PAG enthält “Besondere Bestimmungen über den Einsatz technischer Mittel in Wohnungen”.

765 LT-Drucks. Bayern 15/2096, S. 38.

zu erlangen. Da eine Funkzelle einen Durchmesser bis zu mehreren Kilometern haben kann[766], ist ein Eingriff in die Unverletzlichkeit der Wohnung nicht denkbar. Der bayerische Gesetzgeber hat diese Formulierung augenscheinlich im Zusammenhang mit der Aufnahme von Gesprächen innerhalb einer Wohnung gesetzt, wodurch auch der Aufenthalt der Gesprächspartner bekannt ist.[767] Beim IMSI-Catcher ist Anknüpfungspunkt aber nicht die Wohnung, sondern das Mobiltelefon. Wohnraum kann mit dem IMSI-Catcher nicht überwacht werden, da er lediglich darüber Auskunft gibt, wo sich ein Handy ungefähr befindet.[768]

3. Das Recht auf informationelle Selbstbestimmung

a) Der Schutzbereich des Rechts auf informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung ist Bestandteil und Ausprägung des Allgemeinen Persönlichkeitsrechts. Das Allgemeine Persönlichkeitsrecht als eine den speziellen Freiheitsgrundrechten angenäherte Grundrechtsgarantie ist ein Produkt richterlicher Rechtsfortbildung.[769] Nach der Rechtsprechung des BVerfG findet es seine Grundlage in Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG.[770] Im Unterschied zur unbegrenzten Weite der allgemeinen Handlungsfreiheit handelt es sich um engere Tatbestände, die der Sicherung personaler Autonomie im Sinne eines Integritätsschutzes dienen.[771]

Das Allgemeine Persönlichkeitsrecht gewährleistet die engere persönliche Lebenssphäre und die Erhaltung ihrer Grundbedingungen, die sich durch die traditionelle Freiheitsgarantien nicht abschließend erfassen lassen. Notwendig ist dies im Hinblick auf moderne Entwicklungen und die mit ihnen verbundenen neuen Gefährdungen für den Schutz der menschlichen

---

766 Vgl. *Fox*, DuD 2002, 212 (213).

767 Vgl. LT-Drucks. Bayern 15/2096, S. 38.

768 Auch *Roos*, § 28 POG, Rn. 10, geht davon aus, dass für eine Standortbestimmung durch die Nutzung eines Mobiltelefons die Ermächtigungsgrundlage zur Telekommunikationsüberwachung einschlägig ist.

769 Vgl. *Dreier*, in: Dreier (Hrsg.), Art. 2 Abs. 1 GG, Rn. 68; zur Genese in der Rechtsprechung des BGH, beginnend mit dem „Schachtbrief"-Urteil, BGHZ 13, 334 (337 ff.); *v.Caemmerer*, in: FS für v.Hippel, S.27 ff.; *Brandner*, JZ 1983, 689 ff.; *Jarass*, NJW 1989, 857 (858 ff.). Bundesverfassungsgerichtlich ist die Figur spätestens mit der sog. „Mikrozensus"-Entscheidung des BVerfG akzeptiert: BVerfGE 27, 1 (6 ff.). Siehe auch *Walden*, 1996, S. 58 ff.

770 St.Rspr.; siehe BVerfGE 35, 202 (219); E 72 155 (170); E 82, 236 (269); E 90, 263 (270).

771 Vgl. *Dreier*, in: Dreier (Hrsg.), Art. 2 Abs. 1 GG, Rn. 68.

Persönlichkeit.[772] Es wird konkretisiert durch einzelne Fallgruppen[773], zu denen auch das Recht auf informationelle Selbstbestimmung zählt.

Das Recht auf informationelle Selbstbestimmung ist die Reaktion auf staatliche Informationseingriffe und die neuartigen Möglichkeiten der Datenverarbeitung, deren Gefährdungspotenzial vor allem in der Verfügbarkeit, Transferierbarkeit und Kombinationsmöglichkeit der einmal erhobenen Einzeldaten (Erstellung von Persönlichkeitsprofilen) liegt.[774] Das BVerfG folgert daraus, „die Befugnis des Einzelnen grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden".[775]

b) Der Eingriff in den Schutzbereich

Staatliche Informationserhebungen und –verarbeitungen stellen Eingriffe klassischer Art in das Recht auf informationelle Selbstbestimmung dar; gleiches gilt für den Zwang zur Preisgabe von Sachverhalten, Daten oder Unterlagen.[776] Die mittels IMSI-Catcher mögliche Standortbestimmung ist als Eingriff in das Recht auf informationelle Selbstbestimmung zu qualifizieren.

Der Geheimnisschutz des Art. 10 GG weist eine besondere Nähe zum Schutzbereich des allgemeinen Persönlichkeitsrechts auf. Das durch Art. 10 GG gewährte Fernmeldegeheimnis schützt einen Ausschnitt hieraus, nämlich die persönlichen Äußerungen, die der Urheber unter Zuhilfenahme Dritter an einen anderen übermittelt.[777] Liegen diese Voraussetzungen vor, ist Art. 10 GG das gegenüber Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG speziellere Grundrecht.[778] Gleiches gilt auch für das aus Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG abgeleitete Recht auf informationelle Selbstbestimmung.[779] Da sich die Schutzbereiche aber nur teilweise über-

---

772 Vgl. BVerfGE 54, 148 (153); *Manssen*, 2005, Rn. 245 ff.; *Gallwas*, 1995, Rn. 344 ff.; siehe auch *Degenhardt*, JuS 1992, 361 ff.; *Ehmann*, JuS 1997, 193 ff.

773 Zu den einzelnen Fallgruppen und der Abgrenzung zum privaten Persönlichkeitsrecht *Jarass*, NJW 1989, 857; *Pieroth/Schlink*, 2007, Rn. 373 ff.: Das Allgemeine Persönlichkeitsrecht verbringt das Recht der Selbstbestimmung, Selbstbewahrung und Selbstdarstellung.

774 Vgl. *Dreier*, in: Dreier (Hrsg.), Art. 2 Abs. 1 GG, Rn. 78.

775 BVerfGE 65, 1 (42); 80, 367 (373); 103, 21 (33).

776 Vgl. *Dreier*, in: Dreier (Hrsg.), Art. 2 Abs. 1 GG, Rn. 83; siehe auch *Gusy*, VerwArch 74 (1983), 91 ff; *Rosenbaum*, Jura 1988, 178 ff.; *Pitschas/Aulehner*, NJW 1989, 2353 ff.; *R. Krüger*, DÖV 1990, 641 ff.

777 Vgl. *Hermes*, in: Dreier (Hrsg.), Art. 10 GG Rn. 94.

778 Vgl. BVerfGE 100, 313 (358); BVerfGE 67, 157 (171); *Hermes*, in: Dreier (Hrsg.), Art. 10 GG Rn. 94; *Schuppert*, in: AK-GG, Art. 10 GG, Rn. 14.

779 Vgl. *Hermes*, in: Dreier (Hrsg.), Art. 10 GG, Rn. 94.

schneiden, denn der Geheimnisschutz des Art. 10 GG erfasst einerseits nur kommunikationsbezogene Daten und berücksichtigt andererseits Übermittlungsinhalte und –umstände, die nicht in den Schutzbereich des Rechts auf informationelle Selbstbestimmung fallen, kann das Recht auf informationelle Selbstbestimmung selbstständig neben Art. 10 GG zur Anwendung kommen.[780]

Besondere Bedeutung hat dies bei der Telekommunikationsüberwachung für die Übermittlung der Funkzelle, also der Standortdaten, da diese als Verkehrsdaten nach der hier vertretenen Auffassung dem Fernmeldegeheimnis unterfallen.[781] Nach *R.P. Schenke*[782] würde ein Zurücktreten des Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG hinter die vermeintlich speziellere Freiheitsverbürgung des Art. 10 GG dem Sinngehalt und dem Eingriffsschwerpunkt der Maßnahme jedoch nicht gerecht werden. Die Möglichkeit der Erstellung von Bewegungsprofilen berühre das Grundrecht auf informationelle Selbstbestimmung in einem Bereich, der weit über den Sektor des Fernmeldegeheimnisses hinausreiche.[783] Durch die Funkzellenabfrage seien die örtlichen Veränderungen des Betroffenen und auch seine Verhaltensweisen offenkundig.[784] Je genauer sich der Aufenthaltsort eines Benutzers ermitteln lasse, umso näher rückten Standortbestimmungen in die Nähe einer geheimen polizeilichen Observation, die als solche aber keinen Berührungspunkt zu Art. 10 GG aufweise.[785]

Aus dem BND-Urteil des BVerfG ergibt sich nichts Gegenteiliges. Zwar hat es ausgeführt, dass das aus Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG folgende Recht auf informationelle Selbstbestimmung neben Art. 10 GG nicht zur Anwendung kommt, da bezogen auf den Fernmeldeverkehr Art. 10 GG eine spezielle Garantie enthält, die die allgemeine Vorschrift verdrängt.[786]

Das BVerfG führt dann allerdings aus, was unter dem Begriff „Fernmeldegeheimnis“ zu verstehen ist und subsumiert darunter den Kommunikationsinhalt, also alle mittels Fernmeldetechnik übermittelte Kommunikation und die Kommunikationsumstände, insbesondere ob,

---

780 So für das allgemeine Persönlichkeitsrecht *Murswiek*, in: Sachs (Hrsg.), Art. 2 GG, Rn. 138; *Kunig*, Jura 1993, 595 (603 f.).
781 Vgl. dieses Kapitel unter II.1.a).
782 Vgl. *R.P. Schenke*, AöR 125, 1 (23).
783 Vgl. *R.P. Schenke*, AöR 125, 1 (23). So wohl auch *Saurer*, RDV 2007, 100 (103).
784 Vgl. *R.P. Schenke*, AöR 125, 1 (23).
785 Vgl. *R.P. Schenke*, AöR 125, 1 (23).
786 Vgl. BVerfGE 100, 313 (358).

wann und wie oft zwischen welchen Personen oder Fernmeldeanschlüssen Fernmeldeverkehr stattgefunden hat oder versucht worden ist.[787] Dies stellt zwar schon aufgrund der Wortwahl keine abschließende Aufzählung dar, doch ist offensichtlich, dass das BVerfG bei seiner Abgrenzung bzw. der Annahme eines Spezialitätsverhältnisses zwischen dem Fernmeldegeheimnis und dem Recht auf informationelle Selbstbestimmung nicht die Erstellung von Bewegungsprofilen durch eine Funkzellenabfrage oder den Einsatz des IMSI-Catchers vor Augen hatte, deren Durchführung jeweils von der Kommunikationsbereitschaft des Betroffenen durch ein aktiv geschaltetes Mobilfunkgerät abhängig ist.[788]

Auch in seiner Entscheidung zum Nds.SOG 2005 betont das BVerfG, dass das allgemein aus Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG folgende Recht auf informationelle Selbstbestimmung hinter die speziellere Gewährleistung aus Art. 10 GG zurücktritt, soweit sich die Schutzbereiche überschneiden.[789] Die Überwachung mittels IMSI-Catcher war jedoch ebenfalls nicht Gegenstand der Entscheidung. Das BVerfG stellte zwar bei der Überprüfung der materiellen Verfassungsmäßigkeit fest, dass durch den Zugriff auf die Verbindungsdaten auch Standortkennungen eingeschalteter Mobilfunkendeinrichtungen übermittelt werden, die zur Erstellung von Bewegungsbildern führen können und auch, dass Verbindungsdaten erhebliche Rückschlüsse auf das Kommunikationsverhalten zulassen und die Standortkennung zur Erstellung von Bewegungsbildern führen kann, die Gewohnheiten der betroffenen Personen offen legen.[790] Die vor diesem Hintergrund gebotene Auseinandersetzung mit einer Grundrechtskonkurrenz hat es aber gerade nicht vorgenommen.

Tritt das Recht auf informationelle Selbstbestimmung hinter das Fernmeldegeheimnis jedenfalls für die Erstellung von Bewegungsprofilen und Standortbestimmungen nicht zurück, so könnte umgekehrt ein Zurücktreten des Art. 10 GG hinter Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG in Betracht kommen.

Art. 2 Abs. 1 GG iVm Art. 1 Abs. 1 GG in diesem Fall als lex specialis anzusehen, würde aber die Standortdaten als Bestandteil der Kommunikationsumstände nicht hinreichend berücksichtigen. Die Erstellung von Bewegungsprofilen wird durch die Kommunikationsbereit-

---

787 Vgl. BVerfGE 100, 313 (358).

788 Den Einsatz des IMSI-Catchers hatte es in seine Entscheidung nicht einbezogen, da das G-10-Gesetz diese Maßnahme nicht vorsieht.

789 Vgl. BVerfGE 113, 349 (364). Gleiches soll auch für Art. 5 GG gelten.

790 Vgl. BVerfGE 113, 349 (383).

schaft, das aktiv geschaltete Mobilfunkgerät ermöglicht. Auch die Information „von wo aus" Kommunikation erfolgt, berührt das Fernmeldegeheimnis. Dem ist entsprechend Rechnung zu tragen.

Auch das BVerfG hat in seiner Entscheidung zum IMSI-Catcher[791], in der es davon ausgeht, dass die Erfassung von Standortdaten mittels IMSI-Catcher nicht dem Schutzbereich des Art. 10 GG, sondern dem Recht auf informationelle Selbstbestimmung unterfallen, ausgeführt, dass das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung in einem Ergänzungsverhältnis stehen, jedenfalls soweit es um den Schutz technischer Kommunikationsdaten geht.[792]

Auszugehen ist mit *R.P. Schenke*[793] von Anwendungs- bzw. Gesetzeskonkurrenz[794], so dass die jeweiligen Grundrechte im konkreten Fall nebeneinander betroffen und nacheinander durchzuprüfen sind.[795] Überwiegend wird davon ausgegangen, dass bei Grundrechten mit unterschiedlichen Beschränkungsmöglichkeiten (so genannte schrankendivergierende Grundrechte) die Grundrechte und Grundrechtsschranken nebeneinander stehen und getrennt zu prüfen sind, im Ergebnis aber die Schrankensystematik des stärkeren, d.h. des weniger beschränkbaren, Grundrechts zu gelten habe.[796] Greifen daher die mittels IMSI-Catcher oder Funkzellenabfrage erstellten Bewegungsprofile sowohl in den Schutzbereich des Art. 10 GG als auch in das Grundrecht auf informationelle Selbstbestimmung ein, gelten die jeweils höheren Rechtfertigungsvoraussetzungen, so dass z.B. in jedem Fall ein Parlamentsgesetz Voraussetzung für eine verfassungsmäßige Beschränkung ist.[797]

---

791 BVerfG NJW 2007, 351 ff.

792 BVerfG NJW 2007, 351 (354).

793 *R.P. Schenke*, AöR 125 (2000), 1 (24), geht von Idealkonkurrenz zwischen Art. 10 und 13 GG und dem Recht auf informationelle Selbstbestimmung aus. So im Ergebnis auch *Saurer*, RDV 2007, 100 (103).

794 Zum Lösungsweg des BVerfG bei Grundrechtskonkurrenz, vgl. *Stern*, Staatsrecht, Band III/2, § 92, S. 1385 ff.

795 Vgl. *Pieroth/Schlink*, 2007, Rn. 343; *Bleckmann*, 1997, § 14, Rn. 23; *Saurer*, RDV 2007, 100 (103). Zur Problematik einer „Verstärkungswirkung" in diesen Fällen, vgl. *Manssen*, 1995, Rn. 645 f.; *Würkner*, DÖV 1992, 150 (152).

796 Vgl. *v.Münch*, 2002, Rn. 225; *Pieroth/Schlink*, 2007, Rn. 343.

797 Vgl. dieses Kapitel unter II. 1. c) aa). Das BVerfG geht in seinem Urteil zum IMSI-Catcher davon aus, dass soweit der Eingriff in das Fernmeldegeheimnis die Erlangung personenbezogener Daten betrifft, die Maßgaben, die das BVerfG aus Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG entwickelt hat, grundsätzlich auch auf die speziellere Garantie in Art. 10 Abs. 1 GG zu übertragen sind, vgl. BVerfG NJW 2007, 351 (355).

c) Die Rechtfertigung des Eingriffs

Das allgemeine Persönlichkeitsrecht unterliegt weniger weitgehenden Einschränkungsmöglichkeiten als die allgemeine Handlungsfreiheit. Gerade im Bereich der informationellen Selbstbestimmung werden förmliche Gesetze verlangt, deren Bestimmtheit vergleichsweise hohen Anforderungen unterliegen.[798]

Allgemein muss der Grundrechtsträger Einschränkungen seines Rechts nur im überwiegenden Allgemeininteresse hinnehmen. Die Einschränkung darf nicht weitergehen, als sie zum Schutz öffentlicher Interessen unerlässlich ist.[799] Je tiefer die Daten den Persönlichkeitsbereich betreffen und je umfassender die Daten genutzt werden sollen, desto strengere Anforderungen sind an den mit der Datenerfassung verfolgten Zweck und dessen gesetzliche Bestimmtheit zu stellen.[800] Hierdurch soll sichergestellt werden, dass die Daten tatsächlich nur zu einem bestimmten Zweck verwendet, insbesondere verwertet oder weitergeben werden.[801] Eine bloß allgemein formulierte Aufgabennorm genügt dem ebenso wenig wie die Berufung auf allgemeine Rechtfertigungsgründe.[802] Bei Erhebung und Verwendung individualisierter oder individualisierbarer Daten sind die Rechtfertigungsanforderungen besonders streng.[803] Je undurchsichtiger der informationelle Speicherungs- und Verwendungsvorgang für den außenstehenden Betroffenen ist, desto mehr muss der Gesetzgeber durch verfahrensbezogene Regelungen im Interesse eines vorgezogenen Rechtsschutzes für Transparenz sorgen.[804]

4. Art. 8 EMRK

Im Gegensatz zum Grundgesetz, das die Privatsphäre des Individuums durch eine Reihe von Grundrechten schützt[805], enthält die EMRK mit Art. 8 Abs. 1 eine (einzelne) spezielle Garan-

---

798 Vgl. *Dreier*, in: Dreier (Hrsg.), Art. 2 Abs. 1 GG, Rn. 86; BVerfGE 65, 1 (44); BVerwG NJW 1991, 1246 (1247); BayVGH BayVBl. 1984, 272 (275).

799 Vgl. *Di Fabio*, in: Maunz/Dürig, Art. 2 Abs. 1 GG, Rn. 181; BVerfGE 65, 1 (44); BVerfG EuGRZ 2001, 249 (252); BayVerfGH BayVBl. 1995, 143 (144).

800 Vgl. *Starck*, in: v.Mangoldt/Klein/Starck (Hrsg.), Art. 2 Abs. 1 GG, Rn. 116; *Murswiek*, in: Sachs (Hrsg.), Art. 2 Abs. 1 GG Rn. 121.

801 Vgl. *Di Fabio*, in Maunz/Dürig, Art. 2 Abs. 1 GG, Rn. 182; *Jarass*, NJW 1989, 857 (861).

802 Vgl. *Di Fabio*, in Maunz/Dürig, Art. 2 Abs. 1 GG, Rn. 182.

803 Vgl. *Di Fabio*, in Maunz/Dürig, Art. 2 Abs. 1 GG, Rn. 184.

804 Vgl. *Di Fabio*, in Maunz/Dürig, Art. 2 Abs. 1 GG, Rn. 184; *Murswiek*, in: Sachs (Hrsg.), Art. 2 Abs. 1 GG Rn. 121; BVerfGE 65, 1 (46 ff.); siehe auch *Riegel*, BayVBl. 1998, 523 (524 ff.).

805 So sind die Unverletzlichkeit der Wohnung in Art. 13 GG, das Brief-, Post- und Fernmeldegeheimnis in Art. 10 GG garantiert, Ehe und Familie finden einen besonderen Schutz in Art. 6 GG, Art. 2 Abs. 1 iVm

tie des Schutzes der Privatsphäre. Danach hat jede Person das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz. Aus dem Recht auf Achtung der Privatsphäre folgt der Anspruch, dass der Staat keine Kenntnis von der Privatsphäre eines Individuums erhält.[806] Auch die individuelle Kommunikation mit anderen ist Bestandteil der Privatsphäre. Telefongespräche im häuslichen und im geschäftlichen Bereich sind vom Schutz des Art. 8 EMRK erfasst.[807] Die Telefonüberwachung und der Einsatz anderer technischer Überwachungsgeräte stellt einen typischen Eingriff in die Privatsphäre dar.[808]

Nach Art. 8 Abs. 2 EMRK darf eine Behörde in die Ausübung des Rechts aus Art. 8 Abs. 1 EMRK eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft für die nationale und öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.
Insbesondere in den Verfahren *Klass c. Bundesrepublik Deutschland*[809], *Kopp c. Schweiz*[810] und *Weber u. Savaria c. Bundesrepublik Deutschland*[811] hat sich der EGMR mit der staatlichen Telefonüberwachung und ihrer Vereinbarkeit mit Art. 8 EMRK auseinandergesetzt.

a) Der Fall Klass c. Bundesrepublik Deutschland

Der EGMR hat in der Sache *Klass c. BRD*[812] die Hauptfrage darin gesehen, ob die gemäß dem G-10-Gesetz durchgeführte Telekommunikationsüberwachung nach Art. 8 Abs. 2 EMRK gerechtfertigt ist und dazu ausgeführt, dass Befugnisse zur geheimen Überwachung

---

Art. 1 Abs. 1 GG schützt das allgemeine Persönlichkeitsrecht mit seinem unantastbaren Bereich privater Lebensgestaltung.

806 Vgl. *Villiger*, 1999, Rn. 564.

807 Vgl. EGMR NJW 2007, 1433 (1434); *Grabenwarter*, 2005, § 22, Rn. 9.

808 Vgl. das EGMR-Urteil *Klass c. BRD*, EuGRZ 1979, 278 (284) und das EGMR-Urteil *Malone c. Großbritannien*, EuGRZ 1985, 17 (20); *Villiger*, 1999, Rn. 564; *Meyer-Ladewig*, Art. 8 EMRK, Rn. 10.

809 Urteil des EGMR vom 06.09.1978, deutsche Übersetzung veröffentlicht in EuGRZ 1979, 278 ff.

810 Urteil des EGMR vom 25.03.1998, deutsche Übersetzung in ÖJZ 1999, 115 ff. Siehe auch die Übersetzung und Zusammenfassung des Sachverhalts von *Kühne*, StV 1998, 683.

811 Urteil des EGMR vom 29.06.2006, deutsche Übersetzung veröffentlicht in NJW 2007, 1433 ff.

812 In diesem Verfahren hatte der EGMR zu entscheiden, ob Teile des G-10-Gesetzes gegen die EMRK verstoßen. Fünf deutsche Staatsangehörige rügten mit ihrer Beschwerde, dass Art. 10 Abs. 2 GG und die aufgrund dieser Vorschrift erlassenen Regelungen des G-10-Gesetzes in der Fassung vom 13.08.1968, BGBl. I, S. 949, zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses mit der Konvention nicht vereinbar seien. Sie griffen die Vorschriften insoweit an, als sie Maßnahmen erlaubten, ohne die Behörden in jedem Fall zur nachträglichen Unterrichtung der betroffenen Personen zu verpflichten und den Rechtsweg gegen die Anordnung und den Vollzug jener Maßnahmen ausschlossen.

von Bürgern, wie sie für den Polizeistaat typisch sind, nach der Konvention nur insoweit hingenommen werden können, als sie zur Erhaltung von demokratischen Einrichtungen unbedingt notwendig sind.[813] Gleichzeitig hat er betont, dass die Vertragsstaaten nicht im Namen des Kampfes gegen Spionage und Terrorismus zu jedweder Maßnahme greifen dürfen, die ihnen geeignet erscheinen.[814] Das gewählte Überwachungssystem müsse vielmehr angemessene und wirksame Garantien gegen Missbrauch enthalten.[815]

Nach Ansicht des Gerichtshofes ist dies dann der Fall, wenn die Überwachung voraussetzt, dass tatsächliche Anhaltspunkte für den Verdacht einer Straftat bestehen, die Maßnahme nur verdächtige Personen erfasst, dasselbe Ziel nicht mit anderen Maßnahmen erreicht werden kann, ein besonderes Verfahren für die Überwachung besteht und die Überwachung zeitlich beschränkt ist.[816]

b) Der Fall Kopp c. Schweiz

Der Gerichtshof hat in der Rechtssache *Kopp c. Schweiz*[817] die Anforderungen an einschränkende Maßnahmen im Sinne des Art. 8 Abs. Abs. 2 EMRK weiter präzisiert. So verlangt er,

---

813 Vgl. EGMR EuGRZ 1979, 278 (284).

814 Vgl. EGMR EuGRZ 1979, 278 (285).

815 Diese Beurteilung hängt nach Ansicht des EGMR von allen Umständen des Falles ab, wie Art, Umfang und Dauer der möglichen Maßnahmen, die für ihre Anordnung erforderlichen Gründe, die für ihre Zulassung, Ausführung und Kontrolle zuständigen Behörden und die Art des im nationalen Rechts vorgesehenen Rechtsbehelfs, vgl. EGMR EuGRZ 1979, 278 (285).

816 Der Gerichtshof hat insofern die im G-10-Gesetz enthaltenen Regelungen als genügend angesehen, vgl. EGMR 1979, 278 (285 f.). Das G-10-Gesetz entspricht seiner Ansicht nach den Vorgaben des Art. 8 Abs. 2 EMRK, da Im Hinblick auf die Art der Kontrolle und die anderen im G-10 vorgesehenen Sicherungen kommt der Gerichtshof zu dem Ergebnis, dass der Ausschluss der richterlichen Kontrolle die Grenzen dessen, was in einer demokratischen Gesellschaft als notwendig angesehen werden kann, nicht überschreitet, da mit der G-10-Kommission und dem Parlamentarischen Gremium Organe vorhanden sind, die eine wirksame und ständige Kontrolle ausüben können. Auch die nachträgliche Unterrichtung des Betroffenen, die diesem die Möglichkeit eröffnet, den Rechtsweg zu beschreiten und die nur entfällt, wenn ansonsten der Zweck der Maßnahme gefährdet ist, entspricht nach Ansicht des EGMR den Anforderungen des Art. 8 Abs. 2 EMRK. Dass Unterbleiben einer nachträglichen Bekanntgabe ist nach Meinung des EGMR mit Art. 8 Abs. 2 EMRK vereinbar, wenn es gerade dieser Umstand ist, der die Wirksamkeit des Eingriffs sicherstellt.

817 Im Fall *Kopp c. Schweiz* wurden sämtliche, geschäftlichen und privaten, Telefonanschlüsse der Züricher Rechtsanwaltskanzlei Dr. Kopp & Partner auf Antrag der Schweizer Bundesanwaltschaft und Beschluss der Anklageabteilung des Bundesgerichts in der Zeit vom 21.11.1989 bis 11.12.1989 überwacht. Herr Dr. Kopp galt in diesem Zusammenhang als Dritter, nicht aber als Verdächtiger. Herr Dr. Kopp erhob in Straßburg Beschwerde mit der Begründung, die gesetzliche Grundlage für die Abhörung fehle, da Art. 77 StPO vorsehe, dass Telefongespräche von bestimmten Personen, darunter von Anwälten, nicht abgehört werden dürfen. Der Wortlaut des Art. 77 der Schweizer StPO wird in der Übersetzung wie folgt wiedergegeben: „Rechtsanwälte können nicht zur Aussage über Geheimnisse, welche ihnen Kraft Berufes anvertraut wurden, verhalten werden.“, vgl. EGMR ÖJZ 1999, 115 (116).

dass die Maßnahmen eine Grundlage im nationalen Recht haben und – was die Qualität des fraglichen Gesetzes betrifft – dieses der betroffenen Person zugänglich und die Person darüber hinaus in der Lage sein muss, die Konsequenzen des Gesetzes für sie vorauszusehen. Weiter muss das Gesetz mit den Grundsätzen der Rechtsstaatlichkeit übereinstimmen.[818]

Wenn es um geheime Maßnahmen der Überwachung oder der Kommunikationsbeeinträchtigung von Seiten der Behörden gehe, muss nach Ansicht des EGMR das nationale Recht wegen des Fehlens einer öffentlichen Kontrolle und der Gefahr eines Machtmissbrauchs einen Schutz des Individuums vor willkürlicher Beeinträchtigung der Rechte aus Art. 8 EMRK vorsehen.[819] Daher muss das nationale Recht ausreichend klar in seinen Formulierungen sein, um den Bürgern einen angemessenen Hinweis hinsichtlich der Umstände und Bedingungen zu geben, unter denen die Behörden ermächtigt sind, zu solchen geheimen Maßnahmen zu greifen.[820]

c) Der Fall Weber u. Savaria c. Bundesrepublik Deutschland

Der Gerichtshof hat in dieser Rechtssache[821] klar gestellt, dass die bloße Existenz von Gesetzen, die eine geheime Überwachung des Fernmeldeverkehrs gestatten, eine Bedrohung für die möglicherweise Betroffenen ist Diese Bedrohung sei, unabhängig davon, ob Maßnahmen tatsächlich gegen sie ergriffen werden, ein Eingriff in Art. 8 EMRK.[822]

---

818 Vgl. *Kühne*, StV 1998, 683. Dabei versteht der Gerichtshof den Ausdruck „Gesetz“ immer im „materiellen“ Sinn, nicht im „formellen“ und hat insbesondere ungeschriebenes Recht darin eingeschlossen, vgl. die Urteile *Kruslin* und *Huvig c. Frankreich*, EGMR ÖJZ 1990, 564 (565).

819 Vgl. EGMR ÖJZ 1999, 115 (116).

820 *Kühne*, StV 1998, 638 (684) unter Hinweis auf das Urteil *Halford c. Großbritannien* vom 25.06.1997, EGMR ÖJZ 1998, 311 (312). Diese Voraussetzung hat der EGMR nicht als gegeben angesehen. Die Schweizer Regierung hat zwar argumentiert, dass der Betroffene nicht in seiner Eigenschaft als Rechtsanwalt, sondern als Ehemann eines ehemaligen Mitglieds des Bundesrates abgehört worden war, doch besagt das Gesetz nach Ansicht des EGMR nicht eindeutig, wie, unter welchen Voraussetzungen und von wem die Unterscheidung zwischen solchen Angelegenheiten, die speziell mit der anwaltlichen Tätigkeit zusammenhängen und solchen, die mit anderen Tätigkeiten in Beziehung stehen, getroffen werden soll, vgl. EGMR ÖJZ 1999, 115 (117); *Kühne*, StV 1998, 683 (684).

821 In dem Verfahren *Weber u. Savaria c. Bundesrepublik Deutschland* rügten die Beschwerdeführer, die mit ihrer Verfassungsbeschwerde vor dem BVerfG gegen das G-10-Gesetz unterlegen waren (vgl. BVerfGE 100, 313 ff.) die Verletzung ihrer Rechte u.a. aus Art. 8 EMRK durch die Vorschriften des G-10-Gesetzes. Sie beanstandeten insbesondere das Verfahren der strategischen Überwachung, die Übermittlung und Verwendung personenbezogender Daten, die Vernichtung personenbezogender Daten sowie das Unterlassen der Mitteilung von den Beschränkungen des Fernmeldegeheimnisses, vgl. EGMR NJW 2007, 1433 (1434).

822 Vgl. EGMR NJW 2007, 1433 (14343). Hintergrund war, dass die Beschwerdeführerin als deutsche Staatsangehörige und Journalistin mit Wohnsitz in Uruguay vor allem in den Bereichen recherchierte, die Gegenstand der Überwachung des Bundesnachrichtendienstes sind und der Beschwerdeführer als uruguayischer Staatsbürger, der Informationen für die Beschwerdeführerin entgegennahm und weiterleitete.

Der EGMR hat die Anforderungen an Art. 8 EMRK einschränkende Gesetze erneut dargestellt.[823] Darüber hinaus hat er jedoch auch Aussagen über die Verarbeitung, Weitergabe und Vernichtung der erhobenen personenbezogenen Daten sowie über die Mitteilungspflicht an die Betroffenen getroffen.[824] Der Gerichtshof hat die Regelungen über die Datenverarbeitung im G-10-Gesetz als mit Art. 8 EMRK vereinbar angesehen, da die durch die Telefonüberwachung erlangten Daten entsprechend zu kennzeichnen sind, nur für die gesetzlich geregelten Zwecke verwendet und weitergegeben werden dürfen und dies zu protokollieren ist und damit Schutzvorkehrungen gegen den Missbrauch der erlangten Daten getroffen sind.[825] Gleiches gilt auch für die Regelungen über die Datenvernichtung und die Unterrichtung des Betroffenen.[826]

d) Fazit

Mit der EMRK ist eine staatliche Telekommunikationsüberwachung dann zu vereinbaren, wenn tatsächliche Anhaltspunkte für den Verdacht einer Straftat bestehen, die Personengruppe beschrieben wird, bei denen Telefongespräche abgehört werden dürfen, das verfolgte Ziel nicht mit anderen Maßnahme erreicht werden kann, ein besonderes Verfahren für die Überwachung vorgesehen und diese zeitliche begrenzt ist und die gesetzliche Grundlage so klar formuliert ist, dass für den Betroffenen erkennbar ist wie und unter welchen Voraussetzungen eine Überwachungsmaßnahme möglich ist.[827] Zudem müssen Regelungen zur Datenverarbeitung getroffen sein, die einen Mißbrauch der erhobenen Daten verhindern.[828]

III. Die Vereinbarkeit der Polizeigesetze mit den verfassungsrechtlichen Vorgaben und der EMRK

Die neu eingeführten Regelungen in den hier untersuchten Polizeigesetzen stehen dann in Einklang mit dem Grundgesetz, wenn sie formell und materiell verfassungsgemäß sind. Sie müssen hinreichend klar und bestimmt sein und zudem dem Verhältnismäßigkeitsgrundsatz

---

823 Vgl. EGMR NJW 2007, 1433 (1435 f.).

824 Vgl. EGMR NJW 2007, 1433 (1438 ff.).

825 Vgl. EGMR 2007, 1433 (1438). Angesichts der Gefahr, dass ein System der geheimen Überwachung zum Schutz der nationalen Sicherheit unter dem Vorwand die Demokratie zu verteidigen, den Schutz des Privatlebens zerstören kann, muss sich der Gerichtshof davon überzeugen, dass angemessene und wirksame Garantien gegen Missbrauch vorgesehen sind, vgl. EGMR NJW 2007, 1433 (1437).

826 Vgl. EGMR 2007, 1433 (1439 f.). Die Aussagen des EGMR zur Datenverarbeitung werden im Kapitel „Datenverarbeitung“ noch genauer herausgestellt.

827 Vgl. EGMR EuGRZ 1979, 278 (285 f.); ÖJZ 1999, 115 (116 f.); NJW 2007, 1433 (1435 f.)

828 Vgl. EGMR NJW 2007, 1433 (1437 ff.).

Rechnung tragen. Darüber hinaus dürfen sie nicht gegen die Vorgaben der EMRK verstoßen, da deren Regelungen als geltendes Bundesrecht den Bestimmungen der Landespolizeigesetze vorgehen.[829]

1. Formelle Verfassungsmäßigkeit

Die Regelungen der untersuchten Polizeigesetze entsprechen den formellen Anforderungen, welche an Art. 10 GG einschränkende Gesetze gestellt werden.[830] Alle fünf Landesgesetze sehen die Einschränkung des Art. 10 GG ausdrücklich vor.[831] Zwar verweisen Niedersachsen und Hessen lediglich auf die schon vor der Einführung der Telekommunikationsüberwachung vorgesehene Einschränkung des Art. 10 GG.[832] Allerdings bleibt dies für die hier untersuchten Regelungen zur präventiv-polizeilichen Telekommunikationsüberwachung ohne Konsequenzen.[833] Das BVerfG hatte bisher nicht geklärt, ob es in Fällen, in denen das ändernde Gesetz zu neuen Grundrechtseinschränkungen führt oder ermächtigt, den Anforderungen des Art. 19 Abs. 1, Satz 2 GG genügt, wenn das geänderte Gesetz bereits eine Zitiervorschrift im Sinne dieser Bestimmung enthält.[834] Aus Gründen der Rechtssicherheit führt diese Nichtbeachtung des Zitiergebots daher erst bei solchen grundrechtseinschränkenden Änderungsgesetzen zur Nichtigkeit, die nach dem Zeitpunkt der Verkündung des BVerfG-Urteils zum Nds.SOG 2005 beschlossen werden.[835]

2. Materielle Verfassungsmäßigkeit

Die Ermächtigungsnormen zur präventiven Telekommunikationsüberwachung müssen dem Adressaten nicht nur hinreichend klar und bestimmt zu erkennen geben, wie und unter welchen Voraussetzungen die Überwachungsmaßnahmen durchgeführt werden können, sondern

---

829 Eine Unterscheidung zwischen den Anforderungen des Grundgesetzes und denen der EMRK ist jedoch nicht geboten, da die EMRK als geltendes Bundesrecht ebenfalls mit den Vorgaben des Grundgesetzes als dem höherrangigen Recht vereinbar sein muss und es daher nicht zu unterschiedlichen Voraussetzungen kommen kann.

830 Zur Problematik der Gesetzgebungskompetenz vgl. das Kapitel „Der Zugriff auf die Telekommunikationsdaten“ unter IV. 1.

831 § 11 ThPAG; § 10 Nds.SOG; Art. 74 PAG; § 8 Nr. 3 POG; § 10 HSOG.

832 Vgl. LT-Drucks. Nds. 15/240, S. 15; LT-Drucks. Hessen 16/2352, S. 18.

833 So BVerfGE 113, 349 (365 ff.) für die §§ 33 a – 33 c Nds.SOG 2005.

834 Vgl. BVerfGE 113, 349 (367).

835 Vgl. BVerfGE 113, 349 (367).

die jeweiligen Regelungen müssen auch für den mit ihnen verfolgten Zweck geeignet, erforderlich und angemessen sein.[836]

Die Prüfung der materiellen Verfassungsmäßigkeit erfolgt anhand der einzelnen Tatbestandsvoraussetzungen Schutzgüter, Gefahrenlage, Überwachungssubjekt, Straftatenverhinderung, Verfahrensanforderungen, Richtervorbehalt und Befristung. Besonderes Augenmerk wird dabei auf die Verhältnismäßigkeit im engeren Sinn (Angemessenheit, Zumutbarkeit oder Proportionalität)[837] gerichtet, sowie auf die Bestimmtheit und Klarheit der Regelungen.[838]

a) Schutzgüter und Gefahrenlage

Gemeinsam ist den hier untersuchten Regelungen, dass sie eine präventive Telekommunikationsüberwachung zur klassischen Gefahrenabwehr vorsehen. Die Länder Thüringen, Niedersachsen und Bayern sehen die Kommunikationsüberwachung auch zur Verhinderungsvorsorge und gegen Nachrichtenmittler vor. Niedersachsen zusätzlich auch zur Verfolgungsvorsorge.

Die Telekommunikationsüberwachung greift in das Fernmeldegeheimnis sowie in das Recht auf informationelle Selbstbestimmung ein und verletzt nicht nur die Privatsphäre des potenziellen Störers, sondern auch seiner Kommunikationspartner und derer, die dem Verdacht ausgesetzt sind, dass sie Nachrichten entgegennehmen oder weiterleiten bzw. ihren Kommunikationsanschluss dem eigentlich Verdächtigen zur Verfügung stellen. Die Überwachung der Telekommunikation betrifft damit neben dem eigentlichen Störer einen großen Kreis nichtverdächtiger Personen, deren Anzahl sich beim Einsatz des IMSI-Catchers noch um eine Vielzahl erhöht.[839] Durch die Auskunftserteilung erlangen die Polizeibehörden Kenntnis über Daten, die geeignet sind das Privatleben nicht nur der betroffenen Person zu durchleuchten.

---

836 Vgl. *Jarass*, in: Jarass/Pieroth, Art. 10 GG, 17 f.; *Hermes*, in: Dreier (Hrsg.), Art. 10 GG, Rn. 63 ff.;

837 Vgl. *Pieroth/Schlink*, 2007, Rn. 289 ff.; *Manssen*, 2005, Rn. 190; *Ipsen*, 2007, Rn. 180 ff.

838 Auf die Geeignetheit und Erforderlichkeit der Regelungen wird nicht weiter eingegangen. Geeignet ist ein Eingriff/Mittel dann, wenn es den angestrebten Zweck fördert. Es kommt nicht darauf an, ob es sich um eine oder die optimale Maßnahme handelt. Es genügt, wenn die Maßnahme überhaupt etwas zur Zweckerreichung beiträgt, vgl. BVerfGE 30, 292 (316); E 33, 171 (187); *Manssen*, 2005, Rn. 185; *Ipsen*, 2007, Rn. 176. Dies ist hier gegeben. Die Erforderlichkeit ist dann gewahrt, wenn von mehreren zur Verfügung stehenden Mitteln dasjenige gewählt wurde, das die grundrechtlichen Schutzgüter am wenigsten beeinträchtigt, vgl. *Ipsen*, 2007, Rn. 178; *Manssen*, 2005, Rn. 187 ff. Dem Erforderlichkeitserfordernis ist daher mit den Subsidiaritätsklauseln in den präventiv-polizeilichen Regelungen genüge getan.

839 Vgl. das Kapitel „Der Zugriff auf die Telekommunikationsdaten“ unter V.

Nutzen mehrere Personen denselben Anschluss, so ist der Polizei für jeden einzelnen bekannt, wer mit wem wann wie lange über was gesprochen hat und wo sich die Kommunikationspartner dabei aufgehalten haben.[840]

Werden die Grundrechte der Betroffenen zur Gefahrenabwehr eingeschränkt, müssen sowohl die zu schützenden Rechtsgüter als auch die Wahrscheinlichkeit des Schadenseintritts die Beschränkung rechtfertigen.

Da die präventive Telekommunikationsüberwachung empfindlich in die Grundrechte einer Vielzahl von Personen – insbesondere auch von Nichtstörer – eingreift, ist eine solche Maßnahme nur zum Schutz überragender Rechtsgüter zulässig.[841] Die präventive Telekommunikationsüberwachung als polizeiliche Datenerhebung ist keine Maßnahme, die unmittelbar eine Gefahr abwehrt oder Störung beseitigt, sondern die eigentliche Gefahrenabwehrmaßnahme erst ermöglicht.[842] Sie steht daher im engen Verhältnis zur Gefahrenvorsorge.[843] Im Bereich der Vorsorge wird für die Telekommunikationsüberwachung bei nicht näherer Eingrenzung der zu Grunde gelegten Tatsachen, ein allgemein und im konkreten Fall überragend wichtig zu schützender Allgemeinwohlbelang gefordert.[844]

Die präventive Telekommunikationsüberwachung sollte deswegen nur zum Schutz des Lebens, der Gesundheit und der Freiheit von Personen vorgesehen werden.[845] Eine Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes ist nach der hier vertretenen Meinung nicht ausreichend. Zwar sind die Einrichtungen des Staates in ihrer rechtmäßigen Funktion ebenfalls hohe Schutzgüter. Vor dem Hintergrund des empfindlichen Eingriffs in das Telekommunikationsgeheimnis, müssen sie aber zurücktreten. Einrichtungen des Staates sind z.B. die Volksvertretungen, staatliche Behörden, Selbstverwaltungskörperschaften oder

---

840 Vgl. das Kapitel „Der Zugriff auf die Telekommunikationsdaten“ unter II.

841 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 625 c.

842 Vgl. dazu das Kapitel „Länderübergreifende Sachverhalte“ unter III.

843 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 538; *Riegel*, RDV 1990, 232 ff.

844 Vgl. *Puschke/Singelnstein*, NJW 2005, 3534 (3537) unter Hinweis auf die Entscheidung des BVerfG zum Nds.SOG 2005. Das BVerfG hat sich zwar in dieser Entscheidung hauptsächlich mit der Vorsorge für de Straftatenverhütung und –verfolgung auseinander gesetzt, jedoch ist es auch auf das Vorfeld der Gefahrenabwehr eingegangen und hat hierfür Abwägungsgrundsätze entwickelt, vgl. BVerfG NJW, 2005, 2603 (2607, 2610).

845 Dies sehen auch die Regelungen in Niedersachsen, Rheinland-Pfalz und Hessen vor.

öffentliche Anstalten.[846] Eine Gefahr für Einrichtungen vermag es jedoch nicht, den Geheimnisschutz aus Art. 10 GG zurücktreten zu lassen. Die Vertraulichkeit individueller Kommunikation ist ein hohes Schutzgut. Das Fernmeldegeheimnis gewährleistet die freie Entfaltung der Persönlichkeit durch den vor der Öffentlichkeit verborgenen Austausch von Kommunikation und schützt damit zugleich die Würde des Menschen.[847] Dies bedingt nach der hier vertretenen Auffassung Beschränkungen nur aufgrund weniger hochrangiger Rechtsgüter wie Leib, Leben und Freiheit von Personen zuzulassen.[848]

Der Staat ist Angriffen auf seinen Bestand oder seine Einrichtungen dennoch nicht hilflos ausgesetzt. Denn sind Anschläge auf diese geplant, so sind dabei regelmäßig auch Menschenleben gefährdet. Dann ist ohnehin die präventive Telekommunikationsüberwachung ein zulässiges und adäquates Mittel zur Gefahrenabwehr.[849] Im Vordergrund steht aber immer der Schutz der Bürger, wie es der im Grundgesetz verankerte Schutzauftrag des Staates gebietet.[850]

Eine Telekommunikationsüberwachung zum Schutz von Sachwerten, selbst wenn diese von erheblichem Wert sind, ist abzulehnen. Die Rechtsprechung des BVerfG zum „Großen Lauschangriff“[851] lässt sich insofern nicht auf die präventive Telekommunikationsüberwachung übertragen.[852] Das BVerfG gibt im Rahmen seiner Ausführungen zur Weitergabe von Daten aus einer repressiven Wohnraumüberwachung an Polizeibehörden zu präventiven Zwecken zu verstehen, dass es eine präventive Wohnraumüberwachung als zulässig erachtet, wenn eine gemeine Gefahr für erhebliche Sach- und Vermögenswerte besteht.[853] Mag ein Eingriff in Art. 13 GG im Vergleich zu Art. 10 GG im Grundsatz höher zu bewerten sein, da

---

846 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 403; OVG Münster NJW 1997, 1596; *Drews/Wacke/Vogel/Martens*, 1986, S. 234.

847 Vgl. BVerfGE 113, 349 (391); E 110, 33 (53); E 67, 157 (171); siehe auch *Würtenberger/Heckmann*, 2005, Rn. 625 d. Zum Schutz des Kernbereichs vgl. die Ausführungen in Kapitel 6 unter I. 4.

848 Vgl. zum hohen Stellenwert der Rechtsgüter Leben, Leib und Freiheit gemäß Art. 2 Abs. 1, Satz 1 GG diese Kapitel unter III.2.c) cc) (3).

849 Gleiches gilt nach der hier vertretenen Auffassung auch für Gefährdungen der freiheitlich demokratischen Grundordnung (zur Begriffsbestimmung vgl. § 4 Abs. 2 BVerfSchG und die Kommentierung von *Jarass*, in: Jarass/Pieroth, Art. 21 GG, Rn. 33). Wird mit Gewalt gegen die Grundsätze der demokratischen Ordnung wie freie Wahlen, Bindung der Staatsgewalten an Gesetz und Recht oder die im Grundgesetz konkretisierten Menschenrechte vorgegangen, so sind davon auch regelmäßig Menschenleben derart betroffen, dass eine Telefonüberwachung möglich wäre.

850 Art. 2 Abs. 2 GG.

851 Vgl. BVerfGE 109, 279 ff..

852 Zur Übertragbarkeit der in diesem Urteil aufgestellten Grundsätze zur Datenverarbeitung auf die präventive Telekommunikationsüberwachung vgl. das Kapitel „Datenverarbeitung“.

853 Vgl. BVerfGE 109, 279 (378 f.).

in die letzte Rückzugsmöglichkeit des Betroffenen eingegriffen wird, während sich der betroffene Bürger bei der fernmeldetechnischen Kommunikation Dritter zur Übermittlung bedient, so steht nach der hier vertretenen Auffassung nicht zwingend entgegen, dass Umstände gegeben sein können, die einen Eingriff in Art. 10 GG nur unter höheren Voraussetzungen zulassen als in Art. 13 GG.

Denn bei der Auskunftseinholung und Überwachung der Kommunikation fallen eine Fülle von Daten an, welche die Lebensgewohnheiten und –umstände einer Vielzahl von Personen offen zu legen vermögen. Während die Wohraumüberwachung schon begrifflich eine stationäre Überwachung ist, ist die Telekommunikationsüberwachung nicht ortsgebunden. Die Kommunikationsüberwachung kann zu jeder Zeit und an jedem Ort stattfinden und jede beliebige Person betreffen. Die Wohnung des Überwachten werden kaum Fremde oder flüchtige Bekannte betreten, während Kommunikation nicht von jeweiligen Freundschaftsgrad abhängt. Insbesondere beim Einsatz des IMSI-Catchers besteht bei den davon betroffenen Personen keinerlei Beziehung zum Überwachungssubjekt. Diese Eingriffsweite bedingt es, die Grundrechtsverletzung auf hochrangige Rechtsgüter zu beschränken, wobei Sachgefahren auszuklammern sind. Zwar können Sachen, wie beispielsweise die Infrastruktur oder Versorgungseinrichtungen ebenfalls gewichtige Schutzgüter sein. Doch auch bei drohenden Beeinträchtigungen in diesen Fällen dürften wie bei den Einrichtungen des Staates stets auch Menschenleben gefährdet sein. Sei es als Transportgäste, wie es die Anschläge in Madrid und London auf öffentliche Verkehrsmittel gezeigt haben oder weil die Versorgung der Bürger, z.B. bei Angriffen auf die Wasser- oder Stromversorgung, nicht mehr gewährleistet ist.

Auch an die Gefahrenlage, die Wahrscheinlichkeit des Schadenseintritts, sind angesichts der erheblichen Grundrechtseingriffe strenge Anforderungen zu stellen. Erforderlich ist eine gegenwärtige Gefahrenlage[854], um einer Eingriffsausuferung entgegenzuwirken.[855] Eine Telekommunikationsüberwachung schon bei einem einfachen Gefahrenverdacht zuzulassen, trägt der Vielzahl der davon betroffenen Grundrechtsträger nicht Rechnung. Die (Landes-) Polizei-

---

854 Die gegenwärtige und die unmittelbar bevorstehende Gefahr zeichnen sich durch große zeitliche Nähe und eine an Sicherheit grenzende Wahrscheinlichkeit der schädigenden Einwirkung aus, vgl. *Denninger*, in: Lisken/Denninger (Hrsg.), Kapitel E, Rn. 53 und 59 mit Verweis auf die Landespolizeigesetze. Siehe auch *Würtenberger/Heckmann*, 2005, Rn. 415; *Unger/Siefken*, in: Böhrenz/Unger/Siefken, § 2 Nds.SOG, Anm. 5.

855 Nach *Würtenberger/Heckmann*, 2005, Rn. 625 c wäre eine präventive Telekommunikationsüberwachung in Baden-Württemberg zur Abwehr zeitlich unmittelbar bevorstehender Gefahren zulässig.

gesetze verlangen für die Wohnraumüberwachung zumeist eine unmittelbare oder gegenwärtige Gefahrenlage.[856] Da die Schwere der untersuchten Grundrechtseingriffe in Art. 10 GG keinesfalls hinter Art. 13 GG zurücktritt, sind auch hier hohe Voraussetzungen für die Gefahrenlage erforderlich.

Soweit das PAG als Voraussetzung für eine präventive Telekommunikationsüberwachung eine dringende Gefahr[857] für Leben, Gesundheit oder Freiheit einer Person vorsieht, hält es sich (noch) im Rahmen der grundgesetzlichen Vorgaben.[858] Darüber hinaus lässt es jedoch eine Sachgefahr genügen,[859] sofern für diese eine „gemeine Gefahr" im Sinne einer Gefahr für erhebliche Sachwerte[860] besteht. Dies ist ebenso wie die Überwachungen der Telekommunikation zur Gefahrenabwehr für den Bestand der Bundes oder der Länder nicht mit dem Grundgesetz zu vereinbaren.[861]

b) Überwachungssubjekt

Das grundgesetzliche Bestimmtheitsgebot soll sicherstellen, dass der betroffene Bürger sich auf mögliche belastende Maßnahmen einstellen kann, die gesetzesausführende Verwaltung für ihr Verhalten steuernde und begrenzende Handlungsmaßstäbe vorfindet und die Gerichte

---

856 § 35 Abs. 1 ThPAG; § 35 a Abs. 1 Nds.SOG; § 15 Abs. 4 HSOG.

857 Eine dringende Gefahr wird nach LT-Drucks. Bayern 15/4097, S. 3 und 4 als Gefahr verstanden, die mit hinreichender Wahrscheinlichkeit für wichtige Rechtsgüter droht. Vgl. zur „dringenden Gefahr" iSd Art. 13 GG BVerwG 47, 31 (40); *Jarass*, in: Jarass/Pieroth, Art. 13 GG, Rn. 30 und 37. Zur Auslegung des Begriffs im Polizeirecht vgl. *Denninger*, in Lisken/Denninger (Hrsg.), Kapitel E, Rn. 63 und *Rachor*, in: Lisken/Denninger (Hrsg.), Kapitel F, Rn. 710 ff.

858 Zwar kommt mit dem Begriff der „dringenden" Gefahr regelmäßig nicht die zeitliche unmittelbare Nähe zum Ausdruck, doch muss für die zu befürchtende schwere Grundrechtsverletzung eine hinreichende Wahrscheinlichkeit bestehen, vgl. *Jarass*, in: Jarass/Pieroth, Art. 13 GG, Rn. 37.

859 Die Sachgefahr war ursprünglich auch in den Gesetzesentwürfen Niedersachsens und Rheinland-Pfalz enthalten, ist aber dann nicht in die jeweiligen Regelungen mit aufgenommen worden; vgl. LT-Drucks. Nds. 15/240, S. 4 und LT-Drucks. 14/2287, S. 15.

860 Vgl. *Honnacker/Beinhofer*, Art. 2 PAG, Rn. 21.

861 Dem hohen Schutzgut des Fernmeldegeheimnisses tragen die Gesetzgeber Niedersachsens, Rheinland-Pfalz und Hessens dadurch Rechnung, dass sie an die Gefahrenlage hohe Anforderungen stellen, in dem sie eine gegenwärtige Gefahr fordern und auch nur einige wenige Schutzgüter, nämlich Leib, Leben und Freiheit einer Person, als Rechtfertigungsgründe für eine Einschränkung des Fernmeldegeheimnisses gelten lassen. Das POG lässt sogar nur eine Gefahrenlage für Leib und Leben einer Person zu. In Thüringen erfordert die Überwachung und Auskunft über die Telekommunikation lediglich eine einfache konkrete Gefahrenlage, die besteht, wenn nach allgemeiner Lebenserfahrung zu erwarten ist, dass sich ein Zustand zu einem schädigenden Ereignis verdichten wird, vgl. *Ebert/Honnacker/Seel*, § 2 ThPAG, Rn. 12. Auch lässt sie neben einer Gefahr für Leben, Gesundheit oder Freiheit einer Person die Telekommunikationsüberwachung auch zur Gefahrenabwehr für den Bestand und die Sicherheit des Bundes oder der Länder zu. Die Voraussetzungen des ThPAG genügen daher sowohl hinsichtlich den Anforderungen an die Gefahrenlage als auch an die zu schützenden Rechtsgüter nicht den Anforderungen des Grundgesetzes.

die Rechtskontrolle durchführen können.[862] Das Parlamentsgesetz muss daher die Voraussetzungen und den Umfang der Beschränkungen klar und erkennbar festlegen.[863]

Dies gilt nicht nur für die Anforderungen an die Voraussetzungen, bei denen eine Telekommunikationsüberwachung angeordnet werden kann, sondern auch für die Frage, welche Personen der Überwachung unterliegen, wer also Betroffener der Maßnahme ist. So ist nicht nur festzulegen, ob die Überwachung nur gegen den Störer oder auch Dritte zulässig ist, sondern die betroffenen Personen sind so klar zu bestimmen, dass für den Bürger zu erkennen ist, wer von einer Überwachungsmaßnahme betroffen sein kann.[864]

Nach Art. 34 a Abs. 1 PAG kann die Polizei Daten erheben über den für eine Gefahr Verantwortlichen, über die Person, die Straftaten begehen will, sowie über die Person, die für den potenzielle Störer oder Täter Nachrichten entgegennimmt oder weitergibt, als auch über die Person dessen Kommunikationseinrichtung der potenzielle Störer oder Täter benutzt.[865] Aus der Gesetzesbegründung ergibt sich, dass andere als in Art. 34 a Abs. 1 PAG genannte Personen keine Adressaten sein können und nur von den Maßnahmen betroffen werden dürfen, wenn dies unvermeidbar ist, weil sie Kommunikationspartner des Adressaten sind.[866] Die Regelungen gelten auch für den Einsatz des IMSI-Catchers.

Gegen einen Gefährdeten als Nichtstörer ist die Kommunikationsüberwachung und der IMSI-Catcher-Einsatz nur möglich, wenn eine Gefahr für Leben oder Gesundheit dieser Person besteht.[867]

In Bayern ist damit eindeutig geregelt, wer Adressat der präventiven Telekommunikationsüberwachung sein kann und welche Anschlüsse überwacht werden dürfen. Die übrigen hier

---

862 Vgl. BVerfGE 113, 349 (375 f.).

863 Vgl. BVerfGE 100, 313 (360); E 110, 33 (53 f.); E 113, 349 (375 f.).

864 Vgl. dazu BVerGE 113, 349 (380), welches den verwendeten Begriff der Kontakt- Begleitperson als zu unklar ansieht, um eine Aussage darüber zu treffen, wer mit dem potenziellen Täter so in Verbindung steht, dass Hinweise über die angenommenen Straftaten gewonnen werden können. Siehe dazu auch EGMR ÖJZ 1998, 311 (312) sowie die Ausführungen von *Kühne*, StV 1998, 638 (684).

865 Die Inanspruchnahme von Personen, deren Anschlüsse der potenzielle Störer ohne deren Kenntnis benutzt, ist in Bayern – folgt man dem Gesetzeswortlaut – möglich Die Gesetzesbegründung ist dagegen nicht eindeutig, da sie von „zur Verfügung stellen“ spricht, vgl. LT-Drucks. Bayern 15/2096, S. 52, 53.

866 Vgl. LT-Drucks. Bayern 15/2096, S. 53. Möglich wäre ansonsten aufgrund des Wortlauts auch die Überwachung eines Anschlusses, der vom Nachrichtenmittler zwar genutzt, aber nicht sein eigener ist gewesen, denn Art. 34 c Abs. 3, Satz 2 PAG verlangt als Anordnungsangaben die Rufnummer oder Kennung eines Telekommunikationsanschlusses oder eines Endgerätes.

867 Art. 34 a Abs. 3, Satz 1 PAG.

untersuchten Polizeigesetze enthalten sehr unterschiedliche Vorgaben für die Frage, gegen wen und für welche Anschlüsse eine präventive Telekommunikationsüberwachung angeordnet werden kann.[868] Kritisch zu betrachten sind dabei die Regelungen in Niedersachsen und Thüringen.

In Niedersachsen galt, dass gemäß § 33 a Abs. 2 Satz 2 Nds.SOG 2005 die Datenerhebung nur an Telekommunikationsanschlüssen der in § 33 a Abs. 1 Nds.SOG 2005 genannten Personen erfolgen darf, so auch bei den Kontakt- und Begleitpersonen.[869] Dies sind gemäß § 2 Nr. 11 Nds.SOG 2005 Personen, die mit dem potenziellen Störer in einer Weise in Verbindung stehen, die erwarten lässt, dass durch sie Hinweise auf die angenommene Straftat gewonnen werden können.

Dieser Begriff der Kontakt- und Begleitperson entspricht nicht den rechtsstaatlichen Bestimmtheitsanforderungen.[870] Es ist nicht klar, wer mit dem potenziellen Straftäter so in Verbindung steht, dass Hinweise über die angenommenen Straftaten gewonnen werden können.[871] Der niedersächsische Gesetzgeber hat keine konkretisierenden Einschränkung vorgenommen, da ausweislich der Gesetzesbegründung eine Datenerhebung schon in Betracht kommt, wenn diese „von Relevanz für den Kontakt und demnach für die Verhinderung der betreffenden Straftaten sind“[872]. Auch ist nicht normiert, welcher Art die Hinweise sein müssen, die durch Kontakt- und Begleitpersonen über die Straftat gewonnen werden sollen.[873]

---

868 In Rheinland-Pfalz gestattet § 31 Abs. 1 POG die Datenerhebung über Störer und Nichtstörer. Aus § 31 Abs. 2, Satz 2 POG ergibt sich, dass eine Telekommunikationsüberwachung hinsichtlich der Telekommunikationsanschlüsse zulässig ist, die vom Störer oder Nichtstörer mit hoher Wahrscheinlichkeit genutzt werden. Es müssen also nicht deren eigene sein. Auch der Einsatz des IMSI-Catchers ist zur Feststellung der Polizei nicht bekannter Anschlüsse gegen den Störer und Nichtstörer zulässig. Nach § 15 a Abs. 4, Satz 3 HSOG muss die richterliche Anordnung die Rufnummer oder eine andere Kennung des Telefonanschlusses oder des Telekommunikationsgeräts der Person enthalten, gegen die sich die Anordnung richtet. Dies sind mangels anderweitiger Regelungen der Störer und der Nichtstörer. Überwacht werden können also nur deren eigene Anschlüsse. Gegen den Störer und der Nichtstörer ist auch der Einsatz des IMSI-Catchers zulässig.

869 § 33 a Abs. 1 Nr. 3 Nds.SOG.

870 Vgl. BVerfGE 113, 349 (380). Vgl. jetzt aber die Änderungen in § 2 Nr. 12 Nds.SOG, die infolge des genannten BVerfG-Urteils eingefügt wurden. Siehe dazu auch die Gesetzesbegründung, LT-Drucks. Nds. 15/3810, S. 19.

871 Vgl. BVerfGE 113, 349 (380 f.). Die Überwachung des Anschlusses der Kontakt- und Begleitperson dürfte beispielsweise auch möglich sein, wenn dieser vom Täter genutzt wird, da auch dann die Möglichkeit besteht, Hinweise über die angenommene Straftat zu gewinnen. Gleiches muss für eine „Gutgläubigkeit“ der Kontakt- und Begleitperson gelten. Eine ausdrückliche Regelungen ist aber nicht getroffen.

872 LT-Drucks. Nds. 15/240, S. 18.

873 Vgl. BVerfGE 113, 349 (389).

Es sind Einschränkungen erforderlich, die genau definieren, welcher Art und von welcher Intensität die Beziehung zwischen Kontakt- und Begleitperson und dem potenziellen Straftäter sein muss, um einen Eingriff in deren Grundrechte zu rechtfertigen.[874] Die Regelung im Nds.SOG 2005 verstößt so mangels Bestimmtheit gegen Art. 10 GG und Art. 8 EMRK.

Auch in Thüringen ist die Überwachung der Kontakt- und Begleitpersonen vorgesehen.[875] Sind im Sinne des § 34 a Abs. 1 Nr. 3 ThPAG Kontakt- und Begleitpersonen „Personen, die in einem strafrechtsrelevanten Kontakt zum Störer stehen und als so genannte Nachrichtenmittler auftreten, die Informationen für den Störer entgegennehmen oder weiterleiten“[876], so wird damit die Verbindung zwischen dem potenziellen Straftäter und der Kontakt- und Begleitperson zwar exakter beschreiben als im Nds.SOG 2005, jedoch ist damit nicht ausdrücklich geregelt, ob auch Anschlüsse von Personen überwacht werden dürfen, die kein „aktives Tun“ entfalten, sondern dem potenziellen Störer ihren Anschluss lediglich überlassen oder von diesem ohne Kenntnis der betroffenen Personen genutzt werden. Offen bleibt auch, ob eine Überwachung der Kontakt- und Begleitperson möglich ist, die nicht ihren eigenen Anschluss benutzt. Auch die Regelung des ThPAG verstößt daher mangels Bestimmtheit gegen Art. 10 GG und Art. 8 EMRK. Hinzu tritt jedoch noch ein weiterer Aspekt:

§ 34 a ThPAG sieht keine Überwachung des Nichtstörers vor. Teilnehmer am Kommunikationsverkehr benutzen und besitzen jedoch nicht mehr nur einen Anschluss, sondern mehrere im steten Wechsel und dabei nicht nur ihre eigenen. Diesen auffälligen Wandel im Kommunikationsverhalten hat die Studie des Max-Planck-Institutes aus dem Jahr 2003 über Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a; 100 b StPO und anderer Ermittlungsmaßnahmen festgestellt.[877] Häufig ist unklar, wie das Verhältnis zwischen Anschlussinhaber und Anschlussnutzer zu qualifizieren ist.[878] Dabei spielen insbesondere so genannte Handygeber, also Personen eine Rolle, die Beschuldigten ihre (Mobilfunk-)Anschlüsse zur Verfügung stellen.[879] Dieses Auseinanderfallen von Anschluss-

---

874 Die insofern präzisere Regelung des § 34 a Abs. 1 Nr. 3, § 34 Abs. 3 Nr. 3 ThPAG dürfte den Anforderungen des BVerfG genügen, da die Verbindung zwischen dem potenziellen Straftäter und der Kontakt- und Begleitperson exakter beschrieben ist.

875 § 34 a Abs. 1 Nr. 3 ThPAG.

876 Vgl. LT-Drucks. Th. 3/2128, S. 35.

877 Diese Studie wurde im Auftrag des Bundesministeriums der Justiz erstellt und der Abschlussbericht im Jahr 2003 durch *Albrecht, Hans-Jörg, Dorsch, Claudia und Krüpe, Christiane* vorgelegt.

878 *Albrecht/Dorsch/Krüpe*, 2003, S.270.

879 *Albrecht/Dorsch/Krüpe*, 2003, S.269 und 274.

inhaber und Anschlussnutzer bei Mobiltelefonen, das Auftreten von Strohmännern oder Handygebern, sowie das häufige Anschluss- und Kartenwechseln durch die Täter führt zu einer Verkomplizierung der Anordnungssituation.[880]

Muss die präventive Telekommunikationsüberwachung an sich verhältnismäßig sein, so ist dabei nicht nur an die Verhältnismäßigkeit im engeren Sinn, also die Angemessenheit der Maßnahmen gedacht. Die Überwachungsmaßnahme muss zur Erreichung des verfolgten Zwecks vielmehr auch geeignet und erforderlich sein.[881] Ist die Telekommunikationsüberwachung als ein wichtiges und unabdingbares Ermittlungsinstrument einzuschätzen[882], so kann sie ihren Zweck nur erfüllen, wenn nicht lediglich die Überwachung des „Verdächtigenanschlusses“ oder der Anschlüsse ihm geneigter Personen in Betracht kommt, sondern auch unter engen Voraussetzungen der des Nichtstörers.

c) Straftatenverhinderung

Die Polizeigesetze, die eine präventive Telekommunikationsüberwachung auch zur Straftatenverhinderung vorsehen, haben unterschiedliche Anforderungen festgeschrieben, unter denen die Maßnahmen zulässig sind. Bayern und Niedersachsen[883] verweisen auf ihren eigenen Straftatenkatalog im jeweiligen Polizeigesetz, während Thüringen den Straftatenkatalog der StPO übernommen hat. Bei der Telekommunikationsüberwachung zur Straftatenverhütung[884] sind mehrere verfassungsrechtliche Problemfelder zu unterscheiden.

---

880 Vgl. *Albrecht/Dorsch/Krüpe*, 2003, S. 461, die dazu ausführen, dass viele Teilnehmer der Studie auf die niederländische Regelung der IMEI-Überwachung als Lösung verwiesen haben, die nicht die Telefonnummer, sondern die Gerätenummer zur Überwachung freigibt und ein Wechsel der SIM-Karte das Abhören damit nicht beeinträchtigt und dass andere Praktiker sich eine Überwachung, die sich auf die Person des Beschuldigten unabhängig von den durch diesen genutzten Anschluss konzentriert (im Sinn einer Anordnung, die die Überwachung des Beschuldigten und aller ihm zur Verfügung stehenden Kommunikationsmittel gestattet, ohne dass diese stets aufs Neue in weiteren Anordnungen zur Überwachung freigegeben werden müssten) wünschen würden. Dies sieht die Regelung im POG vor.

881 Vgl. dazu die Ausführungen in diesem Kapitel unter II. 1. c) ee).

882 Jedenfalls für den repressiven Bereich, vgl. *Albrecht/Dorsch/Krüpe*, 2003, S. 463.

883 Durch das Gesetz zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung, GVBl. S. 654, ist die präventive Telekommunikationsüberwachung zur Straftatenverhinderung weggefallen.

884 Thüringen und Bayern sehen die Telekommunikationsüberwachung zur Verhinderungsvorsorge vor, während Niedersachsen diese auch für die Verfolgungsvorsorge vorgesehen hat. Für die Verfolgungsvorsorge hat das BVerfG mit Urteil vom 27.07.2005 (BVerfGE 113, 348 ff.) eine Gesetzgebungskompetenz der Länder verneint.

aa) Notwendigkeit

Betrachtet man die Regelung in § 31 a POG, ist zu überlegen, ob eine Überwachung zur Straftatenverhütung überhaupt angezeigt ist, oder ob nicht vielmehr durch die Gefahrenabwehr für Leib, Leben und Freiheit auch einer vorbeugenden Verbrechensbekämpfung genüge getan ist. Wie die Entscheidung des Landgerichts Kaiserslautern vom 13.08.2004 zeigt, ging das Gericht davon aus, dass ein möglicher Banküberfall, der die §§ 249 ff oder 255 ff StGB zu verwirklichen geeignet ist, geplant war und hat eine Telekommunikationsüberwachung im Hinblick auf die damit verbundenen Gefahren für Leib und Leben als zulässig angesehen.[885]

Doch sind mit einer Lebens- oder Gesundheitsgefahr nicht zwingend alle Delikte umfasst, denen durch eine Telekommunikationsüberwachung begegnet werden soll. So dürften beim organisierten Handel mit Waffen und Drogen nicht ohne weiteres schon konkrete oder gar gegenwärtige Gefahren für Leib und Leben vorliegen, da der Erwerber diese erst einsetzen bzw. konsumieren muss. Die dadurch bedingten Abwägungen und Einschätzungen würden zu Rechtsunsicherheit führen, auch wäre ein hohes Maß an Vorhersehbarkeit eingebüßt. Will der Gesetzgeber die Telekommunikationsüberwachung auch zur vorbeugenden Verbrechensbekämpfung einsetzen, so muss er eine Entscheidung darüber treffen, welche Straftaten so gewichtig sind, dass ihre möglicherweise bevorstehende Verwirklichung einen Eingriff in Art. 10 GG rechtfertigt.

bb) Begehungsverdacht

Die verfassungskonforme Ausgestaltung von Befugnisnormen, die Überwachungsmaßnahmen zu Zwecken der vorbeugenden Bekämpfung von Straftaten gestatten, begegnet einigen Schwierigkeiten. Aufgrund der notwendigen zeitlichen Vorverlagerung des polizeilichen Einschreitens[886] bestehen in einer Vorfeldsituation typischerweise Prognoseschwierigkeiten für den Rechtsanwender.[887] Daraus ergibt sich ein Risiko für Fehlprognosen mit der Folge von Eingriffen in Art. 10 GG bei unbeteiligten Dritten, welches verfassungsrechtlich nur hinnehmbar ist, wenn die betreffenden Befugnisnormen handlungsbegrenzende Tatbestandsele-

---

885 Vgl. LG Kaiserslautern NJW 2005, 443.

886 § 26 Abs. 1 Nr. 2 – 6 PolG BW fordern bspw. nicht durchgängig das Vorliegen einer konkreten Gefahr und bedingen dadurch eine Vorverlagerung der Eingriffsschwelle, vgl. *Würtenberger/Heckmann*, 2005, Rn. 325.

887 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 625 c.

mente enthalten, die einen ausreichenden Standard an Vorhersehbarkeit und Kontrollierbarkeit schaffen.[888]

Um den verfassungsrechtlichen Anforderungen gerecht zu werden, genügt es nicht, Tatsachen zu verlangen, die darauf schließen lassen, dass bestimmte Straftaten begangen werden sollen.[889] Erforderlich ist die Festschreibung weiterer Indikatoren, die den Grad der Wahrscheinlichkeit der Tatbegehung und deren zeitliche Verwirklichung präzisieren.[890]

Nach *Würtenberger/Heckmann*[891] muss zumindest eine konkrete Planung einer Straftat oder Vorbereitungshandlung zu beobachten sein, bevor eine Telekommunikationsüberwachung in Betracht kommt.

Das PAG stellt auf konkrete Vorbereitungshandlungen ab, die für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass Straftaten begangen werden sollen.[892] Konkrete Vorbereitungshandlung soll jede die schwerwiegende Straftat objektiv fördernde Tätigkeit sein, insbesondere konkrete Planungstätigkeiten.[893] Diese Anforderungen genügen daher den verfassungsrechtlichen Vorgaben.

Das Nds.SOG 2005 und das ThPAG beziehen sich dagegen schlicht auf „Tatsachen, die die Annahme rechtfertigen, dass Straftaten begangen werden sollen“[894] und halten insofern den verfassungsrechtlichen Bestimmtheitsanforderungen, die das BVerfG in seinem Urteil zum Nds.SOG 2005 gestellt hat, nicht stand.[895]

---

888 Vgl. BVerfGE 113, 349 (377 f.).

889 So aber die Regelungen in § 33 a Abs. 1 Nr. 2 Nds.SOG 2005 und § 34 Abs. 1 Nr. ThPAG. Nach BVerfGE 113, 349 (378) ist der Begriff der “Tatsache” für sich betrachtet hinreichend bestimmt, da er eine Abgrenzung zur bloßen Vermutung und allgemeinen Erfahrungsgrundsätzen vornimmt. Den Bestimmtheitsanforderungen genügt der Tatsachenbegriff aber dann nicht, wenn auf eine künftige Straftatenbegehung Bezug genommen wird.

890 Vgl. BVerfGE 113, 349 (378 ff.), welches die Regelungen der § 33 Abs. 1 Nr. 2 und 3 Nds.SOG 2005 als unvereinbar mit dem Grundgesetz erklärt hat. Siehe dazu *Rachor*, in: Lisken/Denninger (Hrsg.), Kapitel F, Rn. 179 ff.; *Pieroth/Schlink/Kniesel*, 2007, § 14 Rn. 135; *Jarass*, in: Jarass/Pieroth, Art. 10 GG, Rn. 17.

891 *Würtenberger/Heckmann*, 2005, Rn. 625 c.

892 Art. 34 a Abs. 1 Nr. 2 PAG.

893 Vgl. LT-Drucks. 15/4097, S. 4.

894 § 34 a Abs. 1 Nr. 1 ThPAG und § 33 a Abs. 1 Nr. 2 Nds.SOG 2005.

895 Vgl. Fn. 889.

cc) Delikte

Welche Delikte geeignet sind unter präventiven Gesichtspunkten das Fernmeldegeheimnis einzuschränken, ist von der verfassungsgerichtlichen Rechtsprechung noch nicht entschieden worden. Um eine Einschränkung von Art. 10 GG zu rechtfertigen, müssen diese aber hochrangige Rechtsgüter schützen.[896] Auch das BVerfG hat in seinem Urteil zum Nds.SOG 2005 klargestellt, dass der Eingriff in das Fernmeldegeheimnis bei der Annahme einer künftigen Straftat nur dann angemessen ist, wenn der zu schützende Gemeinwohlbelang allgemein sowie im konkreten Fall überragend wichtig ist.[897]

Daher ist ein auf die Besonderheiten der Telekommunikationsüberwachung zugeschnittenes Konzept erforderlich. Dieses muss zum einen den Schutz besonders hochrangiger Schutzgüter vorsehen, zum anderen aber auch berücksichtigen, ob die Telekommunikationsüberwachung überhaupt ein erforderliches und angemessenes Mittel zur Verhütung und Verfolgung der Verdachtsstraftaten sein kann.[898]

(1) Art. 34 a iVm Art. 30 Abs. 5 PAG

Der Straftatenkatalog des PAG in Art. 30 Abs. 5 PAG enthält eine (zahlenmäßig noch überschaubare[899]) abschließende Aufzählung einzelner Straftatbestände.[900] Besonderes Augenmerk wurde nach der Gesetzesbegründung auf den Strafrahmen gelegt, da Voraussetzung für die Aufnahme in den Katalog war, dass es sich um ausreichend gewichtige Straftaten han-

---

896 Dies gilt jedenfalls soweit eine Verlagerung in das Vorfeld einer drohenden Rechtsgutsverletzung stattfindet, vgl. BVerfGE 100, 313 (392); *Jarass*, in: Jarass/Pieroth, Art. 10 GG, Rn. 18.

897 Vgl. BVerfGE 113, 349 (385).

898 Vgl. BVerfGE 113, 349 (387 f.). Das BVerfG macht dies anschaulich an dem Beispiel, dass die Telekommunikationsüberwachung eingesetzt werden kann bei Begehungsverdacht der Verbreitung oder des öffentlichen Verwendens eines Kennzeichens einer verfassungswidrigen Organisation (§ 86 a StGB), obwohl nicht erkennbar ist, inwieweit eine Telekommunikationsüberwachung ein erforderliches und angemessenes Mittel zur Verhütung und Verfolgung dieser öffentlich begangenen Straftat sein kann, vgl. BVerfGE 113, 349 (388).

899 Zwar enthält auch das PAG mit seinen Verweisen auf das KrWaffG, das AuslG und das WaffG auch Weiterverweisungen, insgesamt sind aber erheblich weniger Delikte umfasst als z.B. von § 100 a StPO. Wann die praktische Erkennbarkeit einer maßgebenden Ermächtigungsgrundlage unter Weiterverweisungen leidet, hat das BVerfG in seiner Entscheidung zum AWG deutlich gemacht. Die Verweisungen des § 39 Abs. 2 AWG bezogen sich nicht nur auf Vorschriften des AWG und des Gesetzes über die Kontrolle von Kriegswaffen, sondern durch Verweisungen in diesen Normen auch auf weitere Straf- und Ordnungswidrigkeitentatbestände sowie auf Anlagen und Genehmigungstatbestände, vgl. BVerfGE 110, 33 (62).

900 Art. 30 PAG unterscheidet schwerwiegende Straftaten (Satz 1) und Straftaten von erheblicher Bedeutung (Satz 2). Während in Satz 2 aufgrund der Formulierung „insbesondere“ keine abschließende Aufzählung enthalten ist, ist dies bei Satz 1 der Fall, vgl. LT-Drucks. Bayern 15/2096, S. 31.

delt, die den Bereich der mittleren Kriminalität überschreiten oder zumindest an dessen Obergrenze liegen.[901] Von einer besonderen Schwere wird dabei ausgegangen, wenn die Delikte mit einer höheren Höchststrafe als fünf Jahre bewehrt sind.[902] Soweit Straftaten aufgenommen wurden, die diesen Strafrahmen unterschreiten, soll es sich dabei um Straftaten handeln, die einen besonderen Bezug zur Organisierten Kriminalität aufweisen, so bei der Bildung krimineller Vereinigungen und dem Menschenhandel, oder bei denen bereits aufgrund der besonderen Schutzwürdigkeit sowie des hohen Ranges der geschützten Rechtsgüter eine Aufnahme in den Straftatenkatalog gerechtfertigt ist, wie bei der Verbreitung der Kinderpornographie und der Vorbereitung eines Explosionsverbrechens.[903]

Eine präventiv-polizeiliche Kommunikationsüberwachung bei Brandstiftungsdelikten, Delikten über gefährliche Eingriffe in den Bahn-, Schiffs-, Luft- und Straßenverkehr sowie des räuberischen Angriffs auf Kraftfahrer vorzusehen, ist nach der hier vertretenen Auffassung verfassungsrechtlich nicht zulässig. Bei den in § 30 Abs. 5, Satz 1, 1. Halbsatz, Nr. 6 PAG aufgeführten Delikten handelt es sich zum Teil um konkrete Gefährdungsdelikte, die eine Gefährdung von Leib und Leben eines anderen Menschen voraussetzen. Der dahinterstehende Schutz der gefährdeten Person[904] wird bereits über die Straftaten gegen die körperliche Unversehrtheit und das Leben erreicht, wie es auch die Regelungen in Art. 30 Abs. 5 Nr. 4 und Art. 34 a Abs. 1 Nr.1 PAG vorsehen.[905]

Art. 30 Abs. 5, Satz 1, 2. Halbsatz PAG beinhaltet zudem eine Regelung für Ausnahmefälle, in denen aufgrund besondere Umstände des Einzelfalls dem Rechtsgüterschutz kein ausreichendes Gewicht beizumessen ist, obwohl eine schwerwiegende Straftat abgewehrt wird. Sie betrifft Fallgestaltungen, in denen vor Tatvollendung klar ist, dass dem Schutz der betroffe-

---

901 Vgl LT-Drucks. Bayern 15/2096, S. 52.

902 Vgl. LT-Drucks. Bayern 15/2096, S. 31.

903 Die Gesetzesbegründung LT-Drucks. 15/2096, S. 32 führt dazu aus: Bei der Gefahrenabwehr kann nicht das Strafmaß allein ausschlaggebend sein, da es wesentlich von den Tatfolgen bestimmt wird. Vielmehr sind die Gefahren, die für die öffentliche Sicherheit und Ordnung von den jeweiligen Straftaten ausgehen, maßgeblicher Gesichtspunkt in der Abwägung. Ziel ist gerade die Verhinderung schwerer Folgen.

904 Vgl. *Tröndle/Fischer*, § 315 StGB, Rn. 2 und *Lackner/Kühl*, § 315 StGB, Rn. 1 für gefährliche Eingriffe in den Bahn-, Schiffs- und Luftverkehr.

905 Eine Überwachung hinsichtlich der Anschläge des 11.September wären möglich gewesen zur Abwehr einer Lebensgefahr und auch hinsichtlich eines Verdachts bzgl. der Delikte §§ 211, 212, 316 c StGB. Auch aus der Bewertung in der Begründung des bayerischen Gesetzgebers ergibt sich nichts Gegenteiliges. Weder überschreiten die genannten Delikte die Höchststrafe von fünf Jahren, noch handelt es sich um Straftaten, die einen (erkennbaren) Bezug zur Organisierten Kriminalität aufweisen, vgl. LT-Drucks.Bayern 15/2096, S.31 ff..

nen Rechtsgüter ausnahmsweise kein hinreichendes Gewicht zukommt, um eine Telekommunikationsüberwachung zu rechtfertigen.[906]

(2) § 33 a iVm § 2 Nr. 10 Nds.SOG 2005

Der Deliktskatalog des § 2 Nr. 10 a Nds.SOG 2005 verweist unter Ausklammerung der §§ 154; 155 StGB auf alle Verbrechen des StGB.[907] Kann Art. 10 GG nur aufgrund hochrangiger Rechtsgüter eingeschränkt werden, so muss dies auch beim geschützten Rechtsgut des jeweiligen Verbrechens zum Ausdruck kommen. Hat der niedersächsische Gesetzgeber daher die die staatliche Rechtspflege schützenden Verbrechen[908] ausgeklammert, so sind derartige Überlegungen auch bei anderen Verbrechen anzustellen.[909] Die §§ 146; 151 StGB schützen das allgemeine Interesse an der Sicherheit und Zuverlässigkeit des Geldverkehrs und des Verkehrs mit Wertpapieren und Wertzeichen[910]; die gewerbsmäßige Bandenhehlerei nach §§ 259; 260 a StGB schützt Vermögenswerte[911]. Hochrangige Rechtsgüter, deren mögliche Verletzung Art. 10 GG einzuschränken geeignet wäre, sind darin kaum zu erkennen.[912]

---

906 Vgl. LT-Drucks. Bayern 15/4097, S. 3.

907 Der Deliktskatalog ist durch das Gesetz zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung, GVBl. S.654, geändert worden. Vgl. nunmehr die neuen Regelungen in § 2 Nr. 10 und 11 Nds.SOG.

908 Vgl. *Tröndle/Fischer*, Vor § 153 StGB, Rn. 2.

909 Die Auswahl der Delikte in § 2 Nr. 10 a und b Nds.SOG 2005 soll sich in erster Linie nach der Schwere der Delikte richten, vgl. *Unger/Siefken*, in: Böhrenz/Unger/Siefken, § 2 Nds.SOG, Anm. 17.

910 Vgl. *Tröndle/Fischer*, Vorbemerkung zur Geld- und Wertzeichenfälschung, Rn. 2.

911 Vgl. *Tröndle/Fischer*, § 259 StGB, Rn. 1.

912 Das BVerfG hat in seinem BND-Urteil die Beschränkungen des Telekommunikationsverkehrs durch den BND zum Zwecke der Erkennung im Ausland begangener Geldfälschungen als unverhältnismäßig angesehen, vgl. BVerfGE 100, 313 (384 f.). Die Zwecke, die nach § 3 Abs. 1, Satz 2 G-10 Beschränkungen des Fernmeldegeheimnisses erlauben, wurden durch das Verbrechensbekämpfungsgesetz vom 28.10.1994, BGBl. I S. 3186, ausgeweitet. Neben die Gefahr eines bewaffneten Angriffs (Nr.1) sind getreten die Gefahr der Begehung internationaler terroristischer Anschläge (Nr.2), der internationalen Verbreitung von Kriegswaffen und des konventionellen Rüstungshandels (Nr.3), des Drogenexports in Bundesrepublik (Nr.4), der im Ausland begangenen Geldfälschungen (Nr. 5) und der Geldwäsche im Zusammenhang mit den in Nummern 3 bis 5 genannten Handlungen (Nr.6). Das BVerfG hat festgestellt, dass der Überwachung nach dem G-10-Gesetz jeder Teilnehmer am internationalen Fernmeldeverkehr ausgesetzt sein kann, ohne dass dies mit seinem Verhalten in irgendeiner Weise in Beziehung gebracht werden könnte oder durch ihn veranlasst worden wäre. Dies führe zu einer schwerwiegenden Beeinträchtigung des Fernmeldegeheimnisses. Bei Geldfälschungen handele es sich aber weder um eine Gefahr, die in ihrer Schwere einem bewaffneten Angriff nahe komme oder derart gewichtige Rechtsgüter betreffe wie die übrigen durch das Verbrechensbekämpfungsgesetz eingefügten Gefahrentatbestände, noch hafte ihr in allen Begehungsformen dasjenige Gefahrenpotenzial an, das den übrigen Tatbeständen eigen sei. Geldfälschungen würden keine notwendig mit dem Ausland verbundene und nicht zwingend eine erhebliche Gefahr für Bestand und Sicherheit der Bundesrepublik bilden. Das schließe zwar nicht aus, dass in einzelnen Fällen Geldfälschungen großen Stils, die im Ausland erfolgen, die Geldwertstabilität der Bundesrepublik und damit die Wirtschaftskraft des Landes in einem Maß beeinträchtigen, das den anderen Gefahren nahe kommt. Eine Eingrenzung auf solche Fälle liege aber nicht vor. Das Ausmaß der Gefahr und das Gewicht der Grundrechtsbeeinträchtigung würden insofern außer Verhältnis geraten vgl. BVerfGE 100, 313 (385). Kritisch hierzu Möstl DVBl. 1999, 1394 (1398 ff.).

Gleiches gilt für den Verweis in § 2 Nr. 10 b Nds.SOG 2005 auf Vergehen der Gefährdung des demokratischen Rechtsstaates, des Landesverrats und der Gefährdung der äußeren Sicherheit sowie der öffentlichen Ordnung. Diese Delikte mögen zwar dem Rechtsgut nach abstrakt zur Einschränkung von Art. 10 GG geeignet sein, nicht aber im Hinblick auf den Strafrahmen. So sehen die §§ 86 und 86 a StGB als Rechtsfolge Geldstrafen oder Freiheitsstrafen bis zu drei Jahren vor. Den hinter diesen Vergehen stehenden Schutzgütern dürfte durch die Verweise auf die Verbrechen, die demselben Rechtsgüterschutz dienen[913], genügt sein.

Etwas anderes gilt für Straftaten gegen die sexuelle Selbstbestimmung. Die sexuelle Selbstbestimmung ist der Teil des der Menschenwürde entspringenden Persönlichkeitsrechts.[914] Dieses hohe Schutzgut ist trotz niedriger Strafandrohung bei einer Abwägung mit dem Fernmeldegeheimnis geeignet dieses einzuschränken.

Weiter verweist § 2 Nr. 10 b Nds.SOG 2005 auf die in § 138 Abs. 1 StGB genannten Vergehen und auf nach dem geschützten Rechtsgut und der Strafandrohung vergleichbare Vergehen. Auch diese gesetzliche Regelung genügt nicht den Anforderungen des Art. 10 GG. Die in § 138 StGB enthaltenen Vergehen schützen unterschiedliche Rechtsgüter. Sie reichen von Delikten des Landesverrats und der Gefährdung der äußeren Sicherheit[915] über Straftaten gegen die persönliche Freiheit[916] bis zu den gemeingefährlichen Straftaten[917]. Die Strafrahmen dieser Delikte umfassen eine Mindeststrafe von drei Monaten bis zu einer Höchststrafe von fünf Jahren.

Der Pauschalverweis auf alle Vergehen, die nach Schutzgut und Strafrahmen den dort aufgeführten Delikten vergleichbar sind, verstößt gegen das Bestimmtheitserfordernis.[918]

Der Polizei sind zwar mit den gemachten Vorgaben[919] Beurteilungsmaßgaben an die Hand gegeben worden. Doch ist nicht klar, wie aus der Bezugnahme auf das Rechtsgut einerseits

---

913 Z.B. §§ 94; 96 StGB.
914 Vgl. BVerfGE 47, 46 (73); E 49, 286 (298); *Jarass*, in: Jarass/Pieroth, Art. 2 GG, Rn. 48.
915 §§ 95; 96 Abs. 2 StGB.
916 § 234 a Abs. 3 StGB.
917 § 310 Abs. 1 Nr. 2 StGB.
918 Vgl. BVerfGE 113, 349 (378 ff.).
919 Vgl. *Unger/Siefken*, in: Böhrenz/Unger/Siefken, § 2 Nds.SOG, Anm. 17 und AB. 10, die einer Beurteilung der Vergleichbarkeit ebenfalls skeptisch gegenüber stehen.

und den Strafrahmen andererseits auf eine Vergleichbarkeit weiterer Straftaten geschlossen werden soll.[920]

Auch der Verweis auf alle im StGB enthaltenen banden- und gewerbsmäßig begangenen Vergehen steht nicht in Einklang mit Art. 10 GG. Die banden- und gewerbsmäßigen Vergehen mögen vor dem Hintergrund aufgenommen worden sein, die Organisierte Kriminalität wirksam bekämpfen zu wollen. Das allein kann einen Eingriff in Art. 10 GG aber nicht rechtfertigen. Dies zeigt sich daran, dass damit auch der einfache Bandendiebstahl umfasst ist, der schon verwirklicht ist, wenn drei Personen gemeinsam einen Diebstahl begehen.[921] Hierbei kann nicht automatisch von organisierter Kriminalität ausgegangen werden.

Schon beim Verdacht einer geplanten Gehilfentätigkeit eine Telekommunikationsüberwachung zuzulassen,[922] verstößt ebenfalls gegen Art. 10 GG. Der Gehilfe gefährdet das geschützte Rechtsgut nicht selbst. Hinzu tritt, dass eine Teilnahme bei allen in § 2 Nr. 10 Nds.SOG 2005 genannten Delikten ausreichen soll. Dies kann sowohl hinsichtlich der dahinter stehenden Rechtsgüter als auch im Hinblick auf die Strafrahmenhöhe keine Geltung haben, zumal die Strafe für den Gehilfen nach §§ 27 Abs. 2; 49 StGB abgemildert wird.

In seiner Entscheidung zum Nds.SOG 2005 ist auch das BVerfG zu dem Ergebnis gekommen, dass der niedersächsische Gesetzgeber den verfassungsrechtlichen Anforderungen an den Rang des geschützten Rechtsguts und an die tatsächlichen Anhaltspunkte der Rechtsgutsgefährdung nicht gerecht geworden ist,[923] da den in § 2 Nr. 10 Nds.SOG 2005 aufgeführten Straftaten kein auf die Besonderheiten der Telekommunikationsüberwachung zugeschnittenes gesetzgeberisches Konzept zu entnehmen sei, das sich auf den Schutz besonders hochrangiger Rechtsgüter bezieht und beschränkt[924] und sich aus der Gesetzesbegründung auch

---

920 Vgl. BVerfGE 113, 349 (379 f.).

921 Der Große Senat für Strafsachen hat mit der Entscheidung vom 22.03.2001, BGHSt 46, 321 ff., die frühere Rechtsprechung aufgehoben, wonach eine Bande schon beim Zusammenwirken von zwei Personen vorliegen konnte.

922 § 33a Abs. 1 Nr. 2, § 2 Nr. 10 d Nds.SOG 2005.

923 Vgl. BVerfGE 113, 349 (387). Was die Überwachung der Kontakt- und Begleitpersonen angeht, so fehlen der Norm nach Ansicht des BVerfG Anhaltspunkte für die abwägende Prüfung, ob die Schwere der zu erwartenden Straftat eine Telekommunikationsüberwachung dieses Personenkreises rechtfertige, vgl. BVerfGE 113, 349 (389).

924 Vgl. BVerfGE 113, 349 (378 ff.).

nicht ergebe, dass der Katalog gerade auf die Telekommunikationsüberwachung ausgerichtet ist.[925]

(3) § 34 a ThPAG iVm § 100 a StPO

Das ThPAG verweist für die Straftatenverhinderung durch präventive Telekommunikationsüberwachung auf den Katalog des § 100 a StPO.[926]

Der Katalog des § 100 a StPO umfasst nahezu 100 Delikte,[927] welche teilweise Weiterverweisungen enthalten.[928] Zwischen den geschützten Rechtsgüter und den vorgesehenen Strafrahmen bestehen große Unterschiede. So reicht der Rechtsgüterschutz von der Geldwäsche nach § 261 StGB, welche die Rechtspflege und das Ermittlungsinteresse der Strafverfolgungsbehörden schützt[929], über den Schutz des Rechtsguts Leben nach §§ 211; 212 StGB. Das Strafmaß reicht bei § 97 Abs. 2 StGB von der Geldstrafe bis zur Freiheitsstrafe von maximal drei Jahren, während § 211 StGB die lebenslange Freiheitsstrafe vorsieht. Mit dem Einschluss von Fahrlässigkeitsdelikten und der Möglichkeit, die Telekommunikationsüberwachung auch bei der Teilnahme an den aufgeführten Delikten anzuordnen, enthält § 100 a StPO auch Fälle aus dem unteren Kriminalitätsbereich.[930]

---

925 Eine Einengung des Katalogs könne auch nicht durch die Auslegung des Begriffs der „Straftat von erheblicher Bedeutung“ erfolgen, da es sich dem Wortlaut des § 33 a Abs. 1 Nr. 2 iVm § 2 Nr.10 Nds.SOG 2005 nach um einen Oberbegriff für die aufgezählten Straftaten, nicht aber um ein zusätzliches Tatbestandsmerkmal handele, vgl. BVerfGE 113, 349 (388). Eine Einschränkung vor dem Hintergrund vorzunehmen, dass die Regelungen im Zusammenhang mit der Bekämpfung der Organisierten Kriminalität und des Terrorismus geschaffen worden sind, vgl. LT-Drucks. Nds. 15/240, S. 16, scheide aus, da dieses gesetzgeberische Ziel weder im Wortlaut der Ermächtigung noch in der Typik der aufgeführten Gesetze einen Ausdruck gefunden habe, vgl. BVerfGE 113, 349 (388).

926 Der Katalog des § 100 a StPO war unter anderem Gegenstand der Max-Planck-Studie, die im Auftrag des Bundesministeriums der Justiz über die Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, b StPO und anderer verdeckter Ermittlungsmaßnahmen erstellt wurde und deren Abschlussbericht im Jahr 2003 durch *Albrecht, Hans-Jörg, Dorsch, Claudia und Krüpe, Christiane* vorgelegt wurde.

927 *Albrecht/Dorsch/Krüpe*, 2003, S. 13 ff. enthält einen guten Überblick über die in § 100 a StPO aufgezählten Delikte.

928 So verweist § 100 a Nr. 3 StPO auf § 52 Abs. 1 Nr. 2 d WaffG, der wie folgt lautet: Mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren wird bestraft, wer ohne Erlaubnis nach § 2 Abs. 2 in Verbindung mit Anlage 2 Abschnitt 2 Unterabschnitt 1 Satz 1 in Verbindung mit § 29 Abs. 1, § 30 Abs. 1, Satz 1 oder § 32 Abs. 1, Satz 1eine Schusswaffe oder Munition in den oder durch den Geltungsbereich dieses Gesetzes verbringt oder mitnimmt.

929 Zu den verschiedenen Ansichten zum geschützten Rechtsgut des § 261 StGB siehe *Tröndle/Fischer*, § 261 StGB, Rn. 3.

930 Vgl. dazu ausführlich *Neuhaus*, in: FS für Rieß, S. 373 ff. *Neuhaus* sieht die Aufnahme von Bagatellkriminalität in den Katalog des § 100 a StPO dadurch gegeben, dass nicht nur zahlreiche Vergehen, wie § 244 I Nr. 3, 260, 261 StGB, § 92 a AuslG aufgenommen wurden, sondern zusätzlich es beim Verdacht der Teilnahme zur Strafrahmenverschiebung nach § 27 Abs. 2, Satz 2, § 49 StGB kommt, S. 387. Der Gesetz-

Schon für repressive Maßnahmen wird der Katalog des § 100 a StPO als veraltet oder zu weitläufig angesehen.[931] Forderungen nach einer Einschränkung beziehen sich dabei auf die in § 100 a I Nr. 1 b und d StPO[932] genannten Delikte, die als nicht mehr zeitgemäß eingestuft werden.[933]

Das BVerfG hat sich zwar noch nicht dem Katalog des § 100 a StPO, jedoch mit dem Katalog des § 100 c Abs. 1 Nr. 3 StPO auseinandergesetzt.[934] Es ist dabei zu dem Ergebnis gekommen, dass die verfassungsrechtlichen Vorgaben eingehalten sind, soweit eine Höchststrafe von über fünf Jahren für die Straftat, derentwegen die repressive Wohraumüberwachung angeordnet wird, vorgesehen ist. Delikte, die lediglich der mittleren Kriminalität zuzuordnen sind, werden den Anforderungen dagegen nicht gerecht.[935] Unmittelbar ist diese Rechtsprechung nicht auf die präventive Telekommunikationsüberwachung übertragbar, da Art. 10 GG keine Art. 13 Abs. 3 GG vergleichbare Regelung enthält. Auch hat das BVerfG zu verstehen gegeben, dass jedenfalls der Eingriff in das Fernmeldegeheimnis durch Auskunftserteilung nicht mit der akustischen Wohnraumüberwachung vergleichbar ist, da keine Kenntnis über die Gesprächsinhalte erlangt wird.[936] Dennoch liefert diese Rechtsprechung wichtige Anhaltspunkte dafür, aufgrund welcher möglicherweise bevorstehenden Straftaten eine präventive Telekommunikationsüberwachung angeordnet werden darf.

---

entwurf zur Telekommunikationsüberwachung und anderen verdeckten Ermittlungsmaßnahmen vom 18.04.2007 sieht vor, den Katalog von Straftaten, die Anlass für eine Telekommunikationsüberwachungsmaßnahme sein können, auf schwere Straftaten zu beschränken. Dabei orientiert sich der Gesetzesentwurf auch an einer Mindesthöchststrafe von 5 Jahren Freiheitsstrafe, vgl. BT-Drucks. 16/5846, S. 40 ff.

931 *Neuhaus*, in: FS für Rieß, S.373 (384 ff.) kritisiert insbesondere die Einbeziehung der abstrakten Gefährdungsdelikte. Siehe auch *Albrecht/Dorsch/Krüpe*, 2003, S. 16 ff. Die in der Max-Planck-Studie getroffenen Feststellungen können zwar schon wegen der unterschiedlichen Zielrichtungen der Maßnahmen nicht ohne weiteres auf den präventiven Bereich übertragen werden, doch liefern sie wichtige Anhaltspunkte für die Telekommunikationsüberwachung zur Gefahrenabwehr.

932 § 100 a Abs. 1 Nr. 1 b) StPO verweist auf die Straftaten zur Landesverteidigung; § 100 a Abs. 1 Nr. 1 d) StPO auf §§ 16, 19 iVm § 1 Abs. 3 Wehrstrafgesetz.

933 Vgl. *Albrecht/Dorsch/Krüpe*, Kurzbericht, S. 33. Reformüberlegungen gehen dahin, ein Kombinationsmodell einzuführen, das einerseits für den Bereich der traditionellen Kriminalität auf einen Katalog rekurriert, für die Fälle der Transaktionskriminalität hingegen auf die banden- und/oder gewerbsmäßige Tatbegehung abstellt, Netzwerkstrukturen verlangt oder allgemein an die marktförmige, kommunikative Begehungsform unter den Voraussetzungen einer abstrakten Schwereandrohung anknüpft, vgl. *Albrecht/Dorsch/Krüpe*, 2003, S. 464.

934 Vgl. BVerfGE 109, 279 ff. Aufgrund der Änderungen durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007, BGBl. I, S. 3198, sind die Katalogtaten nunmehr in § 100 c Abs. 2 StPO aufgeführt.

935 Vgl. BVerfGE 109, 279 (348 f.).

936 Vgl. BVerfGE 109, 279 (345).

Stellt das BVerfG darauf ab, dass ein Eingriff in das Fernmeldegeheimnis durch Auskunftserteilung weniger schwer wiegt, weil keine Kenntnisnahme der Gesprächsinhalte erfolgt, so gilt dies nicht, wenn in das Fernmeldegeheimnis mittels Inhaltsüberwachung eingegriffen wird. Die präventive Telekommunikationsüberwachung deswegen nur bei Verdachtstaten mit einer höheren Höchststrafe als fünf Jahre zuzulassen, ist nicht zwingend. Bei präventiven Maßnahmen soll die Rechtsgutsverletzung, also der Schadenseintritt, verhindert und damit der Schutzauftrag aus Art. 2 Abs. 2, Satz 1 GG erfüllt werden.[937] Die staatliche Schutzpflicht für das Leben ist umfassend; da das menschliche Leben einen Höchstwert darstellt, muss diese Schutzverpflichtung besonders ernst genommen werden.[938] Die Schutzpflicht gebietet es dem Staat, sich schützend und fördernd vor das Leben zu stellen. An diesem Gebot haben sich alle staatlichen Organe, je nach ihren besonderen Aufgaben auszurichten.[939] Sie gilt auch für die körperliche Unversehrheit.[940] Bei repressiven Maßnahmen ist die Rechtsgutverletzung dagegen schon eingetreten und dem staatlichen Strafverfolgungsanspruch ist zur Durchsetzung zu verhelfen. Präventive Maßnahmen, die den Schadenseintritt verhindern können und damit dem Grundrechtsschutz des Bürgers zu seiner Wirksamkeit verhelfen, können daher unter weniger strengen Voraussetzungen als repressive zulässig sein.[941] Der grundrechtliche Schutz des Lebens, dessen tatsächliche Beeinträchtigung irreparabel ist, ist weit vorzuverlagern und bereits auf Gefährdungen zu erstrecken.[942] Es geht um die Abwehr drohender oder bereits eingetretener Gefahren für grundrechtlich geschützte Rechtsgüter. Sie zu schützen, ist die Verpflichtung der staatlichen Gewalt.[943] Ihren Rechtswirkungen nach sind die grundrechtlichen Schutzpflichten für die Staatsgewalten daher in erster Linie Gefahren- und Störungsabwehrpflichten.[944]

---

937 Art. 2 Abs. 2, Satz 1 GG normiert über Abwehrrechte hinaus objektiv-rechtliche Handlungsgebote an den Staat und seine Organe, das Recht auf Leben und körperliche Unversehrtheit zu schützen und zu fördern, BVerfGE 39, 1 (36 ff., 42); E 45, 187 (254 f.); E 46, 160 (164 f.); *Schulze-Fielitz*, in: Dreier (Hrsg.), Art. 2 Abs. 2 GG, Art. 76.

938 Vgl. BVerfGE 46, 160 (164); *Murswiek*, in: Sachs (Hrsg.), Art. 2 GG, Rn. 188

939 So *Kunig*, in: v.Münch/Kunig (Hrsg.), Art. 2 GG, Rn. 55 unter Hinweis auf BVerfGE 46, 160 (164).

940 Vgl. *Schulze-Fielitz*, in: Dreier (Hrsg.), Art. 2 GG, Rn. 77; *Murswiek*, in: Sachs (Hrsg.), Art. 2 GG, Rn. 189.

941 So für die Datenübermittlung zu unterschiedlichen Zwecken BVerfGE 100, 313 (394 f.).

942 Vgl. *Lorenz*, in HStR VI, § 128, Rn. 31.

943 Vgl. *Stern*, Staatsrecht, Band III/1, S. 949.

944 Vgl. *Stern*, Staatsrecht, Band III/1, S. 949 f., der jedoch auch davon ausgeht, dass den Staatsorganen ein Spielraum für die Umsetzung der Schutzpflichten eingeräumt ist. Nach *Lorenz*, HStR VI, § 128, Rn. 53 sind Maßnahmen zur Abwehr lebens- oder gesundheitsbedrohender Gefahren gefordert. Siehe auch *Kunig*, in: v.Münch/Kunig (Hrsg.), Art. 2 GG, Rn. 68. Nach *Schultze-Fielitz*, in: Dreier (Hrsg.), Art. 2 Abs. 2 GG, Rn. 80 gebietet Art. 2 Abs. 2 GG konkrete und abstrakte Gefahren für Leben und Gesundheit abzuwehren und im Sinne vorbeugender Gefahrenabwehr und im Sinne der Gefahrenvorsorge und des Nachweltschutzes präventiv zu minimieren. *Murswiek*, in: Sachs (Hrsg.), Art. 2 GG, Rn. 191 sieht zudem eine

Ein Pauschalverweis auf § 100 a StPO ist aber mit Art. 10 GG nicht vereinbar, da dieser neben Delikten der Schwerkriminalität auch Bagatellstraftaten enthält. Insbesondere ist nicht zu erkennen, wie mittels Telekommunikationsüberwachung Fahrlässigkeitsdelikten vorgebeugt werden soll.

So hält vor dem Hintergrund, dass der thüringer Gesetzgeber der Polizei die Möglichkeit der Telekommunikationsüberwachung zur Bekämpfung der schweren Kriminalität, eröffnen wollte[945], der umfangreiche Katalog des § 100 a StPO nicht stand.[946] Dem könnte entgegengehalten werden, dass es vorteilhaft ist, eine präventive Telekommunikationsüberwachung unter den gleichen Voraussetzungen zuzulassen wie eine repressive. Eine solche Betrachtungsweise würde aber nicht berücksichtigen, dass bei strafprozessualen Maßnahmen die Verletzung von Rechtsgütern bereits stattgefunden hat, während bei der präventiven Telekommunikationsüberwachung zur Straftatenverhinderung die Eingriffsbefugnis weit im Vorfeld einer drohenden Verletzung des Rechtsguts ansetzt. Diese Vorverlagerung kann im Hinblick auf das Fernmeldegeheimnis dann nicht durch den mit den Maßnahmen beabsichtigenden Rechtsgüterschutz gerechtfertigt werden, wenn es sich bei den Rechtsgütern, von denen der Schaden abzuwenden ist, nicht um hochrangige handelt. Hochrangige Rechtsgüter sind jedenfalls Leben, Leib und Freiheit der Bürger.[947] Ob das hinter einem Straftatbestand stehende Rechtsgut hochrangig ist, kann sich zudem aus dem jeweiligen Strafrahmen ergeben.[948]

Bei Fahrlässigkeitsdelikten ist zu berücksichtigen, dass der dahinter stehende Rechtsgüterschutz über die entsprechende Vorsatztat erreicht wird.[949] Bei diesen Delikten können ohnehin schwerlich Tatsachen vorliegen, die die Annahme rechtfertigen, dass der potenzielle Täter sie begehen will, da er gerade ohne Vorsatz handelt.[950]

Verpflichtung des Gesetzgebers, Verletzungen von Leben und körperlicher Unversehrtheit mit Strafsanktionen zu bedrohen.

945 Vgl. LT-Drucks. Th. 3/2128, S.1.

946 Denn dieser enthält neben Fahrlässigkeitsdelikten auch Straftaten aus dem unteren Kriminalitätsbereich. AA wohl *Würtenberger/Heckmann*, 2005, Rn. 625 c.

947 Vgl. Art. 2 Abs. 2, Satz 1 GG.

948 Vgl. BVerfGE 109, 279 (344 f.; 349).

949 Vgl. zum Schutz des Lebens z.B. § 212 StGB (Totschlag) und § 222 (fahrlässige Tötung) StGB.

950 Zur fahrlässigen Tatbestandsverwirklichung vgl. *Tröndle/Fischer*, § 15 StGB, Rn. 12 ff.

Auch ist erforderlich, dass die Telekommunikationsüberwachung tatsächlich zur Verhinderung von Straftaten beitragen kann.[951] Ist sie zudem vor dem Hintergrund normiert worden, die Organisierte Kriminalität wirksam zu bekämpfen, ist dies bei den in den Katalog aufgenommenen Straftaten ebenfalls zu berücksichtigen.[952]

(4) Fazit

Solange die Telekommunikationsüberwachung aufgrund eines eng umrissenen Deliktkatalogs angeordnet wird, dessen Delikte dem hohen Schutzgut des Art. 10 GG dadurch Rechnung tragen, dass sie in einem Bereich angesiedelt sind, der den der mittleren Kriminalität übersteigt und sich dies im geschützten Rechtsgut und dem Strafrahmen niederschlägt, ist eine Vereinbarkeit mit dem Fernmeldegeheimnis gegeben. Der komplette Katalog des § 100a StPO vermag daher die Einschränkung des Art. 10 GG zu Zwecken der Gefahrenabwehr nicht zu rechtfertigen. Gleiches gilt für den Katalog des Nds.SOG 2005, der mit seinen umfassenden Verweisungen eine unnötige Weite und damit Unbestimmtheit birgt. Bei § 30 Abs. 5, Satz 1 PAG sind die Gefährdungsdelikte nicht geeignet, das Fernmeldegeheimnis zu beschränken.

d) Richtervorbehalt und Verfahrensanforderungen

Verdeckte Grundrechtseingriffe durch Sicherheitsbehörden können ihren Zweck im Rahmen der Gefahrenabwehr oder der Strafverfolgung nur dann erfüllen, wenn sie von dem Betroffenen nicht bemerkt werden. Ein vorgängiger Rechtsschutz würde solche Maßnahmen zur Erfolglosigkeit verurteilen. Aber auch ein nachträglicher Rechtsschutz scheidet in der Regel aus, da die gesetzlich vorgesehene nachträgliche Unterrichtung der von den Überwachungsmaßnahmen Betroffenen in der Praxis nur selten stattfindet.[953] Zudem macht der nachträgliche Rechtsschutz die Telekommunikationsüberwachung nicht ungeschehen. Dieses Rechtsschutzdefizit muss daher durch andere Verfahrenssicherungsmaßnahmen kompensiert werden.[954]

---

951 Vgl. BVerfGE 113, 348 (388).

952 Vgl. BVerfGE 113, 348 (388).

953 Vgl. *Kutscha*, NVwZ 2003, 1296 (1297 f.). Vgl. zur Information des Betroffenen und ihren Ausnahmen z.B. § 22 Abs. 8 PolG BW mit den Ausführungen von *Würtenberger/Heckmann*, 2005, Rn. 690 ff.

954 So fordert der SächsVerfGH LKV 1996, 273 (287) in seiner Entscheidung zum sächsischen Polizeirecht vom 14.05.1996 für solche verdeckten Maßnahmen eine „besondere Ausgestaltung des Grundrechtsschutzes durch Verfahren“. Siehe auch *Gusy*, NJW 1981, 1581 (1584 f.).

Alle der hier untersuchten Polizeigesetze haben die Anordnung der Telekommunikationsüberwachung unter einen Richtervorbehalt gestellt.[955] Zwar sind organisatorische und verfahrensmäßige Vorkehrungen grundsätzlich zur Sicherung der durch Art. 10 GG gewährleisteten Vertraulichkeit vor staatlichen Eingriffen oder Übergriffen Dritter erforderlich,[956] Richtervorbehalte sind im Grundgesetz jedoch nur in Art. 13 GG und Art. 104 GG vorgesehen. Wie die Kontrolle bei Art. 10 GG auszugestalten ist, schreibt die Verfassung nicht vor. Dem Gesetzgeber steht es frei, die ihm geeignete Form zu wählen, wenn sie nur hinreichend wirksam ist.[957]

Das BVerfG geht davon aus, dass die Richter aufgrund ihrer persönlichen und sachlichen Unabhängigkeit und ihrer strikten Unterwerfung unter das Gesetz die Rechte der Betroffenen im Einzelfall am besten und sichersten wahren können[958] und „ alle staatlichen Organe verpflichtet sind, dafür Sorge zu tragen, dass der Richtervorbehalt als Grundrechtssicherung praktisch wirksam wird“[959]. So haben die Landesgesetzgeber neben der Konkretisierung der verfassungsmäßig vorgegebenen Richtervorbehalte für Eingriffe in Art. 13 GG und Art. 104 Abs. 2 GG weitere Richtervorbehalte für verdeckte Grundrechtseingriffe bei der polizeilichen Gefahrenabwehr, so für den Einsatz verdeckter Ermittler, die polizeiliche Beobachtung und die Rasterfahndung geschaffen[960].

Abgesehen davon, ob der Richtervorbehalt tatsächlich einen vollwertigen Rechtsschutz des Betroffenen bietet, stellt sich die Frage, ob ein Richter als Teil der Judikative vor dem Hintergrund des Gewaltenteilungsgrundsatzes überhaupt berechtigt ist, im Vorfeld der Maßnah-

---

955 Art. 34 c Abs. 1 iVm Art. 34 Abs. 4, Sätze 1 und 2 PAG; § 34 a Abs. 2 ThPAG; § 33 a Abs. 4 Nds.SOG; § 31 Abs. 5 POG; § 15 a Abs. 4 HSOG.

956 Vgl. *Hermes*, in: Dreier (Hrsg.), Art. 10 GG, Rn. 88 ff.

957 Vgl. BVerfGE 100, 313 (361).

958 So BVerfGE 103, 142 (151); BVerfG NJW 2003, 1787 (1792). Die Literatur sieht ähnlich wie das BVerfG die Funktion des Richtervorbehalts in der Gewährleistung eines *präventiven* Grundrechtsschutzes durch die Dritte Gewalt, der insbesondere bei Überraschungseingriffen der Exekutive notwendig sei, vgl. *Kutscha*, NVwZ 2003, 1296 (1298); *Amelung*, NStZ 2001, 337 (338); *Rabe von Kühlwein*, 2001, S. 417 *Asbrock*, ZRP 1998, 17 (19); *Bachmann*, 1994, S. 72 ff.; *Hilger*, JR 1990, 485 ff. Nach *Würtenberger/Heckmann*, 2005, Rn. 577 erzwingen die vom BVerfG in BVerfGE 65, 1 (44) geforderten organisatorischen und verfahrensrechtlichen Vorkehrungen keinen Richtervorbehalt. Vielmehr stünden dem Gesetzgeber bei der Verfahrensgestaltung neben dem Richtervorbehalt auch sog. Behördenleitervorbehalte, Unterrichtungspflichten gegenüber dem Betroffenen und eine Unterrichtung des Landtags zur Verfügung.

959 BVerfGE 105, 239 (248). In diesem Beschluss hat das BVerfG im Hinblick auf Art. 2 Abs. 2, Satz 2 GG den besonderen Stellenwert des in Art. 104 Abs. 2 GG verankerten Richtervorbehalts zur Geltung gebracht.

960 Siehe dazu *Kutscha*, NVwZ 2003, 1296 (1298); *Roggan*, 2003, S. 90 f. und ausführlich die Darstellungen bei *M. Koch*, 1999, S. 206 ff.; *Bernsmann/Jansen*, StV 1998, 217 ff.; *Lisken/Mokros*, NVwZ 1991, 609 ff.

me (mit-) zu entscheiden.[961] Maßnahmen der Gefahrenabwehr betreffen typische Verwaltungsaufgaben der Polizei. Eine „verwaltungsbegleitende“ richterliche Kontrolle[962] würde sich darauf beschränken, eine Art „Unbedenklichkeitsbescheinigung“, bezogen auf den jeweiligen Erkenntnisstand und die einschlägige Rechtslage, auszustellen.[963]

Gerade im Bereich der heimlichen Eingriffe, in denen nachträglicher Rechtsschutz den Eingriff nicht mehr verhindern kann und zusätzlich von der Information des Betroffenen durch die Behörden abhängig ist, kann die vorgeschaltete gerichtliche Kontrolle jedoch zum Rechtsschutz des Betroffenen beitragen, da sie durch ein Organ erfolgt, dass außerhalb der Eingriffsverwaltung steht.[964]

Nach Ansicht von *Kutscha*[965] vermögen die Richtervorbehalte einen vollwertigen Rechtsschutz für die Betroffenen nicht zu bieten. Es fehle an der Gewährung rechtlichen Gehörs der Betroffenen gemäß Art. 103 Abs. 1 GG, so dass der Richter sich bei seiner Entscheidung lediglich auf die ihm von den Ermittlungsbehörden vorgelegten Informationen stützen könne[966]; die Interessenlage des Betroffenen sei ihm nicht bekannt, weshalb er in der Regel keine qualitativ vergleichbare Rechtsschutzentscheidung treffen könne.[967]

Zwar gilt im FGG-Verfahren, welches für die hier untersuchten präventiven Ermittlungsmaßnahmen Anwendung findet[968], der Amtsermittlungsgrundsatz[969], doch wird sich der Er-

---

961 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 578; *Lisken/Mokros*, NVwZ 1991, 609 (610); *Götz*, 2001, Rn. 515. Nach *Rimmele*, SächsVBl. 1996, 32 (35), würde eine weitläufige Anordnung von Richtervorbehalten die grundgesetzlich garantierte Verwaltungsverantwortung tangieren.

962 Kritisch hierzu *Schmidt-Aßmann*, in: Maunz/Dürig, Art. 19 Abs. 4 GG, Rn. 176; auch der SächsVerfGH in JZ 1996, 957 (964) sieht diese Bedenken gegen den Richtervorbehalt, hält sie aber bei „geeigneter Ausgestaltung dieses Instituts“ für unüberwindbar.

963 Zu den Möglichkeiten und der Optimierung des Instruments des Richtervorbehalte vgl. *Gusy*, ZRP 2003, 275 (277).

964 Auch *Würtenberger/Heckmann*, 2005, Rn. 578 gehen davon aus, dass die Einschaltung eines Richters eine Fehlinterpretation der Rechtslage und damit eine rechtswidrige Entscheidung der Polizei verhindern helfen kann. Siehe zu dem Richtervorbehalten im Polizeirecht und der daraus resultierenden Rechtsschutzproblematik *H.Wolter*, DÖV 1997, 939 (944 f.) sowie *Würtenberger*, 2006, Rn. 174 f.

965 Ausführlich *Kutscha*, NVwZ 2003, 1296 (1298 f.).

966 Vgl. *Kutscha*, NVwZ 2003, 1296 (1298), *Würtenberger/Heckmann*, 2005, Rn. 578. Siehe auch *Amelung*, NStZ 2001, 337 (342); *Aschmann*, 1999, S. 170 f.; *Gusy*, JZ 1998, 167 (171 f.); aA *Braun*, NVwZ 2000, 375 (377 f.), der zu bedenken gibt, dass in einem Rechtsstaat a priori davon auszugehen ist, dass die Polizei auch die Interessen der Betroffenen ausreichend mit einbezieht.

967 Vgl. *Kutscha*, NVwZ 2003, 1296 (1298); siehe dazu *Rabe von Kühlewein*, 2001, 422 ff.

968 Das Anordnungsverfahren für die präventive Telekommunikationsüberwachung durch die Landespolizeibehörden richtet sich in allen untersuchten Polizeigesetzen nach dem FGG. § 33 a Abs. 4, Satz 5 iVm § 19 Abs. 4, Satz 1 Nds.SOG; § 15 a Abs. 4, Satz 2 iVm § 39 Abs. 1, Satz 3 HSOG; § 31 Abs. 5, Satz 6 iVm §

mittlungsrichter maßgeblich auf die Angaben der Gefahrenabwehrbehörden in ihrem Anordnungsantrag stützen.[970] Aufgrund dieser einseitigen Informationsbasis besteht die Gefahr, dass eine eigenständige richterliche Prüfung der gesetzlichen Eingriffsvoraussetzungen nicht stattfindet.[971]

Gestützt wird diese Ansicht durch die Untersuchungsergebnisse der an der Universität Bielefeld im Jahr 2002 durchgeführten Studie zu den „Wirksamkeitsbedingungen von Richtervorbehalten bei Telefonüberwachungen“[972]. Diese Studie kommt zu dem Ergebnis, dass die Richter ihrer Kontroll- und Dokumentationspflicht, die sie nach dem Willen des Gesetzgebers als Ermittlungsrichter bei der Überprüfung eines Anordnungsantrags bezüglich einer Telefonüberwachung haben, nur unzureichend erfüllen.[973]

Nach dem Ergebnis der Studie waren gemessen an den gesetzlichen Kriterien[974] nur knapp ein Viertel der richterlichen Beschlüsse vollständig.[975] Bezeichnend sind auch die Schlussfolgerungen, welche die Verfasser der Studie ziehen: „Weder Staatsanwälte noch Richter mochten sich die Ansicht zu eigen machen, dass der Richtervorbehalt als eine besondere Form des Grundrechtsschutzes für die Betroffenen anzusehen sei“[976] und „Richter fühlen sich nicht dazu aufgerufen, bei ihren Entscheidungen auch die Interessen der über die Tele-

---

21 Abs. 1, Satz 3 POG; § 34 a Abs. 2, Satz 5 ThPAG; Art. 34 c Abs. 1; Art. 34 Abs. 4, Satz 2; Art. 21 Abs. 1, Satz 3 PAG.

969 Vgl. § 12 FGG.

970 Vgl. *Braun*, NVwZ 2000, 375 (377); *Lisken/Mokros*, NVwZ 1991, 609 (611); *Aschmann*, 1999, S. 170..

971 Vgl. *Kutscha*, NVwZ 2003, 1296 (1298).

972 *Backes/Gusy/Begemann/Doka/Finke*, Betrifft JUSTIZ, 2003, 14: Der Studie liegt eine Aktenanalyse von 554 Telefonüberwachungen aus 173 Strafverfahren zugrunde. Der Schwerpunkt der Untersuchung liegt auf TÜ-Verfahren der Jahre 1996-1998. Die Untersuchungen zur Telefonüberwachung beschränken sich auf vier Staatsanwaltschaften, drei aus Nordrhein-Westfalen und einer aus einem Stadtstaat. Darunter sind zwei im Wesentlichen großstädtisch geprägte Staatsanwaltschaftsbezirke und zwei mit größeren ländlichen Anteilen.

973 Vgl. *Backes/Gusy/Begemann/Doka/Finke*, Betrifft JUSTIZ, 2003, 14.

974 Ein richterlicher Beschluss zur Anordnung einer repressiven Telekommunikationsüberwachung ist dann vollständig, wenn er drei Kriterien erfüllt: Der Beschluss muss die Katalogtat benennen, derentwegen die Telefonüberwachung angeordnet wird; der Beschluss muss tatsachenbezogene Ausführungen enthalten, die im konkretem Fall den Tatverdacht begründen und der Beschluss muss einzelfallspezifische Ausführungen zu der Frage enthalten, ob andere Ermittlungsmaßnahmen aussichtslos oder jedenfalls weniger erfolgversprechend sind. Kurz gesagt, der Ermittlungsrichter hat das Vorliegen der Eingriffsvoraussetzungen, also die Rechtmäßigkeit des Eingriffs zu überprüfen, vgl. *Meyer-Goßner*, § 100 b StPO, Rn. 3.

975 In zwei Dritteln der Fälle wurde nur zu einem oder zwei Merkmalen Ausführungen gemacht, und fast 10% der Beschlüsse enthielten nicht ein einziges der geforderten Kriterien, vgl. *Backes/Gusy/Begemann/Doka/Finke*, Betrifft JUSTIZ 2003, 14 (15). Die Anforderungen an die richterlichen Anordnungsbeschlüsse ergeben sich aus § 100 b Abs. 2 StPO. In weit über 90% der Fälle wurde der von der Staatsanwaltschaft mit einem Überwachungsantrag vorgelegte Beschlussentwurf vom Richter wortwörtlich übernommen, vgl. *Backes/Gusy/Begemann/Doka/Finke*, Betrifft JUSTIZ 2003, 14 (15).

976 *Backes/Gusy/Begemann/Doka/Finke*, Betrifft JUSTIZ, 2003, 14 (17).

fonüberwachung naturgemäß nicht informierten Beteiligten in irgendeiner Weise zu berücksichtigen; es fehlt jegliche Sensibilität dafür, dass es sich hierbei um Grundrechtseingriffe handelt“[977].

Im Ergebnis wird die Untersuchung bestätigt durch die Studie des Max-Planck-Instituts.[978] Diese kommt zu der Feststellung, dass Gesetz und Wirklichkeit unter dem Gesichtpunkt der Transparenz, Kontrolle und Nachvollziehbarkeit bei Telekommunikationsüberwachungsmaßnahmen auseinander klaffen.[979]

Unabhängig davon, ob deswegen eine Reform des bestehenden Ermittlungsrichtersystems stattzufinden hat[980] oder nicht, stellt sich die Frage nach möglichen Alternativen.[981] Eine zwingende Notwendigkeit für einen Richtervorbehalt als verfassungsmäßige Voraussetzung für verdeckte Grundrechtseingriffe des Staates lässt sich dem Grundgesetz nicht entnehmen. Auch in der verfassungsgerichtlichen Rechtsprechung wird dies nicht gefordert.[982] Erforderlich ist aber, dass der Gesetzgeber die Wirksamkeit seines „Kontrollmittels“ sicherstellt.[983]

---

977 *Backes/Gusy/Begemann/Doka/Finke*, Betrifft JUSTIZ, 2003, 14 (17).

978 Zwar befassen sich die Studien mit den richterlichen Anordnungen strafprozessualer Überwachungsmaßnahmen, für den präventiven Bereich sind sie jedoch ebenfalls von Bedeutung. Die Anwendung des FGG bei Exekutivanordnungen obliegt dem (Amts-) Richter, dem im Wege der richterlichen Geschäftsverteilung „Polizeisachen“ zugewiesen sind. Das kann ohnehin der (strafrechtliche) Ermittlungsrichter sein, vgl. *Lisken/Mokros*, NVwZ 1991, 609 (611). Weiter wird es kaum so sein, dass im präventiven Bereich eine andere Arbeitsweise zu verzeichnen ist, als im repressiven Bereich. Auch im Bereich der Gefahrenabwehr hat der Richter noch über weitere Maßnahmen, wie die Ingewahrsamnahme und die Wohnraumüberwachung zu entscheiden. Erschwerend kommt hinzu, dass die formalen Anforderungen an den richterlichen Beschluss nach den Polizeigesetzen hinter denen der StPO zurückbleiben. So wird in Niedersachsen und Rheinland-Pfalz nicht einmal gefordert, dass der Beschluss schriftlich zu ergehen hat und die Dauer der Telekommunikationsüberwachung angegeben werden muss.

979 Vgl. *Albrecht, Dorsch, Krupe*, 2003, S. 446. Im Rahmen der Studie befragte Ermittlungsrichter erklärten, dass sie sich für einen Überwachungsbeschluss zehn bis maximal dreißig Minuten Zeit nehmen könnten und ihre Überprüfungsprioritäten auf schwerwiegende Maßnahmen, etwa körperliche Eingriffe oder Haftbefehle, setzten, vgl. *Albrecht, Dorsch, Krupe*, 2003, S. 447. Bei Folgemaßnahmen und Verlängerungsanordnungen als fortwährende und länger andauernde Grundrechtseingriffe fand im Vergleich zu den Erstanordnungen keine inhaltlich tiefergehende Begründungstätigkeit statt, vgl. *Albrecht, Dorsch, Krupe*, 2003, S. 447 f.

980 Die bei *Albrecht, Dorsch, Krupe*, Kurzbericht, S. 37 f. aufgeworfene Frage, ob das Urteil des BVerfG in NJW 2001, 1121 ff. ein Festhalten an Richtervorbehalt und Ermittlungsrichtersystem vorgibt, ist für den Fall der (präventiven) Telekommunikationsüberwachung nicht von grundsätzlicher Bedeutung, da Art. 10 GG gerade keinen Richtervorbehalt kennt.

981 *Würtenberger/Heckmann*, 2005, Rn. 577 nennen z.B. Behördenleitervorbehalte, Unterrichtungspflichten gegenüber dem Betroffenen und eine Unterrichtung des Landtags.

982 Das BVerfGE 100, 313 (361) proklamiert in seinen Entscheidungen zur Zulässigkeit von Eingriffen des Verfassungsschutzes bzw. des BND in das Grundrecht des Art. 10 GG eine „Kontrolle durch unabhängige und an keine Weisungen gebundene staatliche Organe und Hilfsorgane“. Auch der SächsVerfGH LKV 1996, 273 (286) verlangt nur eine „besondere Ausgestaltung des Grundrechtsschutzes durch Verfahren“ und billigt dem Gesetzgeber dabei einen erheblichen Spielraum zu, fordert allerdings, dass die grundrecht-

Im internationalen Vergleich bestehen neben dem Richtervorbehalt kontradiktorische Verfahren unter Beiziehung eines Rechtsanwalts (Dänemark)[984] und Berichtspflichten von Kontrollkommissionen und Ombudsmännern (angloamerikanischer Bereich, Norwegen)[985]. Wird den Ermittlungsrichtern der Vorwurf gemacht, sie würden bei ihren Anordnungsbeschlüssen die Rechte der Betroffenen unzureichend wahren, da sie mehrheitlich die Anträge bzw. vorformulierten Beschlüsse der Staatsanwaltschaft übernehmen, so kann dem dadurch Rechnung getragen werden, dass der Betroffene im Anordnungsverfahren , z.B. durch die Einbindung des Datenschutzbeauftragten, eine Stimme erhält. Mag der Richter am besten dafür geeignet sein, die Rechte des Betroffenen im Einzelfall zu wahren[986], ändert dies nichts an der Tatsache, dass sich dem Ermittlungsrichter – verstärkt durch die meist einseitig durchgeführten Ermittlungen, die auf die Überführung des Betroffenen bzw. die Gefahrenabwehr abzielen – selten eine differenzierte Betrachtungsweise aus der Ermittlungsakte zeigt.[987] Dem Richter muss daher die Möglichkeit eröffnet werden, die bisherigen Ermittlungsergebnisse – ohne großen Mehraufwand – von beiden Seiten zu betrachten.

Für das Recht auf informationelle Selbstbestimmung hat das BVerfG dem Datenschutzbeauftragten – ohne dies als verfassungsmäßig geboten anzusehen – eine wichtige Rolle zugewiesen.[988] Eine generelle Informationspflicht der öffentlichen Stellen über Datenerhebungen an den Datenschutzbeauftragten ist im BDSG nicht verankert. Möglich wäre es, eine solche Mit-

---

lich geschützten Interessen des Betroffenen von „unabhängigen Dritten“ vor der Entscheidung über den Grundrechtseingriff zur Geltung gebracht werden können. Siehe auch MVVerfG LKV 2000, 345 (355).

983 Vgl. BVerfGE 100, 313 (361).

984 In Dänemark erfolgt die Anordnung der Überwachung der Telekommunikation durch den Richter nach Antragsstellung durch die Polizei. Dieser hat vor der Entscheidung dem Betroffenen von Amts wegen einen Rechtsanwalt zu bestellen, dem Gelegenheit dazu zu geben ist, zum Antrag der Polizei Stellung zu nehmen. Die Aufgabe des Anwalts besteht darin, die Interessen des Tatverdächtigen und anderer Betroffener zu vertreten und eine kontradiktorische Verhandlung zu ermöglichen, vgl. *Cornils/Greve*, in: Gropp/Huber (Hrsg.), S. 44 f.

985 Über die Anordnungen von Überwachungen der Telekommunikation sind in den U.S.A. von der Justizverwaltung jährlich Berichte anzufertigen, aus denen sich Anordnungen und Ablehnungen, Straftat, Art und Ort des Anschlusses sowie die Dauer der Überwachung ergibt. Ferner sind zu erfassen die Anzahl der abgehörten Gespräche, die Anzahl belastender Informationen, die Kosten der Überwachung sowie die Festnahmen und Verurteilungen, die sich aus Verfahren mit Anordnungen der Überwachung der Telekommunikation ergeben. In Norwegen ist einer Telefonüberwachungskommission die Aufgabe übertragen worden, die Praxis der Überwachung der Telekommunikation zu kontrollieren, vgl. *Albrecht, Dorsch, Krupe*, 2003, S. 95 zu den U.S.A. und S. 72 zu Norwegen.

986 Vgl. BVerfG NJW 2003, 1787 (1792).

987 Nach Ansicht der Staatsanwälte sind die Richter in der Ermittlungssache ohnehin nicht „drin“ und können sich aufgrund der umfänglichen Aktenlage auch nur ein oberflächliches Bild machen. Demgegenüber betonen die Richter, dass sie in ihren Entscheidungen nur zu prüfen hätten, ob die beantragte Ermittlungsmaßnahme gestattet werden könne, nicht aber, ob sie auch erfolgreich sei, vgl. *Backes/Gusy/Begemann/Doka/Finke*, Betrifft JUSTIZ 2003, 14 (17).

988 Vgl. BVerfGE 65, 1 (46; 60); *Di Fabio*, in: Maunz/Dürig, Art. 2 Abs. 1 GG, Rn. 184.

teilungspflicht auf Landesebene für die Telekommunikationsdatenerhebung einzuführen. Eine ausdrückliche Kompetenz des Bundes zu einer umfassenden Regelung der Querschnittsmaterie des Datenschutzes enthält das Grundgesetz nicht. Die Gesetzgebungskompetenz des Bundes ergibt sich im Rückgriff auf die dem Bund zustehenden Gesetzgebungskompetenzen für verschiedene Bereiche, die für den Datenschutz von Bedeutung sind. Sind allerdings die Länder für eine Gesetzesmaterie ausschließlich kompetent, so wirkt sich das auch auf das Datenschutzrecht aus.[989] Den Ländern ist es damit auf dem Gebiet des Polizeirechts unbenommen, dem Datenschutzbeauftragten eine über seine allgemeine Funktion hinausgehende Kompetenz zuzuweisen. Seine Stellung könnte derart gestärkt werden, dass er zeitgleich mit dem Anordnungsantrag zu unterrichten und vom Richter anzuhören ist. Der Datenschutzbeauftragte verfügt über die notwendige Unabhängigkeit und Ausbildung, da dieser die Befähigung zum Richteramt oder zum höheren (Verwaltungs-)Dienst haben muss[990] und in seiner Amtsausübung unabhängig und nur dem Gesetz unterworfen ist.[991] Die Stellungnahme des Datenschutzbeauftragten wäre vom Ermittlungsrichter bei seiner Entscheidung zu berücksichtigen. In diesem dann kontradiktorischen Verfahren könnten die Rechte des Betroffenen durch den Datenschutzbeauftragten wahrgenommen werden.

Dem kann entgegengehalten werden, dass dadurch Verzögerungen eintreten können, die mit einer effektiven Gefahrenabwehr nicht zu vereinbaren sind. Gelten kann dies jedoch ausschließlich in Notfällen, bei denen ein sofortiges Einschreiten unabdingbar ist, wie z.B. bei einer Selbstmordgefahr. In diesen Fällen wird aber Gefahr in Verzug gegeben sein, so dass die Polizei sofort tätig werden kann. In anderen Fällen ist abgesehen davon, dass grundrechtlicher Schutz nicht einem möglichst schnellen Verfahren geopfert werden darf, davon auszugehen, dass es durch die zeitlichen Verzögerungen nicht zu Behinderungen kommt. Die Telekommunikationsüberwachung zielt im präventiven Bereich darauf ab, kriminelle Strukturen zu durchdringen und Informationen über zukünftiges Verhalten und Gefahren zu erlangen. Die Telekommunikationsüberwachung ist nicht selbst die Gefahrenabwehrmaßnahme, sie soll diese vielmehr ermöglichen und vorbereiten. Durch die Hinzuziehung eines Datenschutzbeauftragten wird die Tätigkeit der Polizei nicht behindert.

---

989 Vgl. *Gola/Klug*, 2003, S. 8.
990 § 21 Abs. 1, Satz 1 NDSG.
991 § 36 Abs. 1 ThDSG; Art. 29 Abs. 2, Satz 1 BayDSG; § 23 Abs. 1 RhPfDSG; Art. 22 HDSG.

Alternativ kann an eine Überprüfungsmöglichkeit durch parlamentarische Kontrollausschüsse gedacht werden[992], wie sie für die Überwachung nach dem G-10-Gesetz vorgesehen ist und wie sie durch das Terrorismusbekämpfungsgesetz für die neuartigen Überwachungsbefugnisse der Nachrichtendienste installiert wurde.[993] Doch auch die Überwachungsbefugnisse der parlamentarischen Kontrollausschüsse bergen Schwierigkeiten: So können sie sich schon in Anbetracht der zahlreichen Möglichkeiten zur Selektion und Aufbereitung der ihnen unterbreiteten Informationen nur ein unzureichendes Bild von der gesamten Überwachungspraxis machen.[994] Darüber hinaus, ist es im speziellen Fall der präventiven Telekommunikationsüberwachung vor allem im Hinblick auf doppelfunktionale Maßnahmen rechtspolitisch sinnvoll, dieselben Verfahrenssicherungsmaßnahmen vorzusehen wie für den repressiven Bereich, um denselben (Verfahrens-)Grundrechtsstandard unabhängig von der Zweckrichtung der Maßnahme zu gewährleisten.

Erforderlich ist, dass die Länder nicht nur tradierte Sicherungsmechanismen übernehmen, sondern sich selbst Gedanken über einen effektiven Schutz durch Verfahren machen. Der thüringer Gesetzgeber schließt seine Ausführungen in der Gesetzesbegründung mit den Worten: „...weil die Zuständigkeiten in der StPO ähnlich geregelt sind“[995]. Auch der niedersächsische Landtag hat ohne weitere Reflexion den Richtervorbehalt vorgesehen.[996] Der bayerische Gesetzgeber gibt in seiner Gesetzesbegründung ebenfalls an, dass sich die Regelung über das Verfahren zur Datenerhebung in Art. 34 c PAG an den entsprechenden Maßgaben der Strafprozessordnung orientiert.[997] Rheinland-Pfalz und Hessen haben den Richtervorbehalt ohne Begründung vorgesehen.

Obwohl es zu begrüßen ist, dass die Länder zur Verfahrenssicherung einen Richtervorbehalt eingeführt haben, sind sie nicht von einer Überprüfung entbunden, ob ihre Verfahrenssicherungsmaßnahmen auch geeignet sind, den Grundrechtsschutz der Betroffenen effektiv her-

---

992 Vgl. *Kutscha*, NVwZ 2003, 1296 (1299).

993 § 8 Abs. 8; § 9 Abs. 4 BVerfSchG; § 8 Abs. 3 a; § 3, Satz 2 BNDG; § 10 Abs. 3; § 5 MADG.

994 Vgl. *Kutscha*, NVwZ 2003, 1296 (1299); *Gusy*, NJW 1981, 1581 (1584).

995 Vgl. LT-Drucks. Th. 3/2128, S. 36.

996 Vgl. LT-Drucks. Nds. 15/240, S. 20. Dies ist umso erstaunlicher, als die SPD-Fraktion des niedersächsischen Landtags einen Beschlussentwurf des Landtags forderte, mit dem der Landtag die Landesregierung zu einer Bundesratsinitiative auffordern sollte, die auf Defizite in der repressiven Telekommunikationsüberwachung hinweisen sollte, vgl. LT-Drucks. Nds. 15/476.

997 Vgl. LT-Drucks. Bayern 15/2096, S. 61.

beizuführen. Hier hätte eine kritischere Betrachtungsweise erfolgen müssen, zumal die Studie der Universität Bielefeld schon im Jahr 2002 veröffentlicht wurde.

Haben sich jedoch die Landesgesetzgeber für den Richtervorbehalt als Verfahrenssicherungsmaßnahme entschieden, so haben sie auch seine Wirksamkeit sicherzustellen. Den Regelungen der Polizeigesetze ist nicht zu entnehmen, dass die Anordnung zwingend Grund und Unentbehrlichkeit der Maßnahme wiedergeben muss. In Niedersachsen und Rheinland-Pfalz ist nicht geregelt, dass die Anordnung schriftlich zu ergehen hat und eine Aussage über die Dauer der Maßnahme zu treffen ist. Auch der Abbruch der Maßnahme und die daraus resultierende Unterrichtung des Richters und des Telekommunikationsunternehmens ist außer im PAG[998] nicht festgehalten. Das PAG sieht auch als einziges der hier untersuchten Gesetze ausdrücklich eine Begründungspflicht vor. Insofern besteht bei allen Polizeigesetzen Nachbesserungsbedarf.

e) Befristung

Was die Befristung der Maßnahmen angeht, so haben sich die Gesetzgeber – bis auf den bayerischen – an der StPO orientiert und für die Anordnungsdauer eine Frist von drei Monaten vorgesehen. Schon am Anfang der Diskussion über die Einführung der präventiven Telefonüberwachung sind Stimmen laut geworden, die sich für eine kürzere Frist aussprachen.[999] Bayern ist bislang das einzige Bundesland, das eine differenzierte Befristung der Überwachungsmaßnahmen abgestuft nach der Schwere des Eingriffs eingeführt hat und zudem als Regelfrist maximal einen Monat vorsieht. Auch im Rahmen der repressiven Telefonüberwachung wird als Folge der Untersuchungen zur Wirksamkeit der Überwachung eine kürzere Befristung gefordert.[1000] Die Max-Planck-Studie kommt zu dem Ergebnis, dass sich die Anordnungsdauer der Telekommunikationsüberwachung zwar am gesetzlichen Maximum orientiert, die tatsächliche Ausführungsdauer dagegen nur in einem Viertel der untersuchten

---

998 Art. 34 c Abs. 3, Satz 6 PAG sieht die Benachrichtigung des Richters vor.

999 Vgl. *Nedden*, Landesbeauftragter für den Datenschutz in Niedersachsen, in seinen Thesen und Anmerkungen zur Änderung des Niedersächsischen Gefahrenabwehrgesetzes, http://www.lfd.niedersachsen.de/master/C2216997_N2216723_L20_D0_I560.html. Auch BT-Drucks. 16/5846, S. 11 sieht für § 100 b StPO eine Frist von nur noch 2 Monaten vor.

1000 Vgl. die Entschließung der 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26.09.2003 zu den Konsequenzen aus der Untersuchung des Max-Planck-Instituts über Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation, S. 4, veröffentlicht als Anlage 27 zu LT-Drucks. RhPf. 14/2627.

Fälle die Zweimonatsgrenze überschritt.[1001] Schon aufgrund dieser Erfahrungswerte ist ein Überdenken der Befristungsdauer im Hinblick auf die Verhältnismäßigkeit der Maßnahmen in den Polizeigesetzen Ländern Niedersachsen, Rheinland-Pfalz, Hessen und Thüringen angezeigt.

Eine § 100 b Abs. 4, Satz 1 StPO vergleichbare Regelung, nach der die Überwachung abzubrechen ist, wenn die Ziele erreicht sind oder nicht mehr erreicht werden können, ist in den Polizeigesetzen nicht (ausdrücklich) zu finden. Zwar mag sich diese Folge auch aus dem Verhältnismäßigkeitsgrundsatz oder anderweitigen Regelungen über die Datenerhebung und –verarbeitung ergeben[1002], gerade aber im Bereich der sensiblen Grundrechtseingriffe ist im Hinblick auf die Schwere des Eingriffs und das Bestimmtheitsgebot eine ausdrückliche Regelung erforderlich, dass die Maßnahme unverzüglich abzubrechen ist, wenn die Voraussetzungen nicht mehr vorliegen oder der Zweck der Maßnahme erreicht ist.[1003]

IV. Der Vergleich mit der sonstigen Rechtsordnung

Staatliche Telekommunikationsüberwachungsmaßnahmen sehen auch die Regelungen der §§ 100 a StPO, im G-10-Gesetz, in den Gesetzen der Nachrichtendienste und der §§ 23 a ff. ZfdG vor. Ermächtigungsgrundlagen für Standortbestimmungen waren bereits vor Einführung der präventive Telekommunikationsüberwachung in den Landespolizeigesetzen enthalten. Erforderlich im Hinblick auf die eingeführten Maßnahmen der präventiv-polizeilichen Telekommunikationsüberwachung ist, dass diese verschiedenen Teilrechtsgebiete keine einander widersprechenden Lösungen hervorbringen, sondern Widersprüche zwischen den einzelnen Teilrechtsordnungen im Hinblick auf die Wahrung der Einheit der Rechtsordnung vermieden werden.[1004]

Zu beachten ist dabei, dass im Anwendungsbereich des G-10-Gesetzes und der Nachrichtendienstgesetze das Instrumentarium der Telekommunikationsüberwachung den Verfassungs-

---

1001 Vgl. *Albrecht, Dorsch, Krupe*, 2003, S. 166 ff.; 170 f.

1002 § 34 a Abs. 3 Satz 2 iVm § 44 Abs. 3 ThPAG; §§ 38 Abs. 1 Satz 1, 39 a Nds.SOG, § 17 Abs. 2 Nr. 1 NDSG; Art. 34 c Abs. 3 Satz 6 PAG; §§ 31 Abs. 8, 33 Abs. 2, 39 Abs. 2 Nr. 1 POG; §§ 20 Abs. 3 Satz 1; 27 Abs. 2 Nr. 1 und Nr. 3, Abs. 3 Sätze 1 und 3 HSOG.

1003 Schon um Missverständnisse und Rechtsunsicherheit zu vermeiden, aber auch als Gewähr für den tatsächlichen Abbruch, sind der betroffene Telekommunikationsdiensteanbieter und der zuständige Richter zu informieren.

1004 Vgl. *Felix*, 1998, S. 142 f.

schutzbehörden des Bundes und der Länder, dem Militärischen Abschirmdienst und dem Bundesnachrichtendienst zu Staatsschutzzwecken zur Verfügung gestellt wird, während die Landespolizeigesetze den Polizeibehörden die Überwachungskompetenz zur Wahrung des Schutzauftrages gegenüber den Bürgern erteilen.[1005] Zu verfassungsrechtlich relevanten Widersprüchen kann es daher kaum kommen, da zum einen andere Behörden zuständigen sind und zum anderen mit den jeweiligen Überwachungsmaßnahmen unterschiedliche Zwecke verfolgt werden.[1006]

Anders verhält es sich dagegen mit den Regelungen der §§ 100 a ff. StPO und den Bestimmungen zur Standortfeststellung in den Polizeigesetzen. Zwar verfolgt die StPO Ziele der Strafverfolgung und nicht der Gefahrenabwehr, doch werden diese Aufgaben meist von denselben Behörden wahrgenommen, auch kann es bei Gemengelage zu Überschneidungen der beiden Aufgabenbereiche kommen. Was die Regelungen zur Standortbestimmung in den Polizeigesetzen angeht, so sind nicht nur dieselben Behörden zuständig, sondern es wird mit der Gefahrenabwehr auch der gleiche Zweck verfolgt.

Widersprüche zu den Regelungen der StPO oder den Standortbestimmungen wären daher schwerlich zu legitimieren.

1. Die Regelungen der StPO

Die Überwachung und Aufzeichnung der Telekommunikation, der Anspruch auf Auskunft über die Telekommunikationsdaten und der Einsatz des IMSI-Catchers sind in der StPO durch mehrere Vorschriften geregelt, die für die einzelnen Maßnahmen nicht nur unterschiedliche Voraussetzungen, sondern auch unterschiedliche Verfahrensanforderungen vorsehen.[1007]

1005 Das ZFdG dagegen konzentriert sich auf die Verhinderung von Straftaten nach dem AWG und die Gefahrenabwehr durch das Zollkriminalamt, wenn ohne Genehmigung oder Entscheidung nach der Verordnung (EG) Nr. 1334/2000 oder nach den §§ 5 c der 5 d der Außenwirtschaftsverordnung die Ausfuhr bestimmter Güter vorbereitet wird.

1006 Vgl. dazu in diesem Kapitel S. 113 ff.

1007 Die Regelungen der §§ 100 a ff. StPO sind durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007, BGBl. I, S. 3198, umfassend geändert worden.

a) Die Überwachung und Aufzeichnung der Telekommunikation nach § 100 a StPO

Die Überwachung und Aufzeichnung der Telekommunikation nach § 100 a StPO darf zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsorts angeordnet werden, wenn der Verdacht der Täterschaft oder Teilnahme an einer Katalogtat[1008] besteht und die Tat auch im Einzelfall schwer wiegt.

Um dem Verhältnismäßigkeitsgrundsatz Rechnung zu tragen, hat der Gesetzgeber die Telekommunikationsüberwachung zu repressiven Zwecken auf bestimmte, abschließend aufgeführte Katalogtaten[1009] beschränkt. Die Katalogtaten des § 100 a Abs. 2 StPO sind dabei nicht nur Verbrechen, sondern auch Vergehen. Sie schützen die unterschiedlichsten Rechtsgüter, wie den Bestand und die Sicherheit der Bundesrepublik, die sexuelle Selbstbestimmung, das Eigentum oder die freie Willensentschließung. Ebenso ist eine Überwachung der Telekommunikation möglich bei Geldwäschedelikten oder Straftaten nach dem Betäubungsmittelgesetz.

Der bezüglich dieser Straftaten erforderliche Verdacht muss durch bestimmte Tatsachen konkretisiert sein, Gerüchte oder Gerede reichen nicht aus.[1010] Es müssen Umstände vorliegen, die nach der Lebenserfahrung, auch der kriminalistischen Erfahrung, in erheblichem Maß darauf hindeuten, dass jemand als Täter oder Teilnehmer eine Katalogtat begangen hat.[1011]

Eine Maßnahme nach § 100 a StPO darf nur angeordnet werden, wenn sie unentbehrlich ist, nämlich, wenn die Erforschung des Sachverhalts oder die Ermittlung des Beschuldigten auf

---

1008 Katalogtaten sind die in § 100 a Abs. 2 StPO aufgeführten schweren Straftaten. Hierunter können nach der Gesetzesbegründung, vgl. BT-Drucks. 16/5846, S. 40, solche Straftaten verstanden werden, die eine Mindesthöchststrafe von fünf Jahren Freiheitsstrafe aufweisen, in Einzelfällen aufgrund der besonderen Bedeutung des geschützten Rechtsguts oder des besonderen öffentlichen Interesses an der Strafverfolgung aber auch eine geringere Freiheitsstrafe. Eine Höchststrafe von einem Jahr Freiheitsstrafe entspricht dem Begriff der schweren Straftat nicht mehr. Gesetzliche Strafmilderungen für minder schwere Fälle bleiben unter Hinweis auf BVerfGE 109, 279 (349) bei dieser Strafrahmenbetrachtung unberücksichtigt.

1009 Vgl. *Meyer-Goßner*, § 100 a StPO, Rn. 4.

1010 Vgl. *Nack*, in: KK, § 100 a StPO, Rn. 22; *Kühn*, NJW 1979, 617 (622); ausführlich zum Straftatverdacht *Fincke*, ZStW 95 (1983), 918 (919 ff.).

1011 Vgl. *Nack*, in: KK, § 100 a StPO, Rn. 22; *Meyer-Goßner*, § 100 a StPO, Rn. 6.

andere Weise aussichtslos oder wesentlich erschwert wäre. Die Telefonüberwachung muss im konkreten Fall zur Beweisführung geeignet sein.[1012]

Die Anordnung darf nur bestimmte Personen betreffen. In erster Linie ist das der Beschuldigte.[1013] Sie kann sich jedoch auch gegen Nachrichtenmittler richten, also gegen Personen, von denen aufgrund bestimmter Tatsachen anzunehmen ist, dass sie Nachrichten, die an den Beschuldigten gerichtet oder von ihm unmittelbar oder mittelbar ausgegangen sind, entgegennehmen oder weiterleiten. Ferner ist die Überwachung von Personen zulässig, deren Anschluss der Beschuldigte benutzt, auch wenn sie hiervon keine Kenntnis haben.[1014]

Die Überwachung der Telekommunikation darf nur durch den Richter angeordnet werden.[1015] Bei Gefahr in Verzug kann die Anordnung auch von der Staatsanwaltschaft getroffen werden.[1016]

b) Die Erhebung von Verkehrsdaten nach § 100 g StPO

Nach § 100 g StPO dürfen Verkehrsdaten im Sinne der §§ 96 und 113 a TKG erhoben werden.[1017] Die Erhebung muss zur Untersuchung einer der in § 100 g Abs. 1 Satz 1 Nr. 1 StPO

1012 Dies ist dann nicht der Fall, wenn ausgeschlossen werden kann, dass der Betroffene Telefongespräche führt, die Bezug zu der Straftat haben, vgl. *Nack*, in: KK, § 100 a StPO, Rn. 23.

1013 Verwertet werden darf aber nicht nur der Inhalt von Gesprächen dieser Person, sondern auch der von Gesprächen, die unbeteiligte Leute über deren Anschluss führen, vgl. *Meyer-Goßner*, § 100 a StPO, Rn. 8; BGHSt 29, 23 (24 f.); aM *Prittwitz*, StV 1984, 302 (308 ff.); *Welp*, Jura 1981, 472 (481 ff.).

1014 Durch die Telekommunikationsüberwachung erlangte Zufallserkenntnisse dürfen nur dann gegen den Beschuldigten, Nachrichtenmittler und Dritte verwendet werden, wenn sie sich auf eine Katalogtat beziehen, BGHSt 28, 122 (129); 32, 10 (15); *Pfeiffer*, § 100 a StPO, Rn. 10. Etwas anderes gilt für die Verwertung von Zufallserkenntnissen bei ordnungsgemäß angeordneter Überwachung im Hinblick auf Nichtkatalogtaten nur dann, wenn ein enger Bezug zu der in der Anordnung aufgeführten Katalogtat besteht, vgl. BGH NStZ, 1998, 426 (427). Beziehen sich die Zufallserkenntnisse auf Nichtkatalogtaten ist lediglich eine mittelbare Verwertung in der Weise zulässig, dass die Zufallserkenntnisse zur Grundlage weiterer Ermittlungen gemacht werden, vgl. *Meyer-Goßner*, StPO, § 100 a, Rn. 19 und 20.

1015 Inhaltlich muss die schriftliche Anordnung außer den Namen und die Anschrift des Betroffenen, gegen den sie sich richtet, auch die Rufnummer oder eine andere Kennung seines Telekommunikationsanschlusses und die dem Beschuldigten zur Last gelegte Straftat, den Grund der Überwachung (Erforschung des Sachverhalts oder Aufenthaltsermittlung) und ihre Unentbehrlichkeit darlegen. Die Dauer der Maßnahmen ist auch dann zu bestimmen, wenn die Höchstdauer von drei Monaten nach § 100 b Abs. 2, Satz 4 StPO festgesetzt wird, vgl. *Meyer-Goßner*, StPO, § 100 b, Rn. 3; *Schäfer*, in: Löwe-Rosenberg, § 100 b StPO, Rn. 9. Die Frist kann jeweils um drei Monate verlängert werden, § 100 b Abs. 2, Satz 5 StPO. Bei der Fernsprechüberwachung ist außer der Bezeichnung der Rufnummer oder der Kennung des Telekommunikationsanschlusses anzugeben, ob und in welchem Umfang die Gespräche aufzuzeichnen, welche von mehreren Anschlüssen zu überwachen sind und ob das durchgehend oder nur zu bestimmten Tageszeiten geschehen soll, vgl. *Meyer-Goßner*, § 100 b StPO, Rn. 3.

1016 Die Anordnung der Staatsanwaltschaft tritt außer Kraft, wenn sie nicht binnen drei Tagen von dem Richter bestätigt wird, § 100 b Abs. 1 StPO.

bezeichneten Straftaten erforderlich sein. Dies sind zum einen Straftaten von erheblicher Bedeutung, insbesondere Katalogtaten nach § 100 a Abs. 2 StPO.[1018] Die Datenerhebung ist darüber hinaus auch bei Straftaten gestattet, die mittels Telekommunikation begangen wurden. Dazu gehören insbesondere telefonische Bedrohungen aus dem Stalking-Bereich.[1019] Die Telekommunikationsauskunft ist nur bei dem in § 100 a StPO genannten Personenkreis, also bei Beschuldigten und bei Nachrichtenmittlern, zulässig.[1020]

c) Der Einsatz des IMSI-Catchers nach § 100 i StPO[1021]

Der Einsatz des IMSI-Catchers hat nach § 100 i Abs. 1 StPO eine zweifache Zweckbestimmung[1022]: die Ermittlung der IMSI und der IMEI sowie die Aufenthaltsfeststellung des Mobilfunkteilnehmers.

1017 Nach § 100 g StPO a.F. konnte nur Auskunft über die in § 100 g Abs. 3 StPO abschließend aufgezählten Kommunikationsdaten verlangt werden. Mit der Ausgestaltung des § 100 g Abs. 1 Satz 1 StPO als umfassende Befugnis zur Erhebung von Verkehrsdaten entfällt die bislang ausdrücklich in § 100 g Abs. 1 StPO a.F. enthaltene Auskunftsverpflichtung der Diensteanbieter aber nicht. Deren Pflicht zur Mitwirkung an einer Ausleitung der Verkehrsdaten in Echtzeit oder zur Auskunftserteilung über gespeicherte Verkehrsdaten folgt vielmehr aus dem Verweis in § 100 g Abs. 2 Satz 1 auf § 100 b Abs. 3 StPO. Hiernach kann über gespeicherte Verkehrsdaten, die Telekommunikationsvorgänge aus der Vergangenheit betreffen, (im Rahmen des Erforderlichen) unbeschränkt Auskunft verlangt werden. Auch kann hiernach weiterhin Auskunft über zukünftig anfallende Verkehrsdaten verlangt werden; insoweit sind allerdings die nach § 100 g Abs. 2 Satz 1 i. V. m. § 100 b Abs. 1 StPO geltenden Anordnungsfristen zu beachten. Für zukünftig anfallende Verkehrsdaten sieht die Regelung daher zwei Möglichkeiten der Erhebung durch die Strafverfolgungsbehörden vor: Zum einen ist es zulässig, diese Daten in Echtzeit zu erheben, d. h. „live“ vom Telekommunikationsdienstleister an die Strafverfolgungsbehörden ausleiten zu lassen; zum anderen kann die Erhebung auch weiterhin in der Weise erfolgen, dass die nach dem Zeitpunkt der Anordnung anfallenden Verkehrsdaten in bestimmten Zeitabständen gebündelt an die Strafverfolgungsbehörde beauskunftet werden, so BT-Drucks. 16/5846, S. 50 f. Die in § 100 g Abs. 2 StPO a.F. enthaltene Ermächtigung zur Zielwahlsuche ist in § 100 g StPO n.F.. nicht mehr enthalten. Zu den Gründen vgl. BT-Drucks. 16/5846, S. 54.

1018 Bagatelldelikte scheiden jedenfalls aus; die Straftat muss mindestens dem mittleren Kriminalitätsbereich zuzurechnen sein, den Rechtsfrieden empfindlich stören und geeignet sein, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen, vgl. *Hilger*, NStZ 1992, (457) 462 dort Fn. 93 zu § 100 c Abs. 1 Nr. 1 b StPO; *Benfer*, MDR 1994, 12 zu § 110 a Abs. 1 StPO; *Möhrenschlager*, wistra 92, 326 (327) zu § 98 a Abs. 1 StPO.

1019 Vgl. BT-Drucks. 16/5846, S. 52.

1020 Bei „Hacker-Angriffen“ unter Ausnutzung von Computernetzwerken sind die Betreiber von dazu missbrauchten, zwischengeschalteten Computernetzwerken Nachrichtenmittler; vgl. BT-Drucks. 14/7008, S. 7.

1021 Der Einsatz des IMSI-Catchers wurde auf Empfehlung des Rechtsausschusses in den Entwurf des Gesetzes zur Änderung der StPO, vgl. BT-Drucks. 14/9088, S. 4 f., 7, aufgenommen und mit Gesetz zur Änderung der Strafprozessordnung vom 06.08.2002, BGBl. I, S. 3018, in die StPO eingefügt. Siehe zur „Einführung“ des IMSI-Catchers in die StPO *Hilger*, GA 2002, S. 557 ff.

1022 Ausführlich dazu das Kapitel „Der Zugriff auf die Telekommunikationsdaten“ unter V.

Für den Einsatz des IMSI-Catchers nach § 100 i Abs. 1 Nr. 1 StPO müssen die Voraussetzungen des § 100 a StPO vorliegen und sein Einsatz muss für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsorts des Beschuldigten erforderlich sein.

Durch den Verweis auf § 100 a Abs. 3 StPO wird der Einsatz des IMSI-Catchers auch gegen Kontaktpersonen des Täters zugelassen.[1023]

d) Unterschiede in den Polizeigesetzen

Die Polizeigesetze der Länder Thüringen, Niedersachsen und Bayern sehen die Überwachung der Telekommunikation bei Delikten vor, die im Katalog des § 100 a StPO enthalten sind.[1024] Das ThPAG übernimmt ihn sogar ganz.

Der Unterschied besteht jedoch darin, dass die Polizeigesetze keine unterschiedlichen Voraussetzungen für die Inhaltsüberwachung und die Erhebung von Verkehrsdaten vorsehen. Lediglich für den Einsatz des IMSI-Catchers werden höhere Voraussetzungen verlangt. Damit stellen sich die polizeigesetzlichen Regelungen aber nicht in Widerspruch zur sonstigen Rechtsordnung, sondern der Landesgesetzgeber hat lediglich von seinem gesetzgeberischen Gestaltungsrecht Gebrauch gemacht.[1025]

Dass die Landespolizeigesetze im Gegensatz zur StPO keine eindeutigen Regelungen zur Frage des Überwachungssubjekts beinhalten oder keine Vorgaben zu den Anforderungen an den richterlichen Anordnungsbeschluss machen, ist kein Aspekt der Widerspruchsfreiheit der

---

1023 Gestrichen wurde die Regelung des § 100 i Abs. 2 Satz 3 StPO, wonach die Standortbestimmung u.a. auch zur Eigensicherung der eingesetzten Beamten des Polizeidienstes möglich war. Ob diese Befugnis in der StPO geregelt werden musste, war ohnehin fraglich, da der Präventionszweck überwiegt. Es waren auch Fallgestaltungen vorstellbar, bei denen zwar keine Straftat von erheblicher Bedeutung vorlag, hingegen eine Lebensgefahr für die Festnahmebeamten bestand, so jedenfalls *Nack*, in: KK, § 100 i StPO, Rn. 8.

1024 § 34 a Abs. 1 Nr.1 ThPAG; §§ 33 a Abs. 1 Nr. 2; 2 Nr.10 Nds.SOG 2005; Art. 34 a Abs. 1 Nr. 2 a; 30 Abs. 5 PAG.

1025 Bundes- und Landesgesetzgeber haben hier nicht dieselbe Rechtsfrage abweichend von einander geregelt, was zur Anwendung von Art. 31 GG führen würde. Vielmehr haben Bund und Länder – jeweils im Rahmen ihrer Zuständigkeiten – ein identisches Verhalten oder einen identischen Sachverhalt unter verschiedenen Gesichtspunkten geregelt. Auch wenn der Wortlaut des Grundgesetzes den Begriff der Einheit der Rechtsordnung nicht kennt, begründet die Verfassung doch zumindest insoweit eine einheitliche Rechtsordnung, als alle Rechtsnormen der Gesamtrechtsordnung ihrerseits mit dem Grundgesetz vereinbar sein müssen, vgl. *Felix*, 1998, S. 177. Der jeweilige Gesetzgeber muss die verfassungsrechtlichen Vorgaben bei der Schaffung jeder einzelnen Norm der Gesamtrechtsordnung beachten. Die in Art. 1 Abs. 3 und 20 Abs. 3 GG enthaltene Bindung des Gesetzgebers bewirkt damit – in gewissem Umfang – auch die Widerspruchslosigkeit der Gesamtrechtsordnung, vgl. *Felix*, 1998, S. 178 und 187.

Rechtsordnung, sondern eine Frage der Vereinbarkeit der Regelungen mit den verfassungsrechtlichen Vorgaben zur Einschränkung von Art. 10 GG.[1026]

2. Die Observation und die Aufenthaltsbestimmung nach den Polizeigesetzen

Durch den Einsatz des IMSI-Catchers ist es den Ländern Niedersachsen, Rheinland-Pfalz, Hessen und Bayern möglich, den Standort des Anschlussinhabers bzw. Handybesitzers zu ermitteln; in Thüringen durch die Auskunft über Standortdaten nur zellgenau. Durch eine Funkzellenabfrage beim Telekommunikationsdiensteanbieter kann die Polizei in allen der fünf Bundesländer die Bewegungsabläufe der überwachten Personen nachvollziehen. Vergleichbar sind diese Möglichkeiten mit der polizeilichen Observation oder dem Einsatz technischer Mittel zur Aufenthaltsbestimmung.

a) § 34 Abs. 1, Abs. 2 ThPAG

Nach § 34 Abs. 1 und 2 ThPAG ist die längerfristige Observation[1027] (Nr. 1) und der verdeckte Einsatz technischer Mittel zur Ermittlung des Aufenthaltsorts einer Person (Nr. 2) zulässig, wenn sie zur Erfüllung einer polizeilichen Aufgabe erforderlich sind und eine dafür wesentliche Aufklärung auf andere Weise erheblich erschwert oder entscheidend verzögert würde und die Maßnahme nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts steht.[1028]

Der Einsatz ist zulässig gegen die für eine Gefahr Verantwortlichen und Nichtstörer, wenn dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes, für Leben, Gesundheit oder Freiheit einer Person oder für Sachen oder Tiere, deren Erhaltung im öffentlichen Interesse geboten erscheint, erforderlich ist sowie bei Personen,

---

1026 Vgl. dazu schon die Erörterungen in diesem Kapitel unter III.

1027 Nach der Legaldefinition in § 34 Abs. 1 Nr. 1 ThPAG ist die längerfristige Observation die planmäßig angelegte Beobachtung einer Person, die durchgehend länger als 24 Stunden oder an mehr als zwei Tagen durchgeführt werden soll.

1028 Der verdeckte Einsatz technischer Mittel zur Ermittlung des Aufenthaltsortes einer Person wurde durch das Thüringer Gesetz zur Änderung des Polizei- und Sicherheitsrechts vom 20.06.2002, Thür. GVBl. S. 247 eingeführt. Damit wird der Einsatz satellitengestützter Navigationssysteme (GPS) oder auch herkömmlicher Peilsender bei Observationseinsätzen rechtlich abgesichert, vgl. *Ebert/Honnacker/Seel*, § 34 ThPAG, Rn. 6. Nach der Gesetzesbegründung ist denkbares Einsatzfeld vor allem die Präparation von Fluchtfahrzeugen bei Geiselnahmen mit Ortungstechnik. Damit soll die mit einer klassischen Observation durch Nachfahren verbundene Gefährdung für die Geiseln vermieden werden, vgl. LT-Drucks. Th. 3/2128, S. 29.

bei denen Tatsachen die Annahme rechtfertigen, dass sie eine Straftat von erheblicher Bedeutung[1029] begehen wollen und deren Kontakt- und Begleitpersonen[1030].

b) §§ 34; 35 Nds.SOG

Die Datenerhebung durch eine längerfristige Observation ist in § 34 Abs. 1 Nds.SOG geregelt. Unter den gleichen Voraussetzungen kann die Polizei durch den verdeckten Einsatz technischer Mittel Bildaufnahmen und –aufzeichnungen anfertigen, das nicht öffentlich gesprochene Wort abhören oder aufzeichnen sowie den jeweiligen Aufenthaltsort einer Person bestimmen.[1031] Technische Mittel sind dabei z.B. Fotoapparate, Videokameras, Peilsender und Richtmikrophone.[1032] Der Einsatz ist zulässig zur:

- Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer der in den §§ 6 und 7 Nds.SOG genannten Personen, wenn die Aufklärung des Sachverhalts auf andere Weise nicht möglich erscheint (§ 34 Abs. 1, Satz 1 Nr.1 a) Nds.SOG),
- Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer der in § 8 Nds.SOG genannten Person, wenn dies für die Aufklärung des Sachverhalts unerlässlich ist und die weiteren Voraussetzungen des § 8 Nds.SOG vorliegen (§ 34 Abs. 1, Satz 1 Nr. 1 b) Nds.SOG),
- Beobachtung von Personen, bei denen Tatsachen die Annahme rechtfertigen, dass sie Straftaten von erheblicher Bedeutung begehen werden und wenn die Verhütung dieser Straftaten auf andere Weise nicht möglich erscheint (§ 34 Abs. 1, Satz 1 Nr. 2 Nds.SOG) sowie
- Beobachtung von Kontakt- und Begleitpersonen der in Nr. 2 genannten Personen, wenn dies zur Verhütung einer Straftat nach Nr. 2 unerlässlich ist (§ 34 Abs. 1, Satz 1 Nr. 3 Nds.SOG).[1033]

1029 § 31 Abs. 5 ThPAG umschreibt den Begriff der „Straftaten von erheblicher Bedeutung“. In dieser nicht abschließenden Aufzählung von Straftaten sind alle Verbrechen, die in § 138 Abs. 1 und 2 StGB und in § 129 StGB genannten Vergehen und gewerbs- und bandenmäßig begangene Vergehen nach einem Beispielkatalog aufgeführt.

1030 § 34 Abs. 3 ThPAG.

1031 § 35 Abs. 1 Nds.SOG.

1032 Vgl. *Unger/Siefken,* in: Böhrenz/Unger/Siefken, § 35 Nds.SOG, AB 35.1.

1033 Das Nds.SOG 2005 sah noch in § 35 Abs. 1 Satz 1 Nr. 2 und 3 die Maßnahmen auch für die Fälle vor, dass die Vorsorge für die Verfolgung von Straftaten auf andere Weise nicht möglich erschien oder unerlässlich war.

c) Art. 33 Abs. 1 Nr. 1 und Nr. 2, Abs. 3 PAG

§ 33 Abs. 1 Nr. 1 PAG regelt die längerfristige Observation, in Nr. 2 a – c ist der verdeckte Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen oder –aufzeichnungen, zur Feststellung des Standorts oder der Bewegungen einer Person oder einer beweglichen Sache und zum Abhören oder zur Aufzeichnung des nichtöffentlich gesprochenen Wortes vorgesehen.

Die längerfristige Observation ist nach Art. 33 Abs. 2, Satz 1 PAG nur zulässig, wenn die Erfüllung einer polizeilichen Aufgabe auf andere Weise gefährdet oder erheblich erschwert würde. Auf Grund des GPS-Urteils des BVerfG[1034] wurde der Einsatz von technischen Mitteln zur Bestimmung des Aufenthaltsortes bzw. der Bewegungen von Personen oder beweglichen Sachen in Art. 33 Abs. 1 Nr. 2 b) PAG ausdrücklich aufgenommen. Technische Mittel im Sinne dieser Regelung sind nach der Gesetzesbegründung Peilsender und GPS-Empfänger.[1035] Der Einsatz technischer Mittel zur Bestimmung des Aufenthaltsortes ist zur Abwehr von Straftaten von erheblicher Bedeutung zulässig sowie zur Gefahrenabwehr hinsichtlich der in Art. 33 Abs. 3 Nr. 1 PAG genannten Rechtsgüter. Der Einsatz kann sich gegen Störer, Nichtstörer, potenzielle Straftäter und Kontakt- und Begleitpersonen richten.

d) § 28 Abs. 1, Abs. 2 Nr. 1 und 5 POG

Durch eine längerfristige Observation nach § 28 Abs. 1 und 2 Nr. 1 POG kann die Polizei personenbezogene Daten erheben über die Verantwortlichen nach den §§ 4; 5 POG und unter den Voraussetzungen des § 7 POG über die dort genannte Personen, soweit die Datenerhebung zur Abwehr einer Gefahr für Leib oder Leben erforderlich ist sowie über Personen, bei denen durch Tatsachen begründete Anhaltspunkte die Annahme rechtfertigen, dass sie zukünftig Straftaten von erheblicher Bedeutung begehen, weiter über Kontakt- und Begleitpersonen und Personen im Umfeld einer in besonderem Maß als gefährdet erscheinenden Person. Unter den gleichen Voraussetzungen ist gemäß § 28 Abs. 1 und 2 Nr. 5 POG die Stand-

---

1034 Vgl. BVerfG NJW 2005, 1338 ff. Gegenstand des Urteils war, ob § 100 c Abs. 1 Nr. 1 b) StPO als Ermächtigungsgrundlage für Beweiserhebungen unter Einsatz des Global Positioning Systems und die anschließende Verwertung dieser Beweise den verfassungsrechtlichen Anforderungen entspricht. Das BVerfG hat in diesem Urteil dargelegt, dass technische Eingriffsinstrumente gesetzlich so genau zu bezeichnen sind, dass der Normadressat den Inhalt erkennen kann, vgl. BVerfG NJW 2005, 1338 (1340).

1035 Vgl. LT-Drucks. Bayern 15/4097, S. 3.

ortfeststellung einer Person oder eines Fahrzeugs erlaubt. Damit ist eine spezielle Befugnis für die Verwendung von GPS oder herkömmlicher Peilsender geschaffen.[1036]

e) § 15 Abs. 1 Nr. 1; Abs. 2 HSOG

Das HSOG lässt eine längerfristige Observation zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person zu, weiter über Personen, wenn tatsächliche Anhaltspunkte bestehen, dass sie eine Straftat mit erheblicher Bedeutung begehen werden sowie über Kontakt- und Begleitpersonen und so genannte Risikopersonen[1037]. Eine spezielle Regelung zur Aufenthaltsbestimmung mit technischen Mitteln ist nicht vorgesehen.

f) Vergleich mit den Regelungen zur Telekommunikationsüberwachung

Die Polizeigesetze sehen für den Einsatz des IMSI-Catchers strengere Voraussetzungen als für eine Observation oder Aufenthaltsermittlung vor und lassen damit keinen Widerspruch zu Rechtsordnung erkennen.[1038] Lediglich das ThPAG, das einen IMSI-Catcher – Einsatz nicht vorsieht, stellt höhere Anforderungen an Observations- und Aufenthaltsermittlungsmaßnahmen als an eine Funkzellenabfrage, da es zur Straftatenverhinderung durch Aufenthaltsermittlung und Observation auf seinen „eigenen“ Straftatenkatalog zurückgreift, welcher enger gefasst ist als der des § 100 a StPO, welcher für die Funkzellenabfrage einschlägig ist. Ein Widerspruch zur sonstigen Rechtsordnung ist damit aber nicht begründet, da durch die Funkzellenabfrage lediglich eine ungefähre Standortbestimmung durchgeführt werden kann, während die Überwachung mittels GPS eine genaue Peilung ermöglicht.[1039]

1036 Vgl. *Roos*, § 28 POG, Rn. 10.

1037 Mit Risikopersonen sind die in § 13 Abs. 2 Nr. 3 HSOG beschriebenen Personen gemeint, also solche, die sich im räumlichen Umfeld gefährdeter Personen aufhalten, vgl. *Meixner/Fredrich*, § 15 HSOG, Rn. 7.

1038 Der Einsatz des IMSI-Catchers mit der Möglichkeit der Erstellung von Bewegungsprofilen bedeutet einen schwereren Eingriff in Art. 2 Abs. 1 iVm 1 Abs. 1 GG als die bloße Observation. Hinzu kommt, dass mit dem Einsatz des IMSI-Catchers auch das Fernmeldegeheimnis betroffen wird.

1039 Vgl. das Kapitel „Der Zugriff auf die Telekommunikationsdaten“ unter V.

Kapitel 6: Datenverarbeitung

Das Datenschutzrecht[1040] ist insbesondere durch das Volkszählungsurteil des BVerfG[1041] geprägt worden. In diesem Urteil traf das BVerfG programmatische Aussagen, die den verfassungsrechtlichen Rahmen für den staatlichen Umgang mit personenbezogenen Daten grundsätzlich beschrieben.[1042] Es bestätigte das damals schon zehn Jahre in der wissenschaftlichen Diskussion erörterte Recht auf informationelle Selbstbestimmung[1043] als verfassungsrechtliche Grundlage des Datenschutzes und forderte für die unfreiwillige Erhebung und Verarbeitung personenbezogener Daten, „dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt“[1044]. Die Einschränkungen müssen außerdem den Grundsätzen des Verhältnismäßigkeitsprinzips entsprechen und ausreichende Sicherungen gegen Missbrauch der Daten bieten.[1045]

Die allgemeinen Datenschutzgesetze können den verfassungsrechtlichen Vorgaben, wonach dem Bürger normenklar aufzuzeigen ist, wann er welche Datenverarbeitungen für welche Zwecke zu akzeptieren hat, nur bedingt gerecht werden. Zwangsläufig müssen sie ihre Erlaubnistatbestände an unbestimmten Rechtsbegriffen und offenen Abwägungsklauseln festmachen.[1046] Um dem Bürger in den besonders sensiblen Bereichen der Datenverarbeitung einen angemessenen Schutz zu gewähren, bedarf es spezieller Datenschutzregelungen. Insoweit kommt dem BDSG und den allgemeinen Datenschutzgesetzen der Länder nur eine Auffangfunktion zu, die darin besteht, den Datenschutz dort sicherzustellen, wo keine speziellen Schutzbestimmungen greifen.[1047]

Aufgrund des Volkszählungsurteils und des dort durch das BVerfG anerkannten, in Art. 2 Abs. 1 GG iVm Art. 1 Abs.1 GG verankerten, Grundrechts auf informationelle Selbstbestimmung enthalten die neueren Polizei- und Ordnungsgesetze umfassende Regelungen der

---

1040 Einen guten Überblick über die Entwicklung des Datenschutzrechts geben *Gola/Schomerus*, Einleitung, Rn. 1 ff.
1041 BVerfGE 65, 1 ff.
1042 Vgl. *Roßnagel*, in: Roßnagel (Hrsg.), Einleitung, Rn. 20.
1043 Vgl. *Roßnagel*, in: Roßnagel (Hrsg.), Einleitung, Rn. 20; *Podlech*, DVR 1976, 23 (25 ff.); *ders.* in: Dierstein/Fiedler/Schulz (Hrsg.), S. 311 (316 f.); *Benda*, in: FS für Geiger, S. 23 (31 ff.); *Mallmann*, 1976, S. 47 ff.
1044 BVerfGE 65, 1 (46).
1045 Vgl. *Roßnagel*, in: Roßnagel (Hrsg.), Einleitung, Rn. 20.
1046 Vgl. *Gola/Klug*, 2003, S. 8.
1047 Vgl. *Gola/Klug*, 2003, S. 9.

polizeilichen Informationsgewinnung und –verarbeitung (Datenverarbeitung)[1048] und tragen somit der Forderung des BVerfG[1049] nach bereichsspezifischen Datenschutzregelungen Rechnung.[1050]

Doch nicht nur im Volkszählungsurteil, sondern auch im BND-Urteil[1051] hat das BVerfG Voraussetzungen für eine verfassungskonforme Verarbeitung von Daten aufgestellt, die aus Eingriffen in das Fernmeldegeheimnis stammen. Durch seine Entscheidungen zum Großen Lauschangriff[1052] und zur Überwachung nach dem AWG[1053] hat das BVerfG diese Voraussetzungen bestätigt und teilweise konkretisiert.

Gegenstand des BVerfG-Urteils zur Telekommunikationsüberwachung nach dem Nds.SOG 2005 waren zwar nicht die Regelungen über die Datenverarbeitung. Dennoch hat das BVerfG auch über diese im Zusammenhang mit der Vereinbarkeit des § 33 a Abs. 1 Nr. 2 und 3 Nds.SOG 2005 mit dem Grundgesetz Aussagen getroffen.[1054]

Auch der EGMR hat in dem Verfahren *Weber u. Savaria c. Deutschland* Anforderungen für die Verarbeitung von Telekommunikationsdaten im Einklang mit Art. 8 EMRK aufgezeigt.[1055]

Die neu eingeführten Regelungen zur Telekommunikationsüberwachung stehen, abgesehen von verfassungsgemäßen Eingriffsvoraussetzungen, daher nur in Einklang mit höherrangigem Recht, wenn sie die – auch durch höchstrichterliche Rechtsprechung ausgestaltete – verfassungsrechtlichen Vorgaben für die Datenverarbeitung einhalten.

1048 Vgl. *W.-R. Schenke*, 2007, Rn. 176 ff.; ausführlich *Würtenberger/Heckmann*, 2005, Rn. 536 ff.; siehe auch *Dix*, Jura 1993, 571 ff. und *Peitsch*, ZRP 1992, 127 ff.

1049 Vgl. BVerfGE 65, 1 (46); zur Kritik der Rechtsprechung siehe *W.-R. Schenke*, NJW 1987, 2777 ff.

1050 Vgl. *W.-R. Schenke*, 2007, Rn. 176 mit dem Verweis auf den Entwurf des Gesetzes zur Änderung des baden-württembergischen Polizeigesetzes vom 07.05.1991, LT-Drucks. BW 10/5230, S. 1 (30), der im Hinblick auf die Einfügung datenschutzrechtlicher Regelungen in das PolG BW ausdrücklich auf das Volkszählungsurteil Bezug genommen hat.

1051 BVerfGE 100, 313 ff. Das BND-Urteil wird auch als „Dritte Abhörentscheidung“ bezeichnet. Zur Terminologie und zur „Ersten Abhörentscheidung“ in BVerfGE 30, 1 ff. und „Zweiten Abhörentscheidung“ in BVerfGE 67, 157 ff. vgl. *Loewer*, in: v.Münch/Kunig (Hrsg.), Art. 10 GG Rn. 47, 50.

1052 BVerfGE 109, 279 ff.

1053 BVerfGE 110, 33 ff.

1054 Vgl. BVerfGE 113, 349 (382 ff.).

1055 Der Gerichtshof geht davon aus, dass die Verwendung der Telekommunikationsdaten durch andere Behörden, sowie die Vernichtung der Daten und eine unterlassene Mitteilung an den Betroffenen Eingriffe in Art. 8 EMRK darstellen, vgl. EGMR NJW 2007, 1433 (1434).

I. Die verfassungsrechtlichen Vorgaben

1. Das BND-Urteil

In seinem BND-Urteil hatte das BVerfG über die Verfassungsmäßigkeit der Verarbeitung personenbezogener Daten nach dem G-10-Gesetz zu entscheiden. Es hat Teile des G-10-Gesetzes in seiner Fassung, die es durch das Verbrechensbekämpfungsgesetz vom 28.10.1994[1056] erhalten hatte, für unvereinbar mit Art. 10 und Art. 19 Abs. 4 GG erklärt.[1057] Darauf hin hat der Gesetzgeber das G-10-Gesetz[1058] neu erlassen.

Das BVerfG hat die besonderen Anforderungen aufgezeigt, die sich an den Gesetzgeber aus Art. 10 GG für die Verarbeitung personenbezogener Daten stellen.[1059] Es hat deutlich gemacht, dass sich insoweit die Maßgaben, die das BVerfG im Volkszählungsurteil aus Art. 2 Abs. 1 GG iVm Art. 1 Abs. 1 GG entwickelt hat[1060], weitgehend auf die (speziellere) Garantie in Art. 10 GG übertragen lassen. Zu diesen verfassungsrechtlichen Anforderungen zählen:

- die Bindung der Daten an ihren Erhebungszweck (Zweckbindung)[1061],
- das Vorliegen einer gesetzlichen Grundlage für Zweckänderungen, die zudem durch Allgemeinbelange gerechtfertigt sein müssen[1062],
- die Kennzeichnung der Daten, die durch einen Eingriff in das Fernmeldegeheimnis erlangt wurden[1063],
- der Anspruch der Grundrechtsträger auf Kenntnis von Maßnahmen der Fernmeldeüberwachung, die sie betroffen haben, als ein Erfordernis effektiven Rechtsschutzes[1064],
- die Kontrolle durch unabhängige und an keine Weisung gebundene staatliche Hilfsorgane[1065],

---

1056 Gesetz zur Änderung des Strafgesetzbuches, der Strafprozessordnung und anderer Gesetze, BGBl. I, S. 3186.

1057 Gegenstand des Verfahrens war allein die strategische Überwachung des Fernmeldeverkehrs durch den BND. Vgl. hierzu die Urteilsanmerkung von *Sachs*, JuS 2000, 597.

1058 BGBl. I, 2001, S. 1254.

1059 Vgl. BVerfGE 100, 313 (354 ff.).

1060 Vgl. BVerfGE 65, 1 (44 ff.).

1061 Vgl. BVerfE 100, 313 (360).

1062 Vgl. BVerfGE 100, 313 (360); E 65, 1 (44 ff.); so auch EGMR NJW 2007, 1433 (1435).

1063 Vgl. BVerfGE 100, 313 (360 f.); so auch EGMR NJW 2007, 1433 (1438).

1064 Vgl. BVerfGE 100, 313 (361); so auch EGMR NJW 2007, 1433 (1439 f.).

- die Vernichtung der Daten, sobald sie für den festgelegten Zweck oder den gerichtlichen Rechtsschutz nicht mehr erforderlich sind[1066] und
- die Dokumentation über die Übermittlung und Vernichtung der Daten, da ansonsten eine effektive Kontrolle nicht stattfinden kann.[1067]

2. Der AWG – Beschluss

In einem Normenkontrollverfahren hatte das BVerfG die §§ 39, 40 und 41 AWG[1068] auf ihre Vereinbarkeit mit dem Grundgesetz zu überprüfen.[1069] Der Überprüfung unterlagen die Befugnis des Zollkriminalamts, Sendungen, die dem Brief-, Post, oder Fernmeldegeheimnis unterliegen, zu öffnen und einzusehen sowie die Telekommunikation zu überwachen und aufzuzeichnen; die Überprüfung betraf außerdem die Befugnis öffentlicher Stellen, die dabei erlangten personenbezogenen Daten zu verarbeiten.[1070] Das BVerfG hat in seiner Entscheidung festgestellt, dass die §§ 39, 40 und 41 AWG mit Art. 10 GG unvereinbar sind. Es hat, da die zur Überprüfung gestellten Paragraphen gemäß § 51 AWG bis zum 31.12.2004 befristet waren, die damalige Rechtslage bis zum Ablauf der vorgesehenen Befristung als hinnehmbar angesehen.[1071] In Ansehung dieses Urteils wurde das Gesetz zur Neuregelung der präventiven Telekommunikations- und Postüberwachung durch das Zollkriminalamt und zur Änderung der Investitionszulagengesetze 2005 und 1999 erlassen.[1072] Durch dessen Art. 1 wurden die §§ 39 bis 43 und 51 AWG aufgehoben und durch Art. 2 in das Zollfahndungs-

---

1065 Vgl. schon BVerfGE 30, 1 (23 f.; 30 f.); BVerfGE 65, 1 (46); BVerfG 67, 157 (185). BVerfGE 100, 313 (364) führt hierzu aus: „Art. 19 Abs. 4 GG gewährt dem Bürger Anspruch auf eine wirksame gerichtliche Kontrolle in Fällen, in denen eine Verletzung seiner Rechte durch die öffentliche Gewalt möglich erscheint. Von dieser Garantie macht das Grundgesetz in Art. 10 Abs. 2, Satz 2 GG aber gerade eine Ausnahme. Diese bleibt nach Art. 19 Abs. 4, Satz 3 GG von der im Übrigen umfassenden Rechtsschutzgarantie unberührt. Allerdings werden die Eingriffe durch diese Vorschriften nicht gänzlich kontrollfrei gestellt. Vielmehr muss an die Stelle des Rechtswegs die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane treten."

1066 Vgl. BVerfGE 100, 313 (362); so auch EGMR NJW 2007, 1433 (1440).

1067 Vgl. BVerfGE 100, 313 (395 f.); siehe dazu *W-R. Schenke*, JZ 2001, 997 (1001); EGMR NJW 2007, 1433 (1439).

1068 §§ 39, 40 und 41 AWG lagen der Überprüfung in ihrer Fassung zugrunde, die sie durch die letzte Änderung durch das Zollfahndungsneuregelungsgesetz vom 16. 08 2002, BGBl. I, S. 3202, erfahren hatten.

1069 § 39 Abs. 1 AWG umschrieb als Aufgabe des Zollkriminalamts die Verhütung von Straftaten nach dem AWG und dem Kriegswaffenkontrollgesetz und erlaubt zu diesem Zweck die Überwachung des Brief- und Telekommunikationsverkehrs. Gemäß § 39 Abs. 2, Satz 1 Nr. 1 AWG sollte die Überwachungsmaßnahme zum Zeitpunkt des Planens einer Straftat erfolgen.

1070 Das Gesetz zur Änderung des Außenwirtschaftsgesetzes, des Strafgesetzbuches und anderer Gesetze vom 28.02.1992, BGBl. I, S. 372, hatte diese Befugnisse dem damaligen Zollkriminalinstitut eingeräumt.

1071 BVerfGE 110, 33 (76).

1072 Art. 2 des Gesetzes vom 21.12.2004, BGBl. I, S. 3603.

dienstgesetz[1073] der Abschnitt 3 mit den §§ 23 a – 23 f eingefügt, die die präventive Telekommunikations- und Postüberwachung regeln.

Das BVerfG hat u.a. § 41 Abs. 2 AWG an den Voraussetzungen gemessen, die an die Weitergabe und Verarbeitung von Daten zu stellen sind, die aus einem Eingriff in Art. 10 GG herrühren. Es hat festgestellt, dass die Vorschrift den Anforderungen, die das BVerfG in seinem BND-Urteil aufgestellt hat, nicht genügt und diese Anforderungen präzisiert.[1074]

Als Voraussetzungen an eine verfassungsgemäße Datenweitergabe hat es neben den Anforderungen des BND-Urteils insbesondere angesehen:

- den Bezug auf eine bestimmte (Daten-)Empfängerbehörde oder zumindest deren Aufgabenbereich[1075] und
- eine Differenzierung hinsichtlich der Weitergabe von Daten des Verdächtigen und Dritter.[1076]

3. Das Urteil zum Großen Lauschangriff

Mit Urteil vom 03.03.2004[1077] hat das BVerfG die Vereinbarkeit des Art. 13 Abs. 3 GG in der Fassung des Gesetzes zur Änderung des Grundgesetzes vom 26.03.1998[1078] als mit Art. 79 Abs.3 GG vereinbar angesehen. Die Vorschriften der Strafprozessordnung zur Durchführung der akustischen Überwachung von Wohnraum zu Zwecken der Strafverfolgung[1079], zu den Beweiserhebungs- und Beweisverwertungsverboten[1080], zur Benachrichtigungspflicht[1081], zur Verwendung personenbezogener Informationen in anderen Verfahren[1082] und zur Datenvernichtung[1083] genügen indes den verfassungsrechtlichen Anforderungen im Hinblick auf den Schutz der Menschenwürde, dem vom Rechtsstaatsprinzip umfassten Grund-

---

1073 Zollfahndungsdienstgesetz vom 16.08.2002, BGBl. I, S. 3202, zuletzt geändert durch Artikel 1 des Gesetzes vom 12. Juni 2007, BGBl. I, S. 1037.
1074 Vgl. BVerfGE 110, 33 (69 f.).
1075 Vgl. BVerfGE 110, 33 (70).
1076 Vgl. BVerfGE 110, 33 (75).
1077 BVerfGE 109, 279 ff..
1078 BGBl. I, S. 610.
1079 § 100 c Abs. 1 Nr. 3, Abs. 2 und Abs. 3 StPO a.F.
1080 § 100 d Abs. 3 StPO a.F.
1081 § 101 StPO a.F.
1082 §§ 100 d Abs. 5 Satz 2; 100 f Abs. 1 StPO a.F.
1083 §§ 100 d Abs. 4 Satz 3; 100 b Abs. 6 StPO a.F.

satz der Verhältnismäßigkeit, der Gewährung effektiven Rechtsschutzes und dem Anspruch auf rechtliches Gehör nicht in vollem Umfang.[1084] Das BVerfG hat dem Gesetzgeber die Pflicht auferlegt, soweit die angegriffenen Vorschriften der Strafprozessordnung unvereinbar mit dem Grundgesetz sind, einen verfassungsmäßigen Rechtszustand bis spätestens zum 30.06.2005 herzustellen.[1085]

Das BVerfG hat die Vorschriften der StPO, die die Verarbeitung der aus der Wohnraumüberwachung gewonnenen Daten regeln, an den Grundsätzen gemessen, die es im BND-Urteil aufgestellt hat.[1086] Darüber hinaus hat das BVerfG konkrete Aussagen darüber getroffen, wann die Regelungen über die Datenvernichtung dem Gebot des effektiven Rechtsschutzes genügen[1087] und unter welchen Voraussetzungen eine Datenweitergabe an Gefahrenabwehrbehörden erfolgen kann.[1088]

4. Das Urteil zum Nds.SOG 2005

Das BVerfG betont in diesem Urteil, dass durch die Zurückstellung oder das Unterbleiben der Unterrichtung über die Maßnahme, die Schwere des Grundrechtseingriffs zusätzlich erhöht werden kann.[1089] Dadurch ist auch ein effektiver Rechtsschutz des Betroffenen gefährdet.[1090]

Wie schon in seinem Urteil zum „Großen Lauschangriff“[1091] so führt das BVerfG auch in seiner Entscheidung zum Nds.SOG 2005 aus, dass Ermächtigungen zur Überwachung der

---

1084 Vgl. zur justizpolitischen Debatte *Denninger*, StV 1998, 401 ff.; *Kutscha/Möritz*, StV 1998, 564 ff.; *Momsen*, ZRP 1998, 459 ff.; *Stümper*, ZRP 1998, 463 ff.; *Schily*, ZRP 1999, 129 ff.; *Zwiehoff* (Hrsg.), 2000, S. 1 ff.

1085 Dem ist der Gesetzgeber durch die Neufassung der §§ 100 c- 100 f StPO durch Art. 1 des Gesetzes zur Umsetzung des Urteils des BVerfG vom 3. März 2004 (akustische Wohnraumüberwachungsgesetz vom 24.06.2005, BGBl. I, S. 1841, nachgekommen.

1086 Vgl. BVerfGE 109, 279 (375 ff.).

1087 Dass der Rechtsschutz durch eine Datenvernichtung nicht unterlaufen wird, kann in der Weise geschehen, dass die Daten einstweilen nicht gelöscht, wohl aber gesperrt und zu keinem anderen Zweck verwendet werden dürfen, als dem zur Information des Betroffenen und zur gerichtlichen Kontrolle, vgl. BVerfGE 109, 279 (380 f.).

1088 Dazu gehört die Rechtfertigung durch Allgemeinbelange, die grundrechtlich geschützte Interessen überwiegen. Der neue Verwendungszweck muss sich auf die Aufgaben und Befugnisse der Behörde beziehen, der die Daten übermittelt werden. Schließlich dürfen der alte und der neue Verwendungszweck nicht miteinander unvereinbar sein, vgl. BVerfGE 109, 279 (375 ff.).

1089 Vgl. BVerfGE 113, 349 (384 ff.).

1090 Vgl. BVerfGE 113, 349 (384).

1091 Nach BVerfGE 109, 279 (318 ff.) ist Art. 13 Abs. 3 GG dahingehend zu verstehen, dass seine gesetzliche Ausgestaltung die Erhebung von Informationen durch die akustische Wohnraumüberwachung dort aus-

Telekommunikation hinreichende Vorkehrungen dafür treffen müssen, dass Eingriffe in den absolut geschützten Kernbereich privater Lebensgestaltung unterbleiben.[1092]

Art. 10 Abs. 1 GG gewährleistet die freie Entfaltung der Persönlichkeit durch einen privaten, vor der Öffentlichkeit verborgenen Austausch von Kommunikation und schützt damit zugleich die Würde des Menschen.[1093] Zwar sind die Bürger zur höchstpersönlichen Kommunikation nicht in gleicher Weise auf Telekommunikation angewiesen wie auf eine Wohnung. Jedoch fordert die nach Art. 1 Abs. 1 GG stets garantierte Unantastbarkeit der Menschenwürde auch im Gewährleistungsbereich des Art. 10 Abs. 1 GG Vorkehrungen zum Schutz individueller Entfaltung im Kernbereich privater Lebensgestaltung.[1094]

Bei der Anordnung oder Durchführung der Kommunikationsüberwachung ist nicht sicher vorhersehbar, ob bzw. dass die Maßnahme Kommunikation aus dem Kernbereich privater Lebensgestaltung umfasst.[1095] Deshalb kann das Risiko nicht ausgeschlossen werden, dass durch Abhörmaßnahmen Kommunikation aus diesem absolut geschützten Bereich erfasst wird. Dieses Risiko ist nur dann verfassungsrechtlich hinnehmbar, wenn das gefährdete Rechtsgut, das Anlass für die Überwachung gab, von besonders hohem Rang ist oder ein unmittelbarer Bezug zur zukünftigen Begehung von Straftaten zu erwarten ist.[1096]

Es müssen dann allerdings gesetzliche Vorkehrungen geschaffen werden, die sichern, dass die betreffenden Gespräche nicht gespeichert und verwertet werden, sondern unverzüglich gelöscht werden.[1097] So sieht das PAG vor, dass die Datenerhebung und die Eingriffe in den Telekommunikationsbereich insoweit unzulässig ist, als erkennbar wird, dass in den Kernbe-

---

schließen muss, wo Ermittlungsmaßnahmen in den durch Art. 13 Abs. 1 iVm Art. 1 Abs. 1 und Art. 2 Abs. 1 GG geschützten unantastbaren Bereich der privaten Lebensgestaltung vordringen würden.

1092 Vgl. BVerfGE 113, 349 (390).

1093 Vgl. BVerfGE 113, 349 (391); E 110, 33 (53); E 67, 157 (171).

1094 Vgl. BVerfGE 113, 349 (391); *Würtenberger/Heckmann*, 2005, Rn. 625 d.

1095 Ob personenbezogene Kommunikation dem Kernbereich privater Lebensgestaltung zuzuordnen ist, hängt davon ab, in welcher Art und Intensität sie aus sich heraus die Sphäre anderer oder Belange der Gemeinschaft berührt, vgl. BVerfGE 113, 349 (391); E 109, 279 (314); E 80, 367 (374). Nicht zum Kernbereich gehören Kommunikationsinhalte, die in unmittelbarem Bezug zu konkreten strafbaren Handlungen stehen, wie etwa Angaben über die Planung bevorstehender oder Berichte über begangene Straftaten, vgl. BVerfGE 113, 349 (391); E 109, 279 (319); E 80, 367 (375).

1096 Vgl. BVerfGE 113, 349 (392); *Würtenberger/Heckmann*, 2005, Rn. 625 d.

1097 Vgl. BVerfGE 113, 349 (392); *Würtenberger/Heckmann*, 2005, Rn. 625 d. Siehe dazu die mit Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, BGBl. I 2007, S. 3198 eingeführte Regelung des § 100 a Abs. 4 StPO.

reich privater Lebensgestaltung eingegriffen wird.[1098] Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind und nicht verwendet werden dürfen, sind daher unverzüglich zu löschen.[1099]

5. Die Übertragbarkeit der bundesverfassungsgerichtlichen Rechtsprechung zur verfassungsgemäßen Datenverarbeitung auf die landesgesetzlichen Regelungen zur präventiven Telekommunikationsüberwachung[1100]

Die Rechtsprechung des BVerfG zum Nds.SOG 2005 hat auch Bedeutung für die Polizeigesetze anderer Bundesländer, soweit diese vergleichbare Regelungen erlassen haben. Ebenfalls ist die Rechtsprechung im BND-Urteil auf die präventiv-polizeiliche Telekommunikationsüberwachung zu übertragen. Zwar lag der Entscheidung des BVerfG zum G-10-Gesetz die strategische Überwachung[1101] zugrunde.[1102] Das BVerfG hat aber bei der Erstreckung der Schutzwirkung des Fernmeldegeheimnisses auf den Datenverarbeitungs- und Informationsprozess seine Ausführungen zu Art. 10 GG allgemein gehalten und keine Einschränkungen auf eine bestimmte Eingriffsform vorgenommen.[1103] Auch in seinem AWG-Beschluss stellt das BVerfG allgemein auf den durch Art. 10 GG vermittelten Schutz ab und überprüft dann, ob die Normen des AWG diesen genügen.[1104]

Anders verhält es sich bei der Entscheidung zum Großen Lauschangriff. Zum einen befasst sich das BVerfG in dieser Entscheidung mit Art. 13 GG, zum anderen stehen repressive und nicht präventive Maßnahmen im Vordergrund. Das BVerfG bezieht sich jedoch bei seinen Aussagen zur Datenverarbeitung eindeutig auf seine Ausführungen zu Art. 10 GG und über-

---

1098 Art. 34 a Abs. 1, Satz 4 PAG. Auch das Nds.SOG hält eine Inhaltsüberwachung für unzulässig, soweit im Einzelfall aufgrund tatsächlicher Anhaltspunkte davon auszugehen ist, dass die Maßnahme ausschließlich eine Kommunikation erfasst, die als höchstpersönlich dem Kernbereich privater Lebensgestaltung zuzurechnen ist, vgl. § 33 a Abs. 3, Satz 1 Nds.SOG.

1099 Art. 34 c Abs. 6, Satz 1 PAG. Im Nds.SOG ist geregelt, dass wenn sich während der Durchführung einer Maßnahme ergibt, dass tatsächliche Anhaltpunkte für eine Kernbereichskommunikation gegeben sind, die Maßnahme zu unterbrechen ist, vgl. § 33 a Abs. 3, Satz 2 Nds. SOG. Die erhobenen Daten dürfen nicht verarbeitet werden; entsprechende Aufzeichnungen sind unverzüglich zu löschen. Die Erhebung und Löschung der Kernbereichsdaten ist zu dokumentieren, vgl. § 33 a Abs. 3, Satz 3 iVm § 35 a Abs. 3, Sätze 2 und 3 Nds.SOG.

1100 Auf die Übertragbarkeit der Rechtsprechung des EGMR wird hier nicht weiter eingegangen, da sich diese im Einklang mit der Rechtsprechung des BVerfG hält, vgl. EGMR NJW 2007, 1433 (1434) und keine neuen Aussagen getroffen werden.

1101 § 3 G-10-Gesetz a.F.; § 5 G-10-Gesetz n.F.

1102 Die strategische Überwachung berührt wegen ihrer Verdachtslosigkeit und Streubreite das Fernmeldegeheimnis besonders nachhaltig, vgl. BVerfGE 100, 313 (392), während die Landespolizeigesetze eine Einzelfallüberwachung vorsehen.

1103 Vgl. BVerfGE 100, 313 (359 ff.).

1104 Vgl. BVerfGE 110, 33 (68 ff.).

trägt die im BND-Urteil aufgestellten Grundsätze auf die Verarbeitung von Daten, die durch einen Eingriff in Art. 13 GG erlangt worden sind.[1105] Nicht eindeutig lässt sich der Entscheidung entnehmen, ob die Aussagen des BVerfG auch auf präventive Maßnahmen und wenn ja, auf die präventive Telekommunikationsüberwachung zu übertragen sind. Doch hat sich das BVerfG vor allem bei der Frage der Datenweitergabe ausdrücklich auf die präventive Wohnraumüberwachung bezogen. Es hat festgestellt, „eine gesetzliche Regelung für die Übermittlung nach § 100 c Abs. 1 Nr. 3 StPO erhobener Daten an Behörden zu präventivpolizeilichen Zwecken hat daher die verfassungsrechtlichen Vorgaben zu berücksichtigen, die in Art. 13 Abs. 4 GG für den Primäreingriff getroffen worden sind“[1106] und gefordert, dass § 100 f Abs. 1 StPO im Hinblick auf Art. 13 Abs. 4 GG verfassungskonform auszulegen ist.[1107] Dies spricht dafür, dass auch die Rechtsprechung zum Großen Lauschangriff auf die präventive Telekommunikationsüberwachung übertragen werden kann.

In der Literatur ist umstritten, ob sich die Anforderungen des BVerfG auf präventiven Maßnahmen übertragen lassen.[1108] Nach Ansicht von *Haas* lassen sich den Ausführungen des Gerichts entnehmen, dass sie nur Geltung für repressive Strafverfolgungsmaßnahmen beanspruchen.[1109] Dagegen hat nach Meinung von *Hirsch* das BVerfG auch zur Nutzung des Lauschangriffs im polizeirechtlichen – also präventiven Bereich – eindeutige Hinweise gegeben, da es eine verfassungskonforme Auslegung des § 100 f Abs. 1 StPO im Lichte des Art. 13 Abs. 4 GG gefordert hat.[1110] Was das BVerfG für die Weitergabe legal erhobener Daten für präventive Zwecke vorschreibe, könne für die eigene Datenerhebung der Polizei nicht ohne Belang sein. Auch diese Tätigkeit sei nicht verfassungsfrei, sondern an die Wertungen der Landesverfassung und des Grundgesetzes gebunden. Bei den vielfältigen Berührungspunkten und den unablässigen Bestrebungen, Prävention und Repression zu vermengen, wäre es unerträglich, wenn es möglich und zugelassen werden würde, die verfassungsrechtlichen Grenzen der Lauschangriffe polizeirechtlich zu unterlaufen.[1111] Auch *Gusy* geht davon aus,

---

1105 Vgl. BVerfGE 109, 279 (379 ff.).

1106 BVerfGE 109, 279 (378).

1107 Vgl. BVerfGE 109, 279 (379).

1108 Dies allerdings vor dem Hintergrund, ob sich die Aussagen zum absolut geschützten Kernbereich auf präventiven Maßnahmen übertragen lassen, vgl. BVerfGE 109, 279 (314 ff.).

1109 Vgl. *Haas*, NJW 2004, 3082 (3084), allerdings ohne Begründung.

1110 Vgl. *B. Hirsch*, NJW 2004, XX.

1111 Vgl. *B. Hirsch*, NJW 2004, XX. Siehe dazu aber *Würtenberger/Heckmann*, 2005, Rn. 624 ff. für den absolut zu schützenden Kernbereich bei Maßnahmen nach Art. 13 Abs. 4 GG, wenn durch Terroristen und Kriminelle die Würde und das Leben Dritter bedroht werden und die in diesen Fällen die Würde der Täter um des Schutzes von Würde und Leben der Opfer willen für einschränkbar halten. Ebenso *Zippeli-*

dass sich die Beurteilung der Verfassungsmäßigkeit der polizeirechtlichen Bestimmungen der Länder über Lauschangriffe an den Maßstäben des Urteils zum Großen Lauschangriff zu orientieren hat, da das BVerfG zum Ausdruck gebracht habe, dass das Instrument der Wohnraumüberwachung nicht ausschließlich auf den Bereich der strafverfolgenden Polizeiarbeit beschränkt sei.[1112] Diese Ansicht wird geteilt von *Kutscha*, der die Landesgesetzgeber zur Präzisierung der Eingriffsgrundlagen für die präventive Wohnraumüberwachung aufgefordert sieht, da die Vorgaben des BVerfG auch bei der Regelung des gefahrenabwehrenden Lauschangriffs Beachtung erfordern würden.[1113]

Bezieht sich das BVerfG bei der Erstreckung des Schutzes von Art. 13 GG auf die weiteren Phasen der Datenverarbeitung ausdrücklich auf seine Rechtsprechung zu Art. 10 GG und dessen Einschränkung durch präventive Maßnahmen, so müssen die im Rahmen des Art. 13 GG getroffenen Feststellungen – jedenfalls was die Datenverarbeitung angeht[1114] – im Umkehrschluss auch für Art. 10 GG gelten, unabhängig von der Einordnung der Maßnahme in den präventiven oder repressiven Bereich. Die Vorgaben des BVerfG zur Verarbeitung von repressiven Wohnraumüberwachungsdaten finden daher auch für die Datenverarbeitung präventiver Telekommunikationsdaten Beachtung.

Die Übertragbarkeit findet ihre Stütze auch in der Entscheidung des BVerfG zum Nds.SOG 2005. Insbesondere bei der Unterrichtungspflicht nimmt das BVerfG nicht nur auf das BND-Urteil, sondern auch auf das Urteil zum „Großen Lauschangriff“ Bezug.[1115] Zwar hebt das BVerfG die Unterschiede zwischen Art. 13 GG und Art. 10 GG beim Kernbereich hervor, doch macht es bei seinen Ausführungen zu den Anforderungen an die Datenverarbeitung keinen Unterschied zwischen repressiven und präventiven Maßnahmen und solchen nach Art. 10 oder Art. 13 GG.[1116]

---

us/Würtenberger, 2005, § 28 II 2 c) bb) und d) die dann für die Erhebung der absolut geschützten Informationen umfängliche verfahrensmäßige Sicherungen fordern.

1112 Vgl. *Gusy*, JuS 2004, 457 (461) auch unter Hinweis auf MVVerfGH, LKV 2000, 345.

1113 Vgl. *Kutscha*, NJW 2005, 20 (22).

1114 Was den Eingriff in den absolut geschützten Kernbereich angeht, mag anderes gelten, vgl. *Würtenberger/Heckmann*, 2005, Rn. 624; *Zippelius/Würtenberger*, 2005, § 28 II 2 c bb).

1115 Vgl. Urteil des BVerfGE 113, 349 (390).

1116 Vgl. Urteil des BVerfGE 113, 349 (390 ff.).

II. Der Datenschutz nach den Landespolizeigesetzen

1. Die Regelungen im PAG

a) Die Zweckbindung

Zu den Anforderungen an die Datenerhebung gehört nicht nur, dass sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Einzelnen erkennbar aus dem Gesetz ergeben. Sondern der Zweck, zu dem Eingriffe in das Fernmeldegeheimnis vorgenommen werden dürfen, muss bereichsspezifisch und präzise bestimmt werden und das erhobene Datenmaterial muss für diesen Zweck geeignet und erforderlich sein. Speicherung und Verwendung erlangter Daten sind daher grundsätzlich an den Zweck gebunden, den das zur Kenntnisnahme ermächtigende Gesetz festgelegt hat.[1117]

Art. 34 c Abs. 4, Satz 2 Nr. 1 PAG[1118] enthält die spezielle Zweckbindung der aus einer Telekommunikationsüberwachung nach Art. 34 a und 34 b PAG erlangten Daten. Diese dürfen nur zu den Zwecken verwendet werden, zu denen sie erhoben wurden. Was unter den Begriff „verwendet werden“ fällt, ergibt sich aus dem Zusammenspiel mit den allgemeinen Regeln zur Datenverarbeitung.[1119] Das allgemeine Zweckbindungsgebot ist in Art. 37 Abs. 2, Satz 1 PAG verankert. Danach darf die Speicherung, Veränderung und Nutzung nur zu dem Zweck erfolgen, zu dem personenbezogene Daten erlangt worden sind. Die Erhebungszwecke, zu denen die gewonnenen Daten verwendet, also gespeichert, verändert und genutzt, werden dürfen, ergeben sich aus Art. 34 a PAG.

b) Die Zweckänderung

Da der von Art. 10 GG vermittelte Geheimnisschutz nicht dadurch verloren geht, dass bereits eine staatliche Stelle von dem Fernmeldevorgang Kenntnis erlangt hat, beziehen sich die Anforderungen des Grundrechts auch auf die Weitergabe der Daten und Informationen, die unter Aufhebung des Fernmeldegeheimnisses erlangt worden sind. Denn bei der Weitergabe

---

1117 Vgl. BVerfGE 100, 313 (360); BVerfGE 110, 33 (53 f.), wo ausgeführt wird, dass die jeweilige Norm zudem so klar formuliert sein muss, dass der Betroffene anhand der gesetzlichen Regelung erkennen können muss, unter welchen Voraussetzungen sein Verhalten mit dem Risiko der Überwachung verbunden ist.

1118 Art. 34 c Abs. 4, Satz 2 Nr. 2 PAG sieht dagegen die Möglichkeit der Zweckänderung zu Strafverfolgungszwecken vor.

1119 Vgl. Art. 37 ff. PAG.

handelt es sich regelmäßig nicht nur um eine Ausweitung der Stellen oder Personen, die über die Kommunikation informiert werden, sondern um die Überführung der Daten in einen anderen Verwendungszusammenhang, der für die Betroffenen mit zusätzlichen, unter Umständen schwereren Folgen verbunden ist, als im ursprünglichen Verwendungszusammenhang.[1120] Zwar schließt der Grundsatz der Zweckbindung Zweckänderungen nicht grundsätzlich aus. Die Zweckänderung bedarf jedoch einer gesetzlichen Grundlage, die formell und materiell mit dem Grundgesetz vereinbar ist.[1121] Erforderlich ist eine Ermächtigungsgrundlage, die dem Bestimmtheitsgrundsatz Rechnung trägt und Bezug auf eine bestimmte Empfängerbehörde oder zumindest deren Aufgabenbereich nimmt.[1122] Weiter müssen die Zweckänderungen durch Allgemeinbelange gerechtfertigt sein, die die grundrechtlich geschützten Interessen überwiegen. Der neue Verwendungszweck muss sich auf die Aufgaben und Befugnisse der Empfängerbehörde beziehen und hinreichend normenklar geregelt sein.[1123] Auch dürfen der Verwendungszweck, zu dem die Erhebung erfolgt ist und der veränderte Verwendungszweck nicht miteinander unvereinbar sein.[1124] Die Gefahrenlagen, deren Verwirklichung bei dem jeweiligen Übermittlungsvorgang in Rede stehen, muss der Gesetzgeber so eingrenzen, dass das von ihnen geschützte Rechtsgut gewichtig genug ist, um die Fortsetzung des Überwachungseingriffs zu rechtfertigen.[1125] Auch sind klare Regelungen erforderlich, ob nur die Daten des Störers oder auch die Dritter weitergegeben werden dürfen.[1126]

Bei der Verwendung dieser Daten zu einem anderen als dem Erhebungszweck, sind folgende Konstellationen zu unterscheiden:

- Die Behörde, die die Daten erhoben hat, will sie zu einem anderen (Gefahrenabwehr-) Zweck verwenden;
- die Erhebungsbehörde will die Daten zu Gefahrenabwehrzwecken an eine andere Behörde weitergeben;

1120 Vgl. BVerfGE 100, 313 (360). Siehe auch *Schenke*, 2007, Rn. 207; *Petri*, in: Lisken/Denninger, Kapitel H, Rn. 411.

1121 Siehe BVerfGE 65, 1 (46); E 100, 313 (389); *Würtenberger/Heckmann*, 2005, Rn. 638; *W.-R. Schenke*, JZ 2001, 997 (998); *Jarass*, in: Jarass/Pieroth, Art. 10 GG, Rn. 19.

1122 Vgl. BVerfGE 110, 33 (70); *Jarass*, in: Jarass/Pieroth, Art. 10 GG, Rn. 17.

1123 *Hermes*, in: Dreier (Hrsg.), Art. 10 GG, Rn. 63; *Jarass*, in: Jarass/Pieroth, Art. 10 GG, Rn. 17

1124 Vgl. BVerfGE 100, 313 (360); BVerfGE 110, 33 (73 f.); *Würtenberger/Heckmann*, 2005, Rn. 638; *Zippelius/Würtenberger*, 2005, § 28 I. 2.a).

1125 Vgl. BVerfGE 110, 33 (75). So für die Anforderungen an die Beschränkungen des Art. 10 Abs. 2 GG *Zippelius/Würtenberger*, 2005, § 28 I. 2.b).

1126 Vgl. BVerfGE 110, 33 (75).

- die Behörde will die Daten zu Strafverfolgungszwecken nutzen.[1127]

Sind unterschiedliche Erhebungsvoraussetzungen vorgesehen, kann ein Abweichen von den eigenen Erhebungsvoraussetzungen dann in Betracht kommen, wenn ansonsten die Empfängerbehörde die Daten nochmals erheben müsste und könnte.[1128]

Dürfen der Verwendungszweck, zu dem die Erhebung erfolgt ist, und der veränderte Verwendungszweck nicht miteinander unvereinbar sein, so liegt eine solche Unvereinbarkeit dann vor, wenn mit der Zweckänderung grundrechtsbezogene Beschränkungen des Einsatzes bestimmter Erhebungsmethoden umgangen würden, also die Informationen für den geänderten Zweck nicht oder nicht in dieser Art und Weise hätten erhoben werden dürfen.[1129]

Auch bei der Weitergabe an andere Gefahrenabwehrbehörden, ausländische Stellen und Private sind die Anforderungen des Fernmeldegeheimnisses zu berücksichtigen und nicht pauschal auf deren Aufgabenerfüllung abzustellen.[1130] Die übermittelnde Behörde hat dabei über die Berechtigung des Auskunftsersuchens zu entscheiden.[1131]

aa) Die Verwendung der Daten zu anderen (Gefahrenabwehr-)Zwecken

Das PAG regelt in Art. 34 c Abs. 4, Satz 2 eindeutig, dass die durch eine Maßnahmen nach Art. 34 a und b gewonnenen Daten nur zu den Zwecken verwendet werden dürfen, zu denen sie erhoben wurden[1132] sowie zu Zwecken der Strafverfolgung, wenn sie zur Verfolgung von Straftaten im Sinne des § 100 a StPO benötigt werden.

1127 Nur die Konstellationen (2) und (3) betreffen damit auch eine Datenweitergabe, da die Daten im Fall (1) bei der Erhebungsbehörde bleiben, es sei denn, sie werden innerhalb der Erhebungsbehörde weitergegeben, vgl. § 40 Abs. 5 Nds.SOG.

1128 Siehe *Walden*, 1996, S. 317 ff. für die Weitergabe präventiver Daten an Strafverfolgungsbehörden, wenn die StPO im Vergleich zu den Polizeigesetzen unterschiedliche Erhebungsvoraussetzungen vorsieht.

1129 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 638.

1130 Vgl. *Petri*, in: Lisken/Denninger, Kapitel H, Rn. 436.

1131 Anderes gilt wohl, bei der Datenübermittlung an Polizei- und andere Behörden. In diesen Fällen soll die Prüfung, ob das Ersuchen im Rahmen der Aufgaben des Empfängers liegt, genügen. Bestehen jedoch Bedenken, so ist die Rechtmäßigkeit aber auch in diesen Fällen vollständig nach zu prüfen, vgl. *Petri*, in: Lisken/Denninger, Kapitel H, Rn. 438.

1132 Spricht eine Vorschrift für die erstmalige Speicherung personenbezogener Daten ganz allgemein von „Zweck“, liegt es nahe, der speichernden Stelle die Aufgabe zuzuweisen, den Zweck der Speicherung festzulegen, wobei sie darüber entscheidet, wie konkret die Zweckbestimmung ist, vgl. *Würtenberger/Heckmann*, 2005, Rn. 636; *Dörr/Schmidt*, 1997, § 14, Rn. 3; *Ehmann*, RDV 1988, 221 (230).

Eine Regelung über die personenbezogenen Daten Dritter ist in Art. 34 a Abs. 2, Sätze 2 und 3 PAG für den Einsatz des IMSI-Catchers vorgesehen. Danach dürfen die Daten Dritter nur erhoben werden, wenn dies aus technischen Gründen unvermeidbar ist. Nach Beendigung der Maßnahme sind sie unverzüglich zu löschen, dürfen also nicht verändert oder weitergegeben werden.

bb) Die Weitergabe an eine andere (Gefahrenabwehr-)Behörde

Die Problematik der Weitergabe von Telekommunikationsdaten an Gefahrenabwehrbehörden ist nicht neu. Die Diskussion drehte sich dabei um die nach den §§ 100 a ff StPO erhobenen repressiven Telekommunikationsdaten und deren Verwendung für präventive Zwecke.[1133]

Der Meinungsstreit darüber, ob für die Weitergabe der repressiv gewonnenen Daten an Gefahrenabwehrbehörden Voraussetzung sei, dass die Polizeigesetze Art. 10 GG als einzuschränkendes Grundrecht zitieren[1134], dürfte nach dem BND-Urteil geklärt sein, da das BVerfG eindeutig zum Ausdruck brachte, dass die Datenübermittlung einen weiteren Grundrechtseingriff in Art. 10 GG darstellt. Art. 10 GG schützt nicht nur vor der staatlichen Kenntnisnahme der Telekommunikationsdaten, sondern sein Schutz erstreckt sich auch auf den Informations- und Datenverarbeitungsprozess, der sich an die zulässige Kenntnisnahme anschließt sowie auf den Gebrauch, der von den erlangten Daten gemacht wird.[1135] Deshalb können an eine solche Datenverwendung grundsätzlich keine geringeren Anforderungen gestellt werden, als an den erstmaligen Eingriff in das Fernmeldegeheimnis.

Konsequent und richtig sind daher die Anforderungen, die das BVerfG an die Übermittlungsschwellen für Telekommunikationsdaten stellt.[1136] Es hat die Datenübermittlung durch den

---

1133 Vgl. *Globig*, ZRP 1991, 81 ff.; *ders.*, ZRP 1991, 289 ff.; *Hassemer*, ZRP 1991, 121 ff.; *Riegel*, ZRP 1991, 286 f.; *Schild*, ZRP 1991, 311 ff. Siehe auch *W.-R. Schenke*, 2007, Rn. 197 a f.; *Würtenberger/Heckmann*, 2005, Rn. 651 ff.

1134 Die Verwendung repressiv gewonnener Telekommunikationsdaten durch die Gefahrenabwehrbehörden, obwohl die wenigsten Polizeigesetze Art. 10 GG als einzuschränkendes Grundrecht benennen, ist damit begründet worden, dass durch die Weitergabe lediglich das Recht auf informationelle Selbstbestimmung betroffen sei, so *Zeitler*, 1998, Rn. 507. Nach *Würz*, 1993, Rn. 348 soll das Zitiergebot aufgrund „immanenter Grundrechtsschranken" nicht greifen, da zu Abwehr von Gefahren für höherwertige Rechtsgüter ein Eingriff in Art. 10 GG zulässig sei. *Würz* übersieht dabei, dass verfassungsimmanente Schranken dann greifen, wenn das Grundrecht vorbehaltlos gewährleistet wird, Art. 10 Abs. 2 GG aber gerade einen Gesetzesvorbehalt vorsieht.

1135 Vgl. BVerfGE 100, 313 (359) mit dem Hinweis auf BVerfGE 65, 1 (46), bestätigt durch BVerfGE 110, 33 (68 ff.).

1136 Vgl. BVerfGE 100, 313 (388 ff.).

BND an die Strafverfolgungsbehörden für unzulässig angesehen, da diese unter Voraussetzungen möglich war, bei deren Vorliegen die Strafverfolgungsbehörden zur Telekommunikationsüberwachung selbst nicht berechtigt gewesen wären.[1137] Das BVerfG hat ausgeführt, dass „es nicht gerechtfertigt ist, die Übermittlungsschwelle für personenbezogene Daten, die aus Eingriffen in das Fernmeldegeheimnis gemäß §§1; 3 G-10-Gesetz stammen, unter diejenige abzusenken, welche auch sonst bei der Strafverfolgung für Eingriffe in das Fernmeldegeheimnis nach § 100 a StPO gilt. Im Hinblick auf die nicht geringe Schwere des Eingriffs erscheint es bei der Übermittlung der vom Bundesnachrichtendienst erhobenen Daten vielmehr verfassungsrechtlich geboten, eine Tatsachenbasis für den Verdacht vorzuschreiben, die der in § 100 a StPO entspricht."[1138]

Im AWG-Beschluss hat das BVerfG die Übermittlungsvorschrift des § 41 Abs. 2 AWG als unvereinbar mit dem Grundgesetz angesehen, da diese keine Bezugnahme auf den bzw. einen bestimmten Aufgabenbereich des Empfängers enthielt. Es hat eine klare Regelung gefordert, inwieweit die Empfängerbehörden befugt sein sollen, die übermittelten Daten zu verwerten.[1139]

Knüpft das BVerfG bei der Datenübermittlung zwischen Gefahrenabwehr- und Strafverfolgungsbehörden daran an, ob die Voraussetzungen für einen Primäreingriff bei der Empfängerbehörde vorliegen, so hat dies den Hintergrund, dass an Eingriffe zu Gefahrenabwehrzwecken und an solche zu Strafverfolgungszwecken unterschiedliche verfassungsrechtliche Anforderungen zu stellen sind.[1140] Werden aber Daten zwischen Gefahrenabwehrbehörden weitergeben, so erfolgt dies zu Zwecken der Gefahrenabwehr.[1141]

Das BVerfG hat festgestellt, dass sich der neue Verwendungszweck auf die Aufgaben und Befugnisse der Empfängerbehörde beziehen muss und der Erhebungszweck mit dem Ver-

---

1137 Vgl. BVerfGE 100, 313 (390 ff.).

1138 BVerfGE 100, 313 (394), bestätigt durch BVerfGE 109, 279 (377). Siehe dazu auch *Würtenberger/Heckmann*, 2005, Rn. 114

1139 Vgl. BVerfGE 110, 33 (74 f.).

1140 Divergieren die Eingriffsvoraussetzungen so ist auf den Schutzzweck der Norm abzustellen: Dient die höhere Eingriffsschwelle wie in aller Regel dem informationelle Selbstbestimmungsrecht oder dem sonstigen Grundrechtsschutz des Betroffenen, ist die Zweckänderung solcher Daten, die unterhalb dieser Eingriffsschwelle verwendet werden sollen, unzulässig, vgl. *Würtenberger/Heckmann*, 2005, Rn. 639.

1141 Allerdings sehen die die hier untersuchten Polizeigesetze unterschiedliche Voraussetzungen für die erstmalige Datenerhebung vor.

wendungszweck nicht unvereinbar sein darf.[1142] Daran sind die Vorschriften der Landespolizeigesetze zu messen. Dürfen die Polizeibehörden Telekommunikationsdaten zu Gefahrenabwehrzwecken unter bestimmten Voraussetzungen erheben und nutzen, so dürfen sie diese an andere Behörden zur Gefahrenabwehr unter diesen Voraussetzungen weitergeben. Sieht die Empfängerbehörde andere (höhere) Voraussetzungen als die Übermittlungsbehörde vor, so kann eine Übermittlung dann stattfinden, wenn die Empfängerbehörde die Daten ansonsten selbst durch einen zusätzlichen Eingriff erheben müsste und dürfte.[1143]

Eine die Weitergabe an eine Gefahrenabwehrbehörde kommt nur in Betracht, wenn deren Ermächtigungsgesetze Art. 10 GG zitieren.[1144] Eine Ausnahme kann allenfalls in Betracht kommen bei der Gefährdung höchstrangiger Rechtsgüter, da hier die staatlichen Schutzpflichten aus Art. 2 Abs. 2 GG Eingang in die verfassungskonforme Auslegung des Polizeirechts finden und die Polizei nicht tatenlos eine Gefährdung überragender Rechtsgüter eintreten lassen kann.[1145]

Die Art. 39 bis 41 PAG enthalten die allgemeinen Regeln der Datenübermittlung, sowie besondere Vorschriften für die Übermittlung innerhalb und außerhalb des öffentlichen Bereichs.

Ist in Art. 34 c Abs. 2, Satz 1 PAG geregelt, dass Telekommunikationsdaten nur verwendet werden dürfen zu dem Zweck zu dem sie erhoben worden sind, gilt dies auch für die Datenübermittlung an andere Behörden. Eine Weitergabe zu beliebigen Gefahrenabwehrzwecken ist nicht zulässig.

1142 Vgl. BVerfGE 100, 313 (360); BVerfGE 110, 33 (74 f.). Siehe auch *Würtenberger/Heckmann*, 2005, Rn. 638.

1143 Vgl. die Regelung in Art. 42 PAG, wonach die bayerische Polizei eine Übermittlung von Telekommunikationsdaten nur verlangen, wenn die Voraussetzungen vorliegen unter denen sie (rechtmäßig) diese Daten erheben darf.

1144 So für die Weitergabe repressiv erlangter Telekommunikationsdaten an die Gefahrenabwehrbehörden *W.-R. Schenke*, JZ 2001, 997 (1001).

1145 So für die Verwendung von Daten nach den §§ 100 a ff StPO für präventive Zwecke, *Würtenberger/Heckmann*, 2005, Rn. 654; *Nack*, in: KK, § 100 g StPO, Rn. 10; *Walden*, 1996, S. 338, 344; aA *W.-R. Schenke*, 2007, Rn. 197 b. Vgl. auch § 41 Abs. 5, Satz 2 ThPAG.

Die Datenübermittlung an die Polizei ist in Art. 42 PAG geregelt.[1146] Danach kann die bayerische Polizei eine Übermittlung von Telekommunikationsdaten nur verlangen, wenn die Voraussetzungen vorliegen unter denen sie (rechtmäßig) diese Daten erheben darf. Gleiches gilt für die Übermittlung ohne Ersuchen.

Eine Regelung über Daten Dritter ist nur beim Einsatz des IMSI-Catchers vorgesehen. Diese sind nach Beendigung der Maßnahme gemäß Art. 34 a Abs. 2, Satz 2 PAG zu löschen, sie dürfen also nicht weitergegeben werden.

cc) Die Weitergabe an die Strafverfolgungsbehörden[1147]

Nach § 161 Abs. 1, Satz 1 StPO[1148] ist die Staatsanwaltschaft befugt, von den Polizeibehörden Auskunft über alle präventiv-polizeilich erhobenen Daten zu verlangen.[1149] Damit ist die Nutzung von Daten aus einer präventiv-polizeilichen Datenerhebung zu Zwecken der Strafverfolgung in der StPO geregelt.[1150]

Eine Einschränkung dieser Zweckänderung ergibt sich aus § 161 Abs. 2 StPO und § 100 d Abs. 5 Nr. 3 StPO für die Verwertung der durch die präventive Wohnraumüberwachung gewonnenen Daten.[1151]

Nach § 161 Abs. 2 StPO ist die Übermittlung präventiv-polizeilich erhobener Telekommunikationsdaten nur zulässig, wenn die Daten zur Aufklärung von Straftaten verwendet werden,

---

1146 Zu den Zweifeln, ob die Regelung der Datenübermittlung an die Polizei in einem Polizeiaufgabengesetz eine Rechtfertigung findet, vgl. *Honnacker/Beinhofer*, § 42 PAG, Rn. 1.

1147 Allgemein zur Verwendung präventiv erhobener Daten zu repressiven Zwecken, vgl. *Hefendehl*, StV 2001, 700 (704 ff.).

1148 § 161 StPO ist durch Art. 1 des Strafverfahrensänderungsgesetzes 1999 vom 02.08.2000, BGBl. I, S. 1253, neu gefasst worden. Die Vorschrift erteilt den Strafverfolgungsbehörden die Befugnis, die zum Zweck der Strafverfolgung erforderlichen Ermittlungshandlungen vorzunehmen und bringt damit den Charakter der Regelung als Eingriffsermächtigung zum Ausdruck, vgl. *Pfeiffer*, § 161 StPO, Rn. 1.

1149 Vgl. *Würtenberger/Heckmann*, 2005, Rn. 641; *Brodersen*, NJW 2000, 2536 (2538 f.).

1150 Diese Rechtslage hat daher für die Auslegung des Begriffs „anderer polizeilicher Zweck“ in § 37 Abs. 2, Satz 2 PolG BW zur Konsequenz, dass davon die Strafverfolgung nicht umfasst wird vgl. *Belz/Mußmann*, § 37 PolG BW Rn. 25, *Würtenberger/Heckmann*, 2005, Rn. 641.

1151 Zu den Änderungen des infolge des BVerfG-Urteils zum „Großen Lauschangriff“ eingeführten § 100 d Abs. 6 Nr. 3 StPO gegenüber § 100 f Abs. 2 StPO a.F., vgl. *Würtenberger/Heckmann*, 2005, Rn. 643. § 100 d Abs. 6 StPO wurde durch das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007, BGBl. I, S. 3198, zu § 100 d Abs. 5 StPO.

bei denen nach § 100 a StPO eine Telekommunikationsüberwachung angeordnet werden dürfte.[1152]

Art. 37 Abs. 4 PAG bestimmt, dass anderweitige Rechtsvorschriften über die Datenspeicherung, -veränderung und –nutzung von den Regeln der Art. 37 ff. PAG unberührt bleiben.[1153] Insbesondere gilt dies für Rechtsvorschriften über die Datenspeicherung im Bereich des Strafverfahrens.[1154] Für den repressiven Bereich schließen die Regelungen der Strafprozessordnung eine unmittelbare Anwendung der Datenverarbeitungsvorschriften des PAG grundsätzlich aus.[1155]

In Art. 34 c Abs. 4, Satz 2 Nr. 2 PAG ist festgehalten, dass Daten aus einer Telekommunikationsüberwachung nur zur Strafverfolgung verwendet werden dürfen, wenn sie zur Verfolgung von Straftaten nach § 100 a Satz 1 StPO erforderlich sind.

c) Die Kennzeichnung

Die erforderliche Bindung der Telekommunikationsdaten an ihren Erhebungszweck lässt sich nur gewährleisten, wenn auch nach der Erhebung erkennbar bleibt, dass es sich um Daten handelt, die aus Eingriffen in das Fernmeldegeheimnis stammen. Eine Kennzeichnung ist daher von Verfassungs wegen geboten.[1156]

In seinem Urteil zum Großen Lauschangriff fordert das BVerfG, dass der Gesetzgeber sowohl den datenerhebenden als auch den datenempfangenden Behörden zur Sicherung der Zweckbindung eine Kennzeichnungspflicht aufzuerlegen hat.[1157]

1152 Vgl. auch den Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG BT-Dr. 16/5846, S. 15.

1153 Die Regelungen des PAG über die Datenspeicherung, Datenveränderung und Datennutzung sind in anderen Rechtsgebieten nur anwendbar, wenn in den Spezialgesetzen keine spezifischen Vorschriften enthalten sind. Dies gilt gemäß Art. 39 Abs. 5 PAG auch für die Datenübermittlung, siehe *Honnacker/Beinhofer*, § 40 PAG, Rn. 1.

1154 Vgl. *Honnacker/Beinhofer*, § 37 PAG, Rn. 7.

1155 Vgl. *Honnacker/Beinhofer*, § 37 PAG, Rn. 7.

1156 Vgl. BVerfGE 100, 313 (361).

1157 Ansonsten könnten die aus der akustischen Wohnraumüberwachung stammenden Daten in einer Weise gespeichert und mit anderen Daten vermischt werden, die ihre Herkunft nicht mehr erkennen lassen, vgl. BVerfGE 109, 279 (379 f.).

Art. 34 c Abs. 4, Satz 1 PAG bestimmt, dass die durch eine Maßnahme nach Art. 34 a und 34 b PAG erlangten Daten besonders zu kennzeichnen sind. Keine Bestimmung wird aber darüber getroffen, ob allgemein Daten zu kennzeichnen sind, die mittels Eingriff in das Fernmeldegeheimnis erlangt und an die Polizeibehörden weitergegeben worden sind.

d) Die Informationspflicht

Art. 10 GG vermittelt den Grundrechtsträgern Anspruch auf Kenntnis von Maßnahmen der Fernmeldeüberwachung, um einen effektiven Grundrechtsschutz zu gewährleisten.[1158]

Wie die Kenntnisgewährung im Einzelnen auszugestalten ist, gibt das Grundgesetz nicht vor. Die Verfassung gebietet nur, dass eine Benachrichtigung dann stattfindet, wenn Datenerhebungen heimlich erfolgen, Auskunftsansprüche aber nicht eingeräumt worden sind oder diese den Rechten der Betroffenen nicht angemessen Rechnung tragen.[1159] Soweit die Kenntnis des Eingriffs in das Fernmeldegeheimnis dazu führen würde, dass dieser seinen Zweck verfehlt, ist es von Verfassungs wegen nicht zu beanstanden, die Kenntnisgewährung entsprechend einzugrenzen.[1160]

Das BVerfG hat diese Grundsätze in seinem Urteil zum Großen Lauschangriff präzisiert. Da die Benachrichtigungspflicht der Gewährung effektiven Schutzes der betroffenen Grundrechte dient, sind diejenigen von der heimlichen Maßnahme zu unterrichten, denen infolge des Eingriffs Rechtsschutzmöglichkeiten und Anhörungsrechte offen stehen müssen.[1161]

1158 Vgl. BVerfGE 100, 313 (361); *Würtenberger/Heckmann*, 2005, Rn. 689; *Kutscha*, NVwZ 2003, 1296 ff. Siehe auch *Lisken*, DRiZ 1987, 184 (188). Das BVerfG hat zu Art. 10 Abs. 2 GG u.a. ausgeführt: „Die Verfassungsvorschrift kann im Hinblick auf den Grundsatz der Verhältnismäßigkeit nur so verstanden werden, dass sie nachträglich die Benachrichtigung zulässt und sie fordert in den Fällen, in denen eine Gefährdung des Schutzes der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes ausgeschlossen werden kann." vgl. BVerfGE 30, 1 (21). Siehe auch BVerfGE 109, 279 (363 ff.).

1159 Vgl. BVerfGE 100, 313 (361); E 109, 279 (363 f.); E 30, 1 (21; 31 f.).

1160 Vgl. BVerfGE 100, 313 (361); E 109, 279 (364). Zur Kritik an den Ausnahmen des § 22 Abs. 8, Satz 2 PolG BW vgl. *Würz*, 1993, Rn. 232; *Petri*, in: Lisken/Denninger, Kap. H, Rn. 547; *Würtenberger/Heckmann*, 2005, Rn. 691 ff.

1161 Vgl. BVerfGE 109, 279 (364). Zielperson einer akustischen Wohnraumüberwachung ist zwar allein der Beschuldigte. Der Grundrechtseingriff einer akustischen Wohnraumüberwachung ist aber nicht auf diese Person begrenzt. Als Beteiligte iSd § 101 Abs. 1 StPO sind daher neben dem Beschuldigten, die Inhaber und Bewohner einer Wohnung zu benachrichtigen, in denen Abhörmaßnahmen durchgeführt worden sind, vgl. BVerfGE 109, 279 (365). Da die Benachrichtigung weiterer Beteiligter den Grundrechtseingriff bei der Zielperson der Maßnahme aber vertiefen kann, hängt das Bestehen von Benachrichtigungspflichten von einer Abwägung ab. Das gilt insbesondere, wenn die Überwachung keine verwertbaren Ergebnisse erbracht hat. Außerdem kann die Benachrichtigungspflicht dort auf praktische Hinweise stoßen, wo die

Verfassungsrechtlich nicht zu beanstanden ist es, dass die Benachrichtigung unter bestimmten Umständen zurückgestellt wird, so wenn dies durch die besondere Geheimhaltungsbedürftigkeit der Maßnahme veranlasst ist und dem Schutz eines überragend wichtigen Rechtsguts dient.[1162] Soweit aber eine Benachrichtigung unterbleibt, weil durch die Unterrichtung die öffentliche Sicherheit oder die weitere Verwendung eines nicht offen ermittelnden Beamten gefährdet werden würde, sei dies mit Art. 13 Abs. 1 GG; 19 Abs. 4 GG und Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG nicht vereinbar.[1163] Das BVerfG führt hierzu aus, dass mit dem Begriff der öffentlichen Sicherheit die Suspendierung der Benachrichtigungspflicht unter eine Generalklausel gestellt wird, aber nicht alle betroffenen Schutzgüter zur Zurückstellung der Benachrichtigung ausreichen. Daher müsse der Gesetzgeber präzisieren, welche der unter den Begriff der öffentlichen Sicherheit zusammengefassten Rechtsgüter er als so gewichtig einschätzt, dass sie eine Zurückstellung oder gar einen Ausschluss der Benachrichtigung bei heimlichen Grundrechtseingriffen rechtfertigen.[1164] Für die vorgesehene Verwendungsgefährdung des verdeckten Ermittlers reiche es aus, wenn infolge der Benachrichtigung jede weitere Verwendung des verdeckt ermittelnden Beamten auch im Zusammenhang mit anderen Vermittlungsverfahren gefährdet wäre. Die Möglichkeit zum weiteren Einsatz eines verdeckten Ermittlers sei jedoch kein gleichgewichtiges Anliegen, um den Eingriff in die Rechte des Betroffenen durch die unterbleibende Benachrichtigung zu rechtfertigen. Die darauf gestützte Hinauszögerung der Benachrichtigung erstrecke sich über einen unabsehbaren Zeit-

---

Identität des Beteiligten im Rahmen der Maßnahme der Behörde nicht bekannt geworden ist. Auch die Nachforschungen zur Feststellung der Identität sonstiger Beteiligter könnte den Grundrechtseingriff sowohl für die Zielperson wie für sonstige Beteiligte noch vertiefen, so BVerfGE 109, 279 (365). Für diese Abwägung ist zum einen die Intensität des Überwachungseingriffs bedeutsam, insbesondere in welchem Umfang und zu welchem Inhalt Kommunikation des unbekannten Betroffenen abgehört und aufgezeichnet worden ist und zum anderen, welchen Aufwand die Feststellung der Identität des Betroffenen fordert und welche Beeinträchtigungen mit ihr für die Zielperson und sonstige Beteiligte verbunden sein können, vgl. BVerfGE 109, 279 (365).

1162 Vgl. BVerfGE 30, 1 (18). Das BVerfG hat durch dieses Urteil vom 15.12.1970 entschieden, dass Art. 1 § 5 V G-10-Gesetz mit Art. 10 Abs. 2 Satz 2 GG insoweit nicht vereinbar und deshalb nichtig sei, als er die Unterrichtung des Betroffenen über die Überwachungsmaßnahmen auch ausschließe, wenn sie ohne Gefährdung des Zwecks der Beschränkung erfolgen kann. Seit dem Urteil des BVerfG war die zuständige Behörde verpflichtet, den Betroffenen zu informieren, sobald dies ohne Gefährdung des Beschränkungszwecks erfolgen konnte. Zu diesem Zweck überprüfte der zuständige Minister jeweils von Amts wegen sofort nach Aufhebung der Maßnahmen oder später in regelmäßigen Abständen, ob die betroffene Person zu unterrichten war. Der Minister legte seine Entscheidung der G-10-Kommission vor. Die G-10-Kommission konnte den Minister anweisen, den Betroffenen davon zu unterrichten, dass er überwacht worden war, vgl. EGMR EuGRZ 1979, 278 (280).

1163 Vgl. BVerfGE 109, 279 (366 f.); so auch *W.-R. Schenke*, 2007, Rn. 197. Differenzierend *Würtenberger/Heckmann*, 2005, Rn. 691.

1164 Vgl. BVerfGE 109, 279 (366).

raum und die Benachrichtigung sei letztlich von zukünftigen ermittlungstaktischen Erwägungen der Strafverfolgungsbehörden abhängig.[1165]

Weiter betont das BVerfG, dass die Befassung unabhängiger Stellen mit der Überprüfung der Gründe für die weitere Geheimhaltung staatlicher Eingriffe ein wesentliches Element des Grundrechtsschutzes sei, den die Betroffenen selbst nicht wahrnehmen können.[1166] Für den Rechtsschutz des Betroffenen sei in Fällen der Informationszurückstellung wichtig, dass auch die Entscheidung über die Zurückstellung gerichtlich kontrolliert wird. Um sicherzustellen, dass die Zurückstellung auch im weiteren Verlauf auf das unbedingt Erforderliche begrenzt bleibe, bedürfe es in Zeitabständen einer wiederkehrenden gerichtlichen Überprüfung. Die grundrechtssichernde Funktion des Richtervorbehalts ende erst, wenn der Betroffene unterrichtet sei und sich selbst bei Gericht gegen die Maßnahme wehren könne.[1167]

Übertragen auf die Telekommunikationsüberwachung bedeutet dies, dass nicht nur die Störer oder Verdachtspersonen, sondern auch davon verschiedene Anschlussinhaber und -nutzer unterrichtet werden, soweit deren Anschlüsse der Überwachung unterlagen.[1168] Dies gilt jedenfalls für Anschlussnutzer, die regelmäßig den Anschluss benutzen, wie z.B. Mitbewohner. Nicht verlangt werden kann sicherlich, jeden Gesprächspartner zu informieren, der vom betroffenen Anschluss aus angerufen wurde oder diesen angerufen hat. Insofern ist der Personenkreis bei der Wohnraumüberwachung eher eingrenzbar. Gleiches gilt für diejenigen,

---

1165 Vgl. BVerfGE 109, 279 (367). *Würtenberger/Heckmann*, 2005, Rn. 691 halten für den Fall der Zurückstellung bzw. des Unterbleibens der Benachrichtigung wegen „Verwendungsgefährdung" eines verdeckten Vermittlers eine Einzelfallabwägung für geboten. Auf der einen Seite stehe das Verwendungsinteresse der Polizei, die in so wichtigen Bereichen wie der Bekämpfung der Organisierten Kriminalität auf den Einsatz verdeckter Ermittler angewiesen ist. Auf der anderen Seite sei das Interesse des Betroffenen an der Unterrichtung zu berücksichtigen. Wer die weiteren Einsatzmöglichkeiten eines verdeckten Ermittlers – wie das BVerfG – unmöglich mache, gefährde damit die Effektivität im Bereich massiver Gefährdungen der öffentlichen Sicherheit.

1166 Vgl. BVerfGE 109, 279 (367) unter Hinweis auf MVVerfG, LKV 2000, 345 (355). Siehe dazu *Würtenberger/Heckmann*, 2005, Rn. 693, die zur Ausnahme des § 22 Abs. 8, Satz 2, 3. Alt. PolG BW, der eine Ausnahme von der Unterrichtungspflicht zulässt, wenn seit Beendigung der Maßnahme 5 Jahre vergangen sind, ausführen, dass die Befriedungsfunktion des Zeitablaufs fragwürdig erscheint, wenn der Rechtsfrieden gerade dadurch hergestellt wird, dass das Gesetz die Rechtsschutzmöglichkeit durch den Ausschluss der Unterrichtung von vornherein vermeidet. Außerdem können – wie es die Rechtspraxis zu dem inzwischen aufgehobenen § 5 Abs. 5, Satz 3 G-10-Gesetz gezeigt hat – schutzwürdige Interessen des Betroffenen an der Kenntnis der Maßnahmen bestehen, die sich erst nach einer Offenbarung verifizieren lassen. Hinzu kommen die gegenüber dem G-10-Gesetz bestehenden weiteren Rechtsschutzdefizite, die (neben der Kontrolle durch den Datenschutzbeauftragten) zumindest durch ein parlamentarisches Kontrollverfahren kompensiert werden müssten.

1167 Vgl. BVerfGE 109, 279 (368).

1168 Auch *P.M. Huber*, ThürVBl. 2005, 33 (39) bejaht eine Benachrichtigungspflicht gegenüber Nichtstörer und sonstigen Dritten.

deren Mobilfunkgeräte sich in eine simulierte Funkzelle eines IMSI-Catchers eingeloggt haben. Nachforschungsmaßnahmen zur Identitätsfeststellung dieser Personen würden den Grundrechtseingriff aufgrund der möglichen Vielzahl der Betroffenen sowohl für die Zielperson als auch die sonstigen Beteiligten nur vertiefen.[1169] Erforderlich ist nicht nur die gerichtliche Überprüfung der Benachrichtigungszurückstellung, sondern auch des Benachrichtigungsausschlusses.

Der bayerische Gesetzgeber hat sich bei seinen Regelungen an den Vorgaben des BVerfG-Urteils zum Großen Lauschangriff orientiert[1170] und die dortigen Anforderungen auf die Telekommunikationsüberwachung übertragen. Er hat eine eigene Abwägung getroffen, unter welchen Umständen eine Unterrichtung erfolgen soll. Dabei hat er auf die Voraussetzungen Bezug genommen unter denen er auch die Einschränkung des Telekommunikationsgeheimnisses zulässt.[1171]

Die Pflicht zur Unterrichtung ist im PAG in Art. 34 c Abs. 5 geregelt. Danach sind die Personen von den Maßnahmen nach Art. 34 a Abs. 1, 2 und 4; 34 b PAG zu unterrichten, gegen die die Maßnahmen gerichtet waren. Ebenfalls sind die Personen zu unterrichten, deren Daten im Rahmen einer solchen Maßnahme erhoben und zu den in Art. 34 c Abs. 4 Satz 2 PAG genannten Zwecken verwendet wurden.[1172]

Die Unterrichtung erfolgt, sobald dies ohne Gefährdung des Zwecks der Maßnahme, der eingesetzten nicht offen ermittelnden Beamten oder der in Art. 34 a Abs. 1 Nr. 1 und Nr. 2 a PAG genannten Rechtsgüter erfolgen kann.[1173] Erfolgt eine Benachrichtigung nicht binnen

---

1169 Ausnahmen sind jedoch denkbar, beispielsweise wenn den Betroffenen Zeugnisverweigerungsrechte zustehen.

1170 Vgl. LT-Drucks. 15/2096, S. 48.

1171 Vgl. auch LT-Drucks. 15/2096, S. 63, 48.

1172 Nach Ansicht des bayerischen Gesetzgebers ist eine Einschränkung des Kreises der zu benachrichtigenden Personen aus dem Rechtsgedanken heraus, dass die grundrechtliche Betroffenheit mit den Interessen des jeweiligen Adressaten abzuwägen ist und dass die Benachrichtigung nicht zu Vertiefung der Eingriffe führen darf, gerechtfertigt, vgl. LT-Drucks. 15/2096, S. 63.

1173 Ist wegen desselben Sachverhalts ein strafrechtliches Ermittlungsverfahren gegen den Betroffenen eingeleitet worden, ist die Unterrichtung in Abstimmung mit der Staatsanwaltschaft nachzuholen, sobald dies der Stand des Ermittlungsverfahrens zulässt, Art. 34 c Abs. 5, Satz 3 iVm Art. 34 Abs. 6, Satz 2 PAG. Wenn sich an den die Maßnahme auslösenden Sachverhalt ein strafprozessuales Ermittlungsverfahren anschließt, wird die Unterrichtung des Betroffenen nicht ausgeschlossen, sondern nur die Entscheidung auf die Staatsanwaltschaft übertragen, vgl. *Würtenberger/Heckmann*, 2005, Rn. 692 für § 22 Abs. 8, Satz 2, Alt. 2 PolG BW. Gegen die Informationsbeschränkungen im Strafprozess bestehen keine Bedenken, vgl. BVerfG DÖV 2001, 777 (779) zur entsprechenden Regelung in § 9 HbgGDVP.

sechs Monate nach Beendigung der Maßnahme, bedarf die weitere Zurückstellung der richterlichen Zustimmung. Die richterliche Entscheidung ist vorbehaltlich einer anderen richterlichen Anordnung jeweils nach einem Jahr erneut einzuholen.[1174] Eine Unterrichtung kann mit richterlicher Zustimmung auf Dauer unterbleiben, wenn überwiegende Interessen eines Betroffenen entgegenstehen oder die Identität oder der Aufenthaltsort eines Betroffenen nur mit unverhältnismäßigem Aufwand ermittelt werden kann.[1175]

e) Die Kontrolle durch staatliche Organe und Hilfsorgane

Nach Art. 10 Abs. 2, Satz 2 GG kann das einschränkende Gesetz bestimmen, dass Beschränkungen dem Betroffenen nicht mitgeteilt werden, und dass an die Stelle des Rechtswegs die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.

Die Vorschrift lässt nach Ansicht des BVerfG Raum, es beim normalen Rechtsweg zu belassen oder statt der Nachprüfung durch von der Volksvertretung bestellte Organe ein besonderes gerichtliches Verfahren vorzusehen.[1176]

Soll an die Stelle des Rechtswegs eine solche Nachprüfung treten, so muss diese materiell und verfahrensmäßig der gerichtlichen Kontrolle gleichwertig sein. Das einschränkende Gesetz muss ein Organ vorsehen, das in richterlicher Unabhängigkeit und für alle an der Vorbereitung, verwaltungsmäßigen Entscheidung und Durchführung der Überwachung Beteiligten verbindlich über die Zulässigkeit der Überwachungsmaßnahme und über die Frage, ob der Betroffene zu benachrichtigen ist, entscheidet und die Überwachungsmaßnahme untersagt, wenn es an den rechtlichen Voraussetzungen fehlt.[1177]

Den staatlichen Organen und Hilfsorganen kann aber auch die Funktion zukommen, durch ihre Unterrichtung zur Wahrnehmung politischer Verantwortung des Parlaments beizutragen. So kann Kenntnis gewonnen werden über die Eignung und Folgen der durchgeführten Maß-

---

1174 Art. 34 c Abs. 5, Satz 3 iVm Art. 34 Abs. 6, Sätze 3 und 4 PAG.

1175 Art. 34 c Abs. 5, Satz 3 iVm Art. 34 Abs. 6, Satz 5 PAG.

1176 Vgl. BVerfGE 30, 1 (21). Wie die Kontrolle auszugestalten ist, schreibt die Verfassung nicht vor. Dem Gesetzgeber steht es frei, die ihm geeignet erscheinende Form zu wählen, wenn sie nur hinreichend wirksam ist, vgl. BVerfGE 100, 313 (361).

1177 Vgl. BVerfGE 30, 1 (23). Zur Wirksamkeit gehört, dass sich die Kontrolle auf alle Schritte des Prozesses der Fernmeldeüberwachung erstreckt. Kontrollbedürftig ist sowohl die Rechtmäßigkeit der Eingriffe als auch die Einhaltung der gesetzlichen Vorkehrungen zum Schutz des Fernmeldegeheimnisses, vgl. BVerfGE 100, 313 (362).

nahmen, um die allgemeine Kontrollfunktion des Parlaments gegenüber der Exekutive auszuüben.[1178]

Das PAG sieht einen Richtervorbehalt für die Anordnung der Telekommunikationsüberwachung vor.[1179] Auch erfolgt grundsätzlich eine Benachrichtigung, so dass der Rechtsweg offen steht.[1180]

f) Die Löschungspflicht

Eine Löschungspflicht ist verfassungsrechtlich jedenfalls dann geboten, wenn die Abhörmaßnahme Kommunikation aus dem Kernbereich privater Lebensgestaltung erfasst. Ist dies der Fall dürfen die Kommunikationsinhalte des höchstpersönlichen Bereichs nicht gespeichert und verwertet werden, sondern sind unverzüglich zu löschen.[1181]

Schließlich müssen die erlangten Daten, da die Erfassung und Aufzeichnung des Fernmeldeverkehrs sowie die Verwendung der dadurch erlangten Informationen an bestimmte Zwecke gebunden sind, aber auch vernichtet werden, sobald sie für die festgelegten Zwecke oder den gerichtlichen Rechtsschutz nicht mehr erforderlich sind.[1182] Die Vernichtungspflicht ist auch im Licht des Art. 19 Abs. 4 GG zu verstehen. Die Rechtsschutzgarantie des Art. 19 Abs. 4 GG verbietet Maßnahmen, die darauf abzielen oder geeignet sind, den Rechtsschutz des Betroffenen zu vereiteln.[1183] Daher muss die Vernichtungspflicht für alle Fälle, in denen der Betroffene die gerichtliche Kontrolle staatlicher Informations- und Datenverarbeitungsmaßnahmen anstrebt, mit der Rechtsschutzgarantie so abgestimmt werden, dass der Rechtsschutz nicht unterlaufen oder vereitelt wird.[1184]

Sicherungsmechanismen, die dafür Sorge tragen, dass der Betroffene vor der Löschung benachrichtigt wird und damit die Rechtmäßigkeit der Maßnahmen gerichtlich überprüfen las-

---

1178 Vgl. BVerfGE 109, 279 (373).

1179 Art. 34 c Abs. 1 iVm Art. 34 Abs. 4, Sätze 1 und 2 PAG. Zur Kritik vgl. das Kapitel „Grundrechtliche Anforderungen“ unter III. 2. d).

1180 Art. 34 c Abs. 5 PAG. Die Zurückstellung oder endgültige Unterlassung der Benachrichtigung ist daher ebenfalls durch einen Richter zu kontrollieren.

1181 Vgl. BVerfGE 113, 349 (392); *Würtenberger/Heckmann*, 2005, Rn. 625 d. Siehe dazu auch die Ausführungen in diesem Kapitel unter I.4.

1182 BVerfGE 100, 313 (362); E 109, 279 (380).

1183 Vgl. BVerfGE 100, 313 (400); E 69, 1 (49).

1184 Vgl. BVerfGE 100, 313 (400); E 109, 279 (380).

sen kann, sind keine spezifische Anforderung an die Telekommunikationsüberwachung, sondern allgemein an die verdeckte Datenerhebung.[1185]

Die spezifische Konfliktlage, dass es einerseits dem Datenschutz entspricht, nicht mehr benötigte Daten zu löschen und dass andererseits durch die Löschung ein effektiver Rechtsschutz erschwert, wenn nicht gar vereitelt wird, kann in der Weise gelöst werden, dass in Fällen, in denen der Betroffene ein ernsthaftes Interesse am Rechtsschutz oder an der Geltendmachung seines Datenschutzrechts gegenüber der zuständigen Stelle haben kann, die Daten einstweilen nicht gelöscht, wohl aber gesperrt werden und zu keinem anderen Zweck als zur Information des Betroffenen und zur gerichtlichen Kontrolle verwendet werden dürfen.[1186] Eine Vernichtung kommt erst dann in Betracht, wenn sichergestellt ist, dass die Daten für eine gerichtliche Nachprüfung der Rechtmäßigkeit der Maßnahme nicht mehr in Betracht kommen.[1187]

Sind die durch Maßnahmen nach Art. 34 a oder 34 b PAG erlangten Daten zur Verwendung der in Art. 34 c Abs. 4 Satz 2 PAG genannten Zwecke nicht erforderlich oder besteht für diese ein Verwendungsverbot, sind sie zu sperren, wenn sie zum Zweck der Information der Betroffenen und zur gerichtlichen Überprüfung der Erhebung oder Verwendung der Daten noch benötigt werden; anderenfalls sind sie zu löschen.[1188]

Im Falle der Unterrichtung des Betroffenen sind die Daten zu löschen, wenn der Betroffene sich nicht innerhalb eines Monats nach seiner Benachrichtigung mit Rechtsbehelfen gegen die Maßnahme gewendet hat; auf diese Frist ist in der Benachrichtigung hinzuweisen. Im Falle eines Rechtsbehelfs sind die Daten nach Abschluss des Rechtsbehelfsverfahrens zu löschen.[1189]

1185 Vgl. dazu SächsVerfGH JZ 1996, 957 (963 ff.) und VGH Baden-Württemberg, DVBl. 1992, 1309 (1311) mit Anmerkung von *Dronsch*, DVBl. 1992, 1314.

1186 Vgl. BVerfGE 109, 279 (380 f.).

1187 § 7 Abs. 4, Satz 1 G-10 ordnet die Vernichtung erst an, wenn sie im Rahmen einer gerichtlichen Nachprüfung der Rechtmäßigkeit der Beschränkungsmaßnahmen nicht mehr von Bedeutung sein können. Das ist nach § 7 Abs. 4, Satz 3 G-10 im Abstand von sechs Monaten zu prüfen. Regelmäßig wird das bedeuten, dass die Daten nach einer Benachrichtigung des Betroffenen noch für sechs Monate aufzubewahren sind, vgl. BVerfGE 100, 313 (400).

1188 Art. 34 c Abs. 6, Satz 2 PAG.

1189 Art. 34 c Abs. 6, Satz 3 iVm Art. 34 Abs. 7, Sätze 3 und 4 PAG.

Für Daten, die den Kernbereich privater Lebensgestaltung betreffen, gelten die Regelungen der Art. 34 a Abs. 1, Satz 4 und Art. 34 c Abs.6, Satz 1 PAG.

g) Die Dokumentationspflicht

Um eine hinreichende Kontrolle durch die vorgesehenen Gremien oder auch im Wege des Gerichtsschutzes zu gewährleisten, besteht eine Dokumentationspflicht dergestalt, dass die Übermittlung und auch die Durchführung sowie die Vernichtung und Löschung der Daten zu protokollieren sind.[1190]

Im PAG ist nur für den Fall eine Dokumentationspflicht vorgesehen, dass Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind und nicht verwendet werden dürfen, unverzüglich zu löschen sind.[1191]

2. Die Regelungen in den übrigen Polizeigesetzen

a) Die Zweckbindung

Der Grundsatz der Zweckbindung ist auch in den übrigen Polizeigesetzen zu finden[1192], jedoch ist in Niedersachsen und Hessen nicht hinreichend klar, ob das Zweckbindungsgebot auch für die sog. „aufgedrängten Daten“[1193] Geltung beanspruchen kann.

Sind die personenbezogenen Daten nicht von der niedersächsischen Polizei erhoben worden, so darf sie diese Daten gemäß § 38 Abs. 1, Satz 2 Nds.SOG zu einem der Gefahrenabwehr dienenden Zweck speichern, verändern oder nutzen; die Zweckbestimmung ist bei der Speicherung festzulegen. Keine Erhebung liegt vor, wenn Daten ohne ein Ersuchen übermittelt worden oder vom Betroffenen freiwillig mitgeteilt worden sind.[1194] Würden daher Telekommunikationsdaten ohne Ersuchen übermittelt, könnte die Polizei diese – jedenfalls dem Wortlaut nach – ohne die hohen Hürden des § 38 Abs. 1 Satz 1 iVm § 33 a Nds.SOG speichern,

---

1190 Vgl. BVerfGE 100, 313 (395 f.). Vgl. dazu auch *W.-R. Schenke*, JZ 2001, 997 (1001).

1191 Art. 34 Abs. 6, Satz 1 PAG.

1192 § 39, Satz 1 ThPAG; § 38 Abs. 1, Satz 1 Nds.SOG; § 30 Abs. 1 und 2 POG; § 20 Abs. 1, Satz 1, Abs. 3, Satz 1 HSOG.

1193 Von ausgedrängten Daten wird gesprochen, wenn Gefahrenabwehr- und Polizeibehörden die Daten von Dritten erlangt haben, obwohl diese dazu nicht aufgefordert wurden und die Behörden die Daten auch nicht selbst erhoben haben, vgl. *Meixner/Fredrich*, § 13 HSOG, Rn. 6.

1194 Vgl. *Unger/Siefken*, in: Böhrenz/Unger/Siefken, § 38 Nds.SOG, Anm. 4.

solange sie einen konkreten Verwendungszweck nach § 1 Nds.SOG festlegt.[1195] Dabei ist jedoch zu differenzieren:

Erlangt die Polizei Kenntnis von Telekommunikationsdaten beispielsweise durch Mitteilung des Gesprächspartners, dass zu einer bestimmten Zeit ein Telefonat mit dem potenziellen Störer stattgefunden hat, so liegt kein Eingriff in Art. 10 GG vor und eine Speicherung zu einem (beliebigen) Gefahrenabwehrzweck ist zulässig. Werden aber der Polizei nach § 41 Nds.SOG Daten, die aus einer Telekommunikationsüberwachung stammen, durch eine andere Behörde übermittelt, so dürfen diese nur zu dem Zweck gespeichert werden, zu denen die niedersächsische Polizei die Daten selbst hätte erheben dürfen, da Art. 10 GG seinen Schutz durch die Weitergabe der Daten nicht einbüßt. Sind die Daten rechtswidrig erhoben worden, ist eine Speicherung abzulehnen.[1196]

Die Regelung des § 20 Abs. 1 HSOG setzt voraus, dass die Polizei auch aufgedrängte Daten zu einem bestimmten Zweck erlangt.[1197] Geht man davon aus, dass andere Behörden Telekommunikationsdaten nur unter den Voraussetzungen, die das BVerfG für eine Datenübermittlung aufgestellt hat, übermitteln, steht dies im Einklang mit Art. 10 GG. Werden diese Vorgaben aber nicht eingehalten, so gelten die gleichen Anforderungen, die an die Vorschriften des Nds.SOG[1198] zu stellen sind.

b) Die Zweckänderung

aa) Die Verwendung der Daten zu anderen Gefahrenabwehrzwecken

Die übrigen Polizeigesetze enthalten im Gegensatz zum PAG weniger strenge Anforderungen an die Zweckbindung.

Die Generalklausel des § 40 Abs. 1 ThPAG, nach der die Polizei rechtmäßig erlangte Daten in Akten oder Dateien speichern, verändern und nutzen kann, soweit dies zur Erfüllung ihrer

---

1195 Vgl. *Unger/Siefken,* in: Böhrenz/Unger/Siefken, § 38 Nds.SOG, Anm. 6.
1196 Vgl. *Unger/Siefken,* in: Böhrenz/Unger/Siefken, § 38 Nds.SOG, Anm. 4.
1197 Der niedersächsische Gesetzgeber geht dagegen mangels entsprechender Regelung offensichtlich davon aus, dass Daten auch ohne Verwendungszweck übermittelt werden.
1198 Vgl. dieses Kapitel unter II. 1. b).

Aufgaben[1199], zu einer zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung[1200] oder zu statistischen sowie zu Ausbildungs- und Fortbildungszwecken[1201] erforderlich ist, wird durch § 39, Satz 2 und § 34 a Abs. 3, Satz 1 ThPAG eingeschränkt.[1202] Telekommunikationsdaten können daher gemäß § 39, Satz 2 ThPAG nur zur (weiteren) Aufgabenerfüllung nach § 2 ThPAG gespeichert, geändert und genutzt werden, wenn sie auch für diese Zwecke hätten erhoben werden können.[1203]

Die Speicherung, Veränderung oder Nutzung von personenbezogenen Daten zu anderen als den in § 38 Abs. 1 Nds.SOG genannten Zwecken ist nach § 39 Abs. 1 Satz 1 Nds.SOG nur zulässig wenn, die Daten zur Erfüllung eines anderen Zwecks der Gefahrenabwehr erforderlich sind und sie auch zu diesem Zweck mit dem Mittel oder der Methode hätten erhoben

---

1199 Die Aufgaben der Polizei ergeben sich aus § 2 ThPAG. Danach kommt der Polizei die Gefahrenabwehr für die öffentliche Sicherheit und Ordnung zu. Sie hat für die Verfolgung von Straftaten vorzusorgen und Straftaten zu verhüten (vorbeugende Bekämpfung von Straftaten) sowie Vorbereitungen zu treffen, um künftige Gefahren abwehren zu können (Vorbereitung auf die Gefahrenabwehr). Ihr obliegt ebenfalls der Schutz privater Rechte, wenn gerichtliche Hilfe nicht rechtzeitig zu erreichen ist. Sie leistet anderen Behörden Vollzugshilfe und erfüllt weiter die ihr durch Rechtsvorschrift übertragenen Aufgaben.

1200 Die Speicherung zur zeitlich befristeten Dokumentation betrifft die kurzfristige Aufzeichnung des polizeilichen Einsatzgeschehens, wie z.B. die Aufzeichnung des Notrufs 110. Die Speicherung zur Vorgangsverwaltung meint die Aktenregistratur auf EDV-Basis, um dem jeweiligen Sachbearbeiter einen Überblick über alle in seinem Aufgabengebiet angefallenen Informationen, z.B. Beschwerden, Anzeigen usw., zu ermöglichen, vgl. *Ebert/Honnacker/Seel*, § 40 ThPAG, Rn. 18. Daten aus einer Telekommunikationsüberwachung sind davon nicht betroffen.

1201 § 40 Abs. 3 und 4 ThPAG.

1202 Das Verhältnis der §§ 40 und 39 ThPAG ist vergleichbar mit den Regelungen des § 37 Abs. 1 und 2 PolG BW. § 37 Abs. 1 PolG BW enthält ebenfalls die Generalklausel zum Speichern, Verändern und Nutzen personenbezogener Daten, wenn dies zur Wahrnehmung polizeilicher Aufgaben erforderlich ist, vgl. *Wolf/Stephan*, § 37 PolG BW, Rn. 8, während § 37 Abs. 2 PolG BW das die Generalklausel einschränkende Gebot der Zweckbindung enthält, vgl. *Wolf/Stephan*, § 37 PolG BW, Rn. 14.

1203 Besondere Regelungen für Daten Dritter sind nicht vorgesehen. Zufallserkenntnisse, die die Polizei im Rahmen einer Telekommunikationsüberwachung erlangt hat, darf sie gemäß § 34 a Abs. 3, Satz 1 ThPAG zu zwei Zwecken speichern, verändern und nutzen: entweder zur Verhütung und Aufklärung von Straftaten im Sinne des § 100 a StPO oder zur Abwehr einer gegenwärtigen erheblichen Gefahr. Eine gegenwärtige Gefahr (vgl. § 54 Nr. 3 b OBG) liegt dann vor, wenn die Einwirkung des schädigenden Ereignisses bereits begonnen hat oder wenn diese Einwirkung unmittelbar oder in allernächster Zeit mit einer an Sicherheit grenzender Wahrscheinlichkeit bevorsteht. Eine bereits eingetretene, noch andauernde Störung ist immer eine gegenwärtige Gefahr. Eine erhebliche Gefahr (vgl. § 54 Nr. 3 c OBG) ist eine Gefahr für ein bedeutsames Rechtsgut, wie z.B. Leben, Gesundheit, Freiheit, wesentliche Vermögenswerte oder den Bestand des Staates sowie eine Gefahr, die eine größere Anzahl von Personen betrifft, vgl. *Ebert/Honnacker/Seel*, § 2 ThPAG, Rn. 19 a). Für Nichtkatalogtaten ist damit eine mittelbare Verwertung in der Form zulässig, dass die gewonnenen Zufallserkenntnisse zur Grundlage weiterer Ermittlungen zur Abwehr einer gegenwärtigen erheblichen Gefahr gemacht werden, vgl. LT-Drucks. Th. 3/2128, S. 36. Die Ausdehnung ist geboten, weil die Polizei dem Legalitätsprinzip nach § 163 StPO unterliegt, so dass sie die Zufallserkenntnisse in ein neues strafprozessuales Verfahren einbringen muss. Daneben kann sie auch nicht sehenden Auges eine Gefahr eintreten lassen, so *Ebert/Honnacker/Seel*, § 34 a ThPAG, Rn. 39; aA *W.-R. Schenke*, 2005, Rn. 197 e, der darin Befugnisse der Polizei sieht, die dieser in Widerspruch zu dem in § 6 EGStPO enthaltenen Kodifikationsprinzip sowie neben den diesbezüglich bereits in der StPO getroffenen Regelungen eingeräumt werden.

werden dürfen (Nr. 1)[1204], die Daten zur Behebung einer Beweisnot unerlässlich sind (Nr. 2)[1205] oder die betroffene Person eingewilligt hat (Nr. 3)[1206].

Die Bestimmungen des § 39 Abs. 1 Nds.SOG zur Zweckdurchbrechung sind aufgrund der besonderen Regelungen in § 33 b Abs. 1, Satz 3 Nds.SOG nicht auf Daten Dritter anzuwenden, die durch den Einsatz des IMSI-Catchers erlangt wurden. Diese Daten dürfen nur für den Abgleich zur Ermittlung der gesuchten Geräte- und Kartennummer verwendet werden und unterliegen insofern einem Verbot der Zweckänderung. Ansonsten ist die Speicherung, Veränderung oder Nutzung personenbezogener Daten über unvermeidbar betroffene Dritte[1207] gemäß § 39 Abs. 5, Satz 1 Nds.SOG nur zulässig, wenn dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben und Freiheit einer Person oder zur Verhütung von Straftaten von erheblicher Bedeutung erforderlich ist.

Das POG enthält durch einen Verweis in § 31 Abs. 7, Satz 1 auf § 29 Abs. 5 eine spezielle Regelung der Zweckänderung für Telekommunikationsdaten. Danach dürfen die aus einer Telekommunikationsüberwachung erlangten Daten nur für andere Zwecke verwendet werden, soweit dies zur Verfolgung von Straftaten von erheblicher Bedeutung[1208], zur Abwehr einer dringenden Gefahr[1209] oder zur vorbeugenden Bekämpfung von Straftaten von erheblicher Bedeutung[1210] erforderlich ist.[1211]

1204 Zur Datenverwendung zu einem anderen Gefahrenabwehrzweck ist es erforderlich, dass die Polizei die Daten zu diesem Zweck auch mit den angewandten Mitteln oder Methoden hätte erheben dürfen. Das kommt bei Telekommunikationsdaten nur in Betracht zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person (§ 33 a I Nds.SOG). Mit dieser Zweckbindung folgt der niedersächsische Gesetzgeber den Vorgaben des BVerfG aus dem BND- Urteil, vgl. *Unger/Siefken*, in: Böhrenz/Unger/Siefken, § 39 Nds.SOG, Anm. 3.

1205 Diese liegt dann vor, wenn es einem Prozessbeteiligten auch unter gerichtlicher Mithilfe unmöglich ist, noch erforderliche Beweismittel zu benennen oder beizubringen, vgl. *Unger/Siefken*, in: Böhrenz/Unger/Siefken, § 39 Nds.SOG, Anm. 5. Im Hinblick auf das hohe Schutzgut des Art. 10 GG kann das nicht für jedes gerichtliche Verfahren gelten. Insofern ist zu fordern, den Begriff „unerlässlich" entsprechend auszulegen, so dass eine Änderung nur bei einer sonst drohenden Gefährdung oder Verletzung hochrangiger Rechtsgüter in Betracht kommt.

1206 Die Verarbeitung zu wissenschaftlichen Zwecken ist mit Art. 10 GG vereinbar, da die Daten zu anonymisieren sind. Willigt der Grundrechtsinhaber in die weitere Verarbeitung ein, ist sie ebenfalls zulässig.

1207 Bei der Telekommunikationsüberwachung handelt es sich bei unvermeidbar betroffenen Dritten um Personen, die mit den in § 33 a Abs. 1 Nds.SOG genannten Personen kommunizieren. Daten Dritter werden erfasst, wenn eine TKÜ-Maßnahme durchgeführt wird und die überwachte Person mit der oder dem Dritten kommuniziert. Da Gesprächsinhalte nur dann einen Sinn ergeben, wenn sie im Zusammenhang erfasst werden, ist es – unabhängig von den technischen Möglichkeiten – nicht ausreichend, nur die Äußerungen des Maßnahmeadressaten zu erfassen, vgl. *Unger/Siefken*, in Böhrenz/Unger/Siefken, § 33 a Nds.SOG, Anm. 5.

1208 Die Zweckänderung zu Strafverfolgungszwecken wird in diesem Kapitel unter II. 2. c) genauer erläutert.

1209 Eine dringende Gefahr besteht schon dann, wenn sie einem wichtigen Rechtsgut droht, ohne dass sie bereits eingetreten zu sein oder unmittelbar bevorzustehen braucht. Die Gefahr ist unmittelbar aus Art. 13

§ 31 Abs. 3 POG sieht vor, dass Daten Dritter beim Einsatz des IMSI-Catchers nach § 31 Abs. 2, Satz 1 Nr. 4 POG nur erhoben werden dürfen, wenn dies aus technischen Gründen unvermeidbar ist. Sie dürfen nur für den Datenabgleich verwendet werden und sind ansonsten unverzüglich zu löschen (so genanntes Zweckänderungs- und -verwendungsverbot)[1212].

§ 20 Abs. 3, Satz 2 HSOG sieht Ausnahmen vom Zweckbindungsgebot des § 20 Abs. 3, Satz 1 HSOG vor. Danach ist die Verarbeitung zu einem anderen gefahrenabwehrbehördlichen Zweck zulässig, soweit die Gefahrenabwehr – und die Polizeibehörden die Daten auch zu diesem Zweck hätten erheben und verarbeiten können[1213]

bb) Die Weitergabe an eine andere (Gefahrenabwehr-)Behörde

Auch in Thüringen und Niedersachsen ist die Datenweitergabe nur für die Zwecke zulässig, zu denen die Daten erhoben oder gespeichert wurden.

Abs. 7 GG in das POG übertragen. Die dringende Gefahr ist nur auf die Wichtigkeit des Rechtsguts bezogen, nicht aber auf die zeitliche Nähe oder die Wahrscheinlichkeit des Schadensereignisses, vgl. *Roos*, § 9 POG, Rn. 28.

1210 § 28 Abs. 3 POG benennt die Straftaten von erheblicher Bedeutung in Form eines offenen Straftatenkataloges. § 28 Abs. 3 Nr. 1 POG erfasst alle Verbrechen im Sinne des § 12 Abs. 1 StGB. Nach § 28 Abs. 3 Nr. 2 POG wird jedes Vergehen erfasst, sofern es im Einzelfall nach Art und Schwere geeignet ist, den Rechtsfrieden besonders zu stören und einer der aufgezählten Fallgruppen zuzurechnen ist. Die Tat muss sich entweder gegen hochrangige Rechtsgüter richten (Leib, Leben, Freiheit, bedeutende Sach-/Vermögenswerte) oder bestimmten Deliktsbereichen zuzuordnen sein (Verkehr mit Waffen oder Betäubungsmitteln, Geld-/Wertzeichenfälschungen, Hochverrat, Landesverrat, Friedensverrat oder Gefährdung der Landesverteidigung) oder gewerbs-, gewohnheits-, serien- oder bandenmäßig oder sonst organisiert begangen werden, vgl. *Roos*, § 28 POG, Rn. 11.

1211 Die weitere Nutzung der Telekommunikationsdaten ist damit unter geringeren Voraussetzungen vorgesehen als ihre Erhebung, was nur zulässig sein kann, soweit die Nutzung zur Abwehr von Gefahren für solche Rechtsgüter erfolgt, wie sie in § 31 Abs. 1 POG für die Datenerhebung vorgesehen sind. Der Straftatenkatalog entspricht nicht den Anforderungen, die an die Einschränkung des Art. 10 GG zu stellen sind. Zwar wird gefordert, dass die Straftaten im Einzelfall geeignet sein müssen, den Rechtsfrieden besonders zu stören, doch wird keine Eingrenzung, z.B. durch einen bestimmten (Mindest-)Strafrahmen, vorgenommen. Auch die abstrakte Zuordnung der Straftaten in bestimmte Deliktsbereiche oder ihre Begehungsweise reicht für sich genommen nicht aus, um eine Einschränkung des Art. 10 GG zu rechtfertigen, vgl. das Kapitel 6 unter IV. 4. c) cc).

1212 Vgl. *Roos*, § 31 POG, Rn. 6.

1213 Vgl. *Meixner/Fredrich*, § 20 HSOG, Rn. 12. Die Verwertung von Zufallserkenntnissen ist nach § 15 a Abs. 5 Satz 2 HSOG jedoch außer zur Abwehr einer Gefahr im Sinne des § 15 a Abs. 1 HSOG nur zur Strafverfolgung zulässig oder wenn Bundesrecht eine Pflicht zur Übermittlung vorsieht, vgl. *Meixner/Fredrich*, § 15 a HSOG, Rn. 4. Regelungen über Daten Dritter sind nicht speziell vorgesehen.

Im ThPAG ist die Datenübermittlung in § 41 ThPAG geregelt.[1214] Die Datenübermittlung ist zulässig zur Erfüllung polizeilicher Aufgaben und darf nur zu dem Zweck erfolgen, zu dem die Daten erlangt worden sind.[1215] Andere Behörden und sonstige öffentliche Stellen können personenbezogene Daten an die thüringer Polizei übermitteln, soweit dies zur Erfüllung polizeilicher Aufgaben erforderlich erscheint.[1216] Auf Verlangen sind die Daten zu übermitteln. Die Polizei darf entsprechende Übermittlungsersuchen nur stellen, wenn die Voraussetzungen für die Datenerhebung vorliegen.[1217]

§ 40 Nds.SOG enthält die allgemeinen Regeln der Datenübermittlung[1218]. Sein Absatz 1, der die Durchbrechung des Zweckbindungsgrundsatzes nur unter den Voraussetzungen des § 39 Abs. 1, 2 und 6 Nds.SOG zulässt, ergänzt die §§ 41 bis 44 Nds.SOG[1219] für die Übermittlung von Daten zur Gefahrenabwehr durch die Verwaltungsbehörden und die Polizei, wenn diese

---

1214 § 41 Abs. 1 ThPAG regelt die Übermittlung zwischen Dienststellen der thüringer Polizei. Diese Regelung gilt in gleicher Weise für Dienststellen anderer Länder oder des Bundes, vgl. *Ebert/Honnacker/Seel*, § 41 ThPAG, Rn. 4. Durch die Trennung der Verwaltungspolizei von der Vollzugspolizei sind andere Behörden (Verwaltungsgemeinschaften, Gemeinden) in vielen Fällen für die Gefahrenabwehr zuständig, vgl. *Ebert/Honnacker/Seel*, § 41 ThPAG, Rn. 5. § 41 Abs. 2 ThPAG regelt daher die Datenweitergabe an andere für die Gefahrenabwehr zuständige Behörden oder öffentliche Stellen. § 41 Abs. 3, Satz 1 ThPAG ist die Rechtsgrundlage für Datenübermittlungen durch die Polizei an andere Behörden oder öffentliche Stellen. § 41 Abs. 3, Satz 2 ThPAG lässt die Übermittlung personenbezogener Daten an nicht öffentliche Stellen und an Einzelpersonen zu. § 41 Abs. 4 ThPAG regelt die Übermittlung der Polizei an ausländische öffentliche Stellen. Bei der Übermittlung wird zwischen Störerdaten und Daten Dritter keine Unterscheidung getroffen.

1215 Vgl. § 41 Abs. 2, Satz 2; 39, Satz 1 ThPAG und § 41 Abs. 2 bis 4 iVm § 41 Abs. 5, Satz 1 ThPAG. Die Ausnahme in § 41 Abs. 5, Satz 2 ThPAG findet für die Datenerhebung durch Telekommunikationsüberwachung keine Anwendung. Das der Empfänger die Daten nur zu dem Zweck nutzen darf, zu dem sie ihm übermittelt worden sind, ergibt sich aus § 41 Abs. 9, Satz 1 ThPAG.

1216 § 41 Abs. 7 ThPAG. Die Polizei ist dann gemäß §§ 39 Satz 1; 40 Abs. 1 ThPAG an den Übermittlungszweck gebunden und darf die Daten nur speichern, wenn die Übermittlung rechtmäßig war.

1217 § 41 Abs. 7, Satz 3 ThPAG. Ob für eine derartige Regelung dem thüringer Landtag die Gesetzgebungskompetenz zukommt, ist zweifelhaft. Vorschriften über die Datenweitergabe an die thüringer Polizei müssten vielmehr im jeweiligen Spezialgesetz, wie beispielsweise dem Melderechtsrahmengesetz oder dem Pass- oder Personalausweisgesetz geregelt werden. Sind keine Regelungen in den Spezialgesetzen vorhanden, so darf der Landesgesetzgeber diese Lücke nicht durch eine entsprechende Übermittlungsverpflichtung im Polizeigesetz ausfüllen. Die Übermittlungsverpflichtung der Telekommunikationsunternehmen, wie sie jetzt in § 34 a ThPAG geregelt ist, ist nur möglich, weil § 88 Abs. 3, Satz 3 TKG einen sog. Erlaubnistatbestand darstellt und (auch) dem Landesgesetzgeber damit diese Möglichkeit eröffnet ist. Ansonsten steht der Polizei ein Amtshilfegesuch offen, vgl. dazu *Kopp/Ramsauer*, § 5 VwVfG Rn. 4; *Ebert/Honnacker/Seel*, § 41 ThPAG, Rn. 24.

1218 Nach der Legaldefinition des § 3 Abs. 2 Nr. 4 NDSG ist das Übermitteln von Daten das Bekanntgeben von Daten an Dritte (Empfänger) in der Weise, dass die Daten durch die datenverarbeitende Stelle weitergegeben werden oder Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsehen oder abrufen.

1219 § 41 Nds.SOG regelt die Datenübermittlung zwischen Verwaltungsbehörden, zwischen Polizeibehörden und zwischen Verwaltungs- und Polizeibehörden. Die Datenübermittlung an andere öffentliche Stellen, an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen ist in § 43 Nds.SOG geregelt. § 44 Nds.SOG regelt die Datenweitergabe an Personen oder Stellen außerhalb des öffentlichen Bereichs und die Bekanntgabe an die Öffentlichkeit.

Daten zu einem anderen Zweck als dem, zu dem sie erlangt oder (zuletzt) gespeichert worden sind, übermittelt werden sollen.[1220]

Ein Übermittlungsgesuch an andere Polizeibehörden mit der Bitte um Übermittlung von Telekommunikationsdaten kann die niedersächsische Polizei nur stellen, wenn die Erhebungsvoraussetzungen des § 33 a Nds.SOG vorliegen.[1221]

Im POG und HSOG werden dagegen weniger strenge Anforderungen an die Datenweitergabe gestellt.

Im POG ist die Datenübermittlung in § 34 geregelt, der durch die Bestimmungen in § 35 POG ergänzt wird. Die Übermittlung ist zulässig, soweit dies zur Erfüllung polizeilicher oder ordnungsbehördlicher Aufgaben erforderlich ist.[1222] Einschränkungen für die Übermittlung personenbezogener Daten, die einer besonderen Zweckbindung unterliegen, gelten gemäß § 34 Abs. 3, Satz 3 POG lediglich für die Übermittlung an Verfassungsschutzbehörden. Auch Daten aus einem durch ein Amts- oder Berufsgeheimnisgeschütztes Vertrauensverhältnis dürfen nur übermittelt werden, wenn der Empfänger die personenbezogenen Daten zur Erfüllung des gleichen Zwecks benötigt, zu dem sie erlangt wurden.[1223]

Für Telekommunikationsdaten sind solche Beschränkungen nicht eindeutig vorgesehen. Die Einschränkungen für Telekommunikationsdaten ergeben sich indirekt aus § 31 Abs. 7, Satz 1 in Verbindung mit § 29 Abs. 9 POG.[1224] Zwar sollten durch die Änderung des POG die bereichsspezifischen Datenschutzbestimmungen insgesamt neu geregelt werden, um der erforderlichen Anpassung an die allgemeine Rechtsentwicklung und Rechtsprechung zu genü-

---

1220 Vgl. *Unger/Siefken*, in: Böhrenz/Unger/Siefken, § 40 Nds.SOG, Anm. 1. Da es für die Daten über unvermeidbar betroffene Dritte im Gegensatz zu den mit besonderen Mitteln und Methoden erhobenen Daten keine besondere Prüfungspflicht gibt, dürfen diese grundsätzlich unter den allgemeinen Voraussetzungen des § 38 Abs. 1 Nds.SOG übermittelt werden. vgl. *Unger/Siefken*, in: Böhrenz/Unger/Siefken, § 40 Nds.SOG, Anm. 3.

1221 Vgl. *Unger/Siefken*, in: Böhrenz/Unger/Siefken, § 38 Nds.SOG, Anm. 4.

1222 § 34 I POG enthält die Datenübermittlung zwischen Polizeibehörden, allgemeinen Ordnungsbehörden und zwischen diesen Behörden. § 34 Abs. 2 POG sieht die Initiativübermittlung und § 34 Abs. 3 Satz 1 POG die Anlassübermittlung an öffentliche in- und ausländische Stellen vor. Die Initiativ- und Anlassübermittlung an nicht öffentliche in- und ausländische Stellen sind in § 34 Abs. 4 und 5 POG geregelt. § 35 POG erhält ergänzende Bestimmungen für die Datenübermittlung.

1223 § 35 Abs. 4 POG.

1224 Auch die Weitergabe ist eine Zweckumwidmung, die die entsprechenden Voraussetzungen einhalten muss, vgl. *Roos*, § 29 POG, Rn. 11.

gen,[1225] doch gelten bei der Weitergabe die gleichen Bedenken wie bei der Zweckänderung. Denn diese ist unter geringeren Voraussetzungen möglich als der Primäreingriff.

Nach § 34 Abs. 6 POG können in- und ausländische Stellen von sich aus personenbezogene Daten an die allgemeinen Ordnungsbehörden und die Polizei übermitteln, wenn angenommen werden kann, dass die Kenntnis dieser Daten zur Erfüllung polizeilicher oder ordnungsbehördlicher Aufgaben erforderlich ist. Demgegenüber sind die allgemeinen Ordnungsbehörden und die Polizei zur Prüfung verpflichtet, ob die ihnen übermittelten Daten tatsächlich für die Erfüllung ihrer gesetzlich zugewiesenen Aufgaben erforderlich sind.[1226] Dies ist bei Telekommunikationsdaten nur der Fall, wenn sie für die in § 31 Abs. 1 POG genannten Zwecke benötigt werden.

Die Datenübermittlung ist im HSOG in den §§ 21 bis 23 geregelt.[1227] Dass auch bei der Datenübermittlung die Grenzen der Zweckbindung einzuhalten sind und die Empfängerbehörde die Daten nur zu dem Zweck verarbeiten darf, zu dem sie ihr übermittelt wurden, ist als Grundsatz in § 21 Abs. 1, Satz 1; Abs. 6 HSOG festgeschrieben. Allerdings gilt dies vorbehaltlich anderer Regelungen, die sich für die Telekommunikationsdaten in §§ 21 Abs. 3, Satz 3; 20 Abs. 6, Satz 2 HSOG finden.[1228] Danach dürfen Telekommunikationsdaten nur übermittelt werden, wenn dies zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist.

Zweck der Datenerhebung durch die Telekommunikationsüberwachung ist die Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person. Die Datenübermittlung ist daher entgegen § 21 Abs. 1 Satz 1 HSOG unter leichteren Voraussetzungen möglich, als die Erhebung der Daten.[1229] Diese Regelung ist nicht nachzuvollziehen, da sie der hessische Ge-

---

1225 Vgl. LT-Drucks. RhPf. 14/2287, S. 31.

1226 Vgl. *Roos*, § 34 POG, Rn. 23.

1227 § 21 HSOG enthält die allgemeinen Regeln der Datenübermittlung, § 22 HSOG regelt die Übermittlung innerhalb des öffentlichen Bereichs und § 23 HSOG die Datenübermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs. Zwischen Störerdaten und Daten Dritter wird nicht unterschieden.

1228 Dies ergibt sich durch den Verweis auf § 20 Abs. 6 Satz 2 HSOG.

1229 Diesen Widerspruch sieht auch *Ronellenfitsch*, 33. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten vorgelegt zum 31.12.2004, Punkt 5.1.1.2, http://www.datenschutz.hessen.de/Tb33/Inhalt.htm. Lediglich für die Datenübermittlung innerhalb des öffentlichen Bereichs nach § 21 Abs. 1 HSOG gilt § 20 Abs. 3 HSOG entsprechend. Danach können die Polizeibehörden Telekommunikationsdaten nur zu den Zwecken weitergeben, zu denen sie die Daten erlangt haben. Zu einem anderen Zweck ist die Datenweitergabe nur zulässig, wenn die Polizeibehörde die Daten auch zu diesem Zweck hätte erheben können.

setzgeber gerade unter dem Eindruck des BND-Urteils und des AWG-Beschlusses in das HSOG aufgenommen hat.[1230]

Zur Übermittlung von Daten an die hessische Polizei sind andere Behörden verpflichtet, wenn es für die Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person erforderlich ist.[1231]

cc) Die Weitergabe an die Strafverfolgungsbehörden

Auch die übrigen Polizeigesetze enthalten Regelungen, wonach die präventiv erhobenen Telekommunikationsdaten nach Maßgabe der StPO für strafprozessuale Zwecke verwendet werden dürfen.[1232]

c) Die Kennzeichnung

Das ThPAG enthält keine Kennzeichnungspflicht. Zwar ist in § 41 Abs. 9 ThPAG die Zweckbindungsverpflichtung der Empfängerbehörde enthalten, damit ist aber nicht gewährleistet, dass diese Daten nicht mit anderen vermischt werden und ihre Herkunft aus einer Telekommunikationsüberwachung erkennbar ist.[1233]

§ 38 Abs. 2 Nds.SOG enthält eine Kennzeichnungspflicht für die mit besonderen Mitteln oder Methoden erhobenen Daten, zu denen auch die Telekommunikationsüberwachung zählt.[1234] Ob diese Kennzeichnungspflicht bei übermittelten Daten zur Durchsetzung gelangt, ist fragwürdig.

1230 LT-Drucks. Hessen 16/2352, S. 22. Dort heißt es zur Änderung des § 21 HSOG: „... wird durch die Anfügung von Satz 3 (an Absatz 3) einer Forderung des Bundesverfassungsgerichts aus dem Beschluss vom 3. März 2004 zur Telekommunikationsüberwachung nach dem Außenwirtschaftsgesetz Rechnung getragen. Dort hat das BVerfG unter Hinweis auf sein BND-Urteil sowie auf das Urteil zur Wohnraumüberwachung vom selben Tag erklärt, dass die Datenübermittlung ausschließlich für solche Zwecke verfassungsgemäß ist, die auch als Rechtfertigung für die ursprüngliche Erhebung ausgereicht hätten."

1231 § 22 Abs. 5, Satz 2 HSOG. Für Telekommunkationsdaten kann dies aber nur gelten, wenn eine gegenwärtige Gefahrenlage gegeben ist.

1232 § 41 Abs. 1, Satz 1 ThPAG; § 39 Abs. 6 Nds.SOG; § 33 Abs. 2, Satz 3 POG; §§ 21 Abs. 7, 22 Abs. 2 HSOG.

1233 Vgl. BVerfGE 100, 313 (397).

1234 Dies ergibt sich aus § 30 Abs. 2 Nr. 2 Nds.SOG. Durch die Kennzeichnung soll gewährleistet werden, dass die Verarbeitungsbeschränkungen nach § 39 Abs. 1 und 4 Nds.SOG beachtet werden. Die Kennzeichnung besteht in einem dem Aktenvorgang vorzuheftenden Hinweis auf § 38 Nds.SOG und der Angabe der Seiten, auf denen sich die genannten Daten in der Akte befinden; vgl. *Unger/Siefken*, in: Böhrenz/Unger/Siefken, § 38 Nds.SOG, Anm. 7.

W.-R. Schenke hielt eine Verwendung von Daten aus einer strafprozessualen Telekommunikationsüberwachung trotz des Zitats des Art. 10 GG und der Vorschrift des § 38 Abs. 2[1235] im NGefAG für unzulässig, da das NGefAG seiner Ansicht nach eine Kennzeichnungspflicht für repressive erhobene und weitergegebene Daten nicht vorsah. Seiner Ansicht nach zählte die Datenerhebung nach der StPO aus systematischen Überlegungen nicht zu den besonderen Mitteln und Methoden. Auch sei in § 39 Abs. 5, Satz 2 NGefAG von einer Ermittlungspflicht abgesehen worden.[1236]

Eine § 39 Abs. 5 NGefAG entsprechende Regelung ist im Nds.SOG nicht mehr vorhanden. Eine Kennzeichnungspflicht besteht dennoch auch für übermittelte Telekommunikationsdaten gemäß § 38 Abs. 2 iVm §§ 30 Abs. 2 Nr. 2; 33 a Nds.SOG. § 38 Abs. 2 Nds.SOG spricht allgemein von „mit besonderen Mitteln oder Methoden erhobenen Daten“. Erheben meint die eigene Datenerhebung oder die Übermittlung auf Ersuchen.[1237] Darunter fällt auch die Übermittlung von Daten zu Gefahrenabwehrzwecken, die die Polizei nach den Vorschriften der StPO erhoben hat.

Der Kennzeichnungspflicht wäre auch bei der Datenübermittlung durch andere Gefahrenabwehrbehörden an die niedersächsische Polizei genüge getan, wenn diese durch eine entsprechende Kennzeichnung zu erkennen geben, dass die Daten durch eine Telekommunikationsüberwachung erhoben worden sind, da dann die niedersächsische Polizei nach § 38 Abs. 2 Nds.SOG angehalten ist, die Kennzeichnung weiterzuführen. Sind für andere Gefahrenabwehrbehörden jedoch keine Kennzeichnungspflichten vorgesehen, dürfte die Regelung des § 38 Abs. 2 Nds.SOG ins Leere laufen, da eine Nachforschungspflicht für die Polizei durch die

---

1235 § 38 Abs. 2 NGefAG lautete: In Akten gespeicherte personenbezogene Daten, die mit besonderen Mitteln und Methoden erhoben worden sind oder die die Voraussetzungen des § 39 Abs. 5 erfüllen, sind zu kennzeichnen.

1236 Vgl. *W.-R. Schenke*, JZ 2001 997, (1003). Allerdings verpflichtete § 39 Abs. 5, Satz 1 NGefAG die Polizei, die sich aus § 39 Abs. 4, Satz 1 NGefAG ergebenden speziellen Zweckbindungen auch dann zu beachten, wenn Daten nach anderen Gesetzen mit besonderen Mitteln und Methoden erhoben wurden, die denen der §§ 34 bis 37 NGefAG vergleichbar waren. Dies galt unabhängig davon, ob die Polizei die Daten selbst aufgrund von Vorschriften der StPO erhoben hatte oder ob die Daten von einer Stelle außerhalb des Landes oder aus einer Verbunddatei übermittelt worden waren. Den besonderen Mitteln und Methoden des NGefAG sollten insbesondere die Rasterfahndung und die Telefonüberwachung auf strafprozessualer Grundlage vergleichbar sein. War aus den Daten und den in diesem Zusammenhang gegebenenfalls hinzugezogenen Unterlagen nicht erkennbar, dass sie mit besonderen Mitteln oder Methoden erhoben worden waren, die denen der §§ 34 bis 37 NGefAG vergleichbar waren, brauchten aber diesbezüglich keine Nachforschungen angestellt zu werden, vgl. *Franke/Unger*, in: Böhrenz/Franke, § 39 NGefAG, Anm. 10.

1237 Vgl. *Unger/Siefken*, in: Böhrenz/Unger/Siefken, § 38 Nds.SOG, Anm. 4.

Streichung des § 39 Abs. 5 NGefAG sicher nicht begründet wurde, war doch diese Regelung als zu eng angesehen worden.[1238]

Durch den Verweis in § 31 Abs. 7 auf § 29 Abs. 9 POG besteht für die nach § 31 Abs. 1 POG erhobenen Daten eine Kennzeichnungspflicht. Diese Kennzeichnung ist vom Gesetzgeber wegen der Intensität und Schwere des Rechtseingriffs und der Sensibilität der gewonnenen personenbezogenen Daten vorgesehen worden. Damit soll sichergestellt werden, dass bei einer Datenübermittlung auch für den Empfänger der Daten stets erkennbar ist, dass diese Daten einen bestimmten Schutz genießen.[1239] Wie im Nds.SOG ist aber nicht eindeutig geregelt, dass Telekommunikationsdaten auch zu kennzeichnen sind, wenn die rheinland-pfälzische Polizei die Daten nicht selbst erhoben hat, sondern ihr übermittelt oder sonst bekannt geworden sind.

Die Kennzeichnungspflicht für Telekommunikationsdaten unabhängig von ihrer Erhebungsweise ist in § 20 Abs. 6, Satz 2 HSOG enthalten. Diese ist schon durch das Hessisches Gesetz über die Umorganisation der Polizei (HPUOG) vom 22.12.2000[1240] im Hinblick auf die Rechtsprechung des BND-Urteils eingefügt worden.[1241]

d) Die Informationspflicht

Eine Informationspflicht bei Erhebung von Telekommunikationsdaten ergibt sich aus dem Verweis in § 34 a Abs. 3, Satz 2 ThPAG auf § 34 Abs. 7 ThPAG[1242]. § 47 Ab. 1 ThPAG enthält zudem einen Auskunftsanspruch des Betroffenen über die zu seiner Person gespeicherten Daten.

1238 Vgl. LT-Drucks. 15/240, S. 21. Gleiches gilt, wenn der niedersächsischen Polizei Daten ohne Ersuchen übermittelt werden, da in diesem Fall keine Datenerhebung vorliegen soll, vgl. *Unger/Siefken*, in: Böhrenz/Unger/Siefken, § 38 Nds.SOG, Rn. 4. Auch in diesem Fall ist eine Kennzeichnung erforderlich.

1239 Vgl. *Roos*, § 29 POG, Rn. 10.

1240 GVBl. Hessen I, S. 577.

1241 Vgl. *Meixner/Fredrich*, § 20 HSOG, Rn. 26.

1242 § 34 Abs. 7 ThPAG lautet: Personen, gegen die sich die Datenerhebungen richten, sind nach Abschluss der Maßnahmen darüber durch die Polizei zu unterrichten, sobald dies ohne Gefährdung des Zwecks der Datenerhebung, der eingesetzten Person, der Möglichkeit ihrer weiteren Verwendung oder der öffentlichen Sicherheit geschehen kann. Die Unterrichtung unterbleibt, wenn wegen desselben Sachverhalts ein strafrechtliches Ermittlungsverfahren gegen den Betroffenen eingeleitet worden ist.

Eine Unterrichtung des Betroffenen[1243] mag nach § 34 Abs. 7 ThPAG unterbleiben können, wenn wegen desselben Sachverhalts ein strafrechtliches Ermittlungsverfahren eingeleitet wird und solange der Zweck der Maßnahme oder die eingesetzten Personen gefährdet werden[1244], nicht aber soweit die weitere Verwendung dieser Person oder die öffentliche Sicherheit gefährdet sein kann.[1245] Die gerichtliche Überprüfung der Zurückstellung ist im ThPAG nicht vorgesehen.

In Niedersachsen ist die Pflicht zur Information des Betroffenen und ihre Ausnahmen allgemein in § 30 Abs. 4 und 5 Nds.SOG geregelt.[1246] Zu den betroffenen Personen gehören auch die unvermeidbar betroffenen Dritten, soweit deren Daten nach § 38 Abs. 1 - 4 Nds.SOG gespeichert werden.[1247] Die Unterrichtung erfolgt, sobald dies möglich ist ohne die Maßnahme zu gefährden und soweit zur Durchführung der Unterrichtung nicht in unverhältnismäßiger Weise weitere Daten der betroffenen Person erhoben werden müssten.[1248] Die Ausnahmen von der Unterrichtungspflicht sind in § 30 Abs. 5 Nds.SOG geregelt.[1249] Wie im ThPAG kann jedoch die Unterrichtung nicht unterbleiben, weil Zwecke der Verfolgung einer beliebigen Straftat entgegenstehen.[1250]

1243 Geht man von der Terminologie des allgemeinen Datenschutzrechts aus, so fällt unter den Begriff des Betroffenen die bestimmte oder bestimmbare natürliche Person, über deren persönliche oder sächliche Verhältnisse die Einzelangaben etwas aussagen, vgl. *Dammann*, in: Simitis (Hrsg), § 3 BDSG, Rn. 40. Das wären Störer und Kontakt- und Begleitpersonen. Siehe *Würtenberger/Heckmann*, 2005, Rn. 562, wonach die befragte Person Adressat, Betroffener der Datenerhebung dagegen derjenige ist, um dessen persönliche Daten es geht.

1244 Nach *Ebert/Honnacker/Seel*, § 34 ThPAG, Rn. 48 sind dies Gefahren für Leib und Leben der verdeckten Ermittler.

1245 Vgl. BVerfGE 109, 279 (366 f.). Dass der Gesetzgeber eine von *Würtenberger/Heckmann*, 2005, Rn. 691 geforderte Einzelfallabwägung vorgenommen hat, ist nicht zu erkennen.

1246 Die betroffene Person ist mit der Unterrichtung auf die Rechtsgrundlage der Datenverarbeitung und das Auskunftsrecht nach § 16 NDSG hinzuweisen. § 16 NDSG beinhaltet ein Auskunftsrecht über gespeicherte Daten, Zweck und Rechtsgrundlage der Speicherung, Herkunft der Daten und den Empfänger von Übermittlungen.

1247 *Unger/Siefken*, in: Böhrenz/Unger/Siefken, § 30 Nds.SOG, Anm. 15, wobei beim Begriff der „unvermeidbar betroffenen Dritten“ auf § 34 Abs. 1, Satz 2 Nds.SOG abgestellt wird, der jedoch identisch ist mit der Formulierung in § 33 a Abs. 2, Satz 3 und § 33 b Abs. 1, Satz 2 Nds.SOG.

1248 § 30 Abs. 4, Sätze 3 und 4 Nds.SOG. Bei der Erfüllung der Unterrichtungspflicht ist keine bestimmte Frist vorgeschrieben. Die Polizeibehörde hat bei dem ihr eingeräumten Beurteilungsspielraum auch den Zeitpunkt zu prüfen, zu dem eine Unterrichtung erfolgen kann, ohne den Zweck der Maßnahme, nicht aber die polizeiliche Aufgabenerfüllung insgesamt, zu gefährden, *Unger/Siefken*, in: Böhrenz/Unger/Siefken, § 30 Nds.SOG, AB 30.4.

1249 Gemäß § 30 Abs. 5 Nds.SOG unterbleibt die Unterrichtung, solange Zwecke der Verfolgung einer Straftat entgegenstehen (Nr.1), solange durch das Bekanntwerden der Datenerhebung Leib, Leben, Freiheit oder ähnlich schutzwürdige Belange einer Person gefährdet werden (Nr.2) oder solange ihr überwiegende schutzwürdige Belange einer anderen betroffenen Person entgegenstehen (Nr.3).

1250 Vgl. BVerfGE 113, 349 (390). Durch das Gesetz zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung, Nds.GVBl. 2007, S. 645 wurde in § 30 Abs. 5 Nr. 1 Nds.SOG 2005 die Regelung gestrichen, dass die Unterrichtung auch bei der Verfolgung einer Ordnungswidrigkeit unter-

Soll die Unterrichtung über eine Telekommunikationsüberwachungsmaßnahme nach Ablauf von sechs Monaten weiter zurückgestellt werden, so entscheidet das Amtsgericht, das die Maßnahme angeordnet oder bestätigt hat.[1251]

Auskunftsansprüche und Unterrichtungspflichten im POG ergeben sich aus § 40. Dessen Absatz 5 regelt speziell die Unterrichtung bei verdeckten Datenerhebungen. Die Benachrichtigungspflicht erstreckt sich auf die Personen, gegen die sich die Maßnahme gerichtet hat.[1252]

Ist eine Unterrichtung nach § 40 Abs. 5, Satz 1 POG auch 12 Monate nach Abschluss der Maßnahme aus gesetzlichen Gründen nicht zulässig,[1253] bedarf die weitere Zurückstellung der Unterrichtung der richterlichen Zustimmung.[1254]

§ 40 Abs. 6 POG enthält neben § 40 Abs. 5, Satz 4 POG Ausnahmen von der Unterrichtungspflicht und sieht u.a. vor, dass eine Unterrichtung unterbleibt, wenn die Daten unverzüglich nach Beendigung der Maßnahme vernichtet worden sind. Da die Telekommunikationsüberwachung jedoch gemäß § 31 Abs. 5, Satz1 POG für drei Monate angeordnet werden kann, stehen die Daten der Polizei für den Überwachungszeitraum zur Verfügung. Auch bei der Löschung von personenbezogenen Daten ist sicher zu stellen, dass Rechtsschutzmöglichkeiten des Betroffenen nicht vereitelt werden.[1255]

Die Unterrichtungspflicht bei verdeckten Datenerhebungen ergibt sich für Hessen aus § 29 Abs. 6 HSOG. Danach sind die betroffenen Personen nach Abschluss der Maßnahme über

---

bleibt. Warum hier der Gesetzgeber nicht die Möglichkeit genutzt hat, die Regelungen vollständig den Vorgaben der BVerfG anzupassen, vgl. BVerfGE 113, 348 (390), ist nicht verständlich.

1251 So die Regelung in § 30 Abs. 5, Satz 3 Nds.SOG. Zu den Zurückstellungsfristen vgl. § 30 Abs. 5, Sätze 4 und 5 Nds.SOG. Der niedersächsische Gesetzgeber hat diese Regelungen, die durch das Gesetz zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung, Nds.GVBl. 2007, S. 645, eingefügt wurden, aufgrund der Urteils des BVerfG zum Nds.SOG 2005 aufgenommen, vgl. LT-Drucks. Nds. 15/3810, S. 26.

1252 Dem Wortlaut nach sind dies die in §§ 4, 5 und 7 POG bezeichneten Personen. Sonstige Personen, also z.B. unvermeidbar betroffenen Dritte, sind nach Maßgabe des § 40 Abs. 5, Satz 2 POG zu unterrichten, soweit eine Datenerhebung nach § 29 POG erfolgt ist oder besonders schutzwürdige Interessen dies erfordern. Als besonders schutzwürdiges Interesse wird z.B. angesehen, wenn durch die Datenerhebung ein besonders geschütztes Vertrauensverhältnis berührt wird, vgl. *Roos*, § 40 POG, Rn. 13.

1253 Vgl. § 40 Abs. 5, Satz 4 und Abs. 6 POG.

1254 Entsprechendes gilt nach Ablauf von jeweils 12 weiteren Monaten. Über die Zustimmung entscheidet das Gericht, das für die Anordnung der Maßnahme zuständig gewesen ist, vgl. § 40 Abs. 5, Sätze 6 und 7 POG.

1255 Etwas anderes gilt dann, wenn die Daten unverzüglich nach der Aufzeichnung gelöscht wurden. Vgl. auch die Ausführungen in diesem Kapitel unter II. 6.

die Datenerhebung zu informieren. „Betroffen“ sind dabei die Personen, gegen die sich die Maßnahme gerichtet hat, deren Gesprächspartner sowie der Inhaber einer Wohnung in den Fällen des § 15 Abs. 4 HSOG.[1256] Im Falle der präventiven Telekommunikationsüberwachung sind dies der jeweilige Anschlussinhaber, der Störer sowie deren Gesprächspartner.

Nach § 29 Abs. 6, Satz 3 HSOG unterbleibt die Maßnahme endgültig, soweit dies im überwiegenden Interesse des Maßnahmeadressaten liegt[1257] oder wenn die Ermittlung der betroffenen Person oder deren Anschrift einen unverhältnismäßigen Verwaltungsaufwand erfordern würde.[1258] Ein unverhältnismäßiger Verwaltungsaufwand allein vermag das Unterbleiben der Unterrichtung jedoch nicht zu rechtfertigen, da damit nicht der Schutz eines überragend wichtigen Rechtsguts im Raum steht. Auch hier ist zu fordern, dass durch die Adress- oder Identitätsermittlung weitere Grundrechtseingriffe zu befürchten sind, etwa wenn alle Mobilfunkteilnehmer ermittelt werden sollen, deren Mobiltelefone sich in die von einem IMSI-Catcher simulierte Funkzelle eingeloggt haben.

Die Entscheidung über die Zurückstellung oder das Unterbleiben der Unterrichtung trifft die Behördenleitung oder einer von dieser beauftragter Bediensteter. Über die Zurückstellung der Unterrichtung ist der Hessische Datenschutzbeauftragte spätestens sechs Monate nach Abschluss der Maßnahme und danach in halbjährlichen Abständen in Kenntnis zu setzen.[1259] Eine gerichtliche Überprüfung ist nicht vorgesehen.

e) Die Kontrolle durch staatliche Organe und Hilfsorgane

Auch die weiter untersuchten Polizeigesetze haben die Anordnung der Telekommunikationsüberwachung unter einen Richtervorbehalt gestellt.[1260] Weiter erfolgt grundsätzlich eine Benachrichtigung, so dass der Rechtsweg offen steht.[1261]

1256 § 29 Abs. 6, Satz 2 HSOG.

1257 Ein überwiegendes Interesse des Maßnahmeadressaten liegt nach Ansicht des Gesetzgebers vor, wenn sich durch die Unterrichtung der Grundrechtseingriff intensiviert, etwa dass ein Dritter durch die Unterrichtung erstmals von den Maßnahmen gegen die Zielperson erfahren würde, vgl. LT-Druck. Hessen 16/2352, S. 24.

1258 Eine Unterrichtung kann ferner zurückgestellt werden, solange sie den Zweck der Maßnahme, ein sich anschließendes Ermittlungsverfahren oder Leib, Leben oder Freiheit einer Person gefährden würde, vgl. § 29 Abs. 6, Satz 4 HSOG.

1259 § 29 Abs. 6, Satz 6 HSOG.

1260 § 34 a Abs. 2 ThPAG; § 33 a Abs. 4 Nds.SOG; § 31 Abs. 5 POG; § 15 a Abs. 4 HSOG.

1261 § 34 a Abs. 3, Satz 3 iVm § 34 Abs. 7 ThPAG; § 30 Abs. 4 und 5 Nds.SOG; § 40 POG; § 29 Abs. 6 HSOG.

Eine zusätzliche parlamentarische Kontrolle ist in Thüringen und Niedersachsen sowie teilweise in Rheinland-Pfalz vorgesehen.[1262] Sie dient dazu, die Vorgehensweise der Polizei zu überprüfen und Kenntnisse über die Effektivität der Maßnahme zu sammeln.[1263]

f) Die Löschungspflicht

Das ThPAG sieht pauschal eine Löschungspflicht vor, wenn der Zweck der Maßnahme erreicht ist oder nicht erreicht werden kann[1264].

Die Regelung, dass die Telekommunikationsdaten zu löschen sind, wenn sie nicht mehr gebraucht werden oder nicht mehr erforderlich sind, enthalten auch die Polizeigesetze der Länder Niedersachsen, Rheinland-Pfalz und Hessen.[1265] Sie sehen aber im Gegensatz zum ThPAG differenzierte Löschungspflichten vor.

Eine Löschung nach § 39 a Nds.SOG unterbleibt, wenn Grund zu der Annahme besteht, dass schutzwürdige Belange der betroffenen Person beeinträchtigt würden.[1266] Findet die Ausnahmeregelung Anwendung, sind die personenbezogenen Daten zu sperren.[1267] Für die Löschung von Daten, die den Kernbereich privater Lebensgestaltung betreffen, gelten die Regelungen der §§ 33 a Abs. 3 und 35 a Abs. 3, Sätze 2 und 3 Nds.SOG.

1262 Nach § 34 a Abs. 3, Satz 3 ThPAG unterrichtet die Landesregierung den Landtag jährlich über die nach § 34 a Abs. 1 ThPAG durchgeführten Maßnahmen. In Niedersachsen ist eine Regelung in § 37 a Nds.SOG enthalten. § 31 Abs. 7, Satz 2 POG verweist nur bezüglich der Inhaltsdatenerhebung auf § 29 Abs. 12 POG. Im Gegensatz zur Auskunftserteilung sieht der Gesetzgeber eine Unterrichtung bei der Inhaltsüberwachung wegen des besonders grundrechtsrelevanten Eingriffs als notwendig an, vgl. LT-Drucks. 14/2287, S. 48. Das PAG und HSOG sehen eine Kontrolle durch staatliche Organe und Hilfsorgane nur für die Wohnraum- nicht auch für die Telekommunikationsüberwachung vor.

1263 Siehe LT-Drucks. Th. 3 /2128, S. 37.

1264 Dies ergibt sich aus dem Verweis in § 34 a Abs. 3, Satz 2 ThPAG auf § 44 Abs. 3 ThPAG. § 44 Abs. 3 ThPAG lautet: Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten Daten auf dem Datenträger zu löschen und die Unterlagen, soweit sie nicht für ein mit dem Sacherhalt zusammenhängendes Verfahren erforderlich sind, zu vernichten. Über die getroffenen Maßnahmen ist eine Niederschrift anzufertigen. Diese Niederschrift ist gesondert aufzubewahren, durch technische oder organisatorische Maßnahmen zu sichern und am Ende des Kalenderjahres, das dem Jahr der Vernichtung der Unterlagen nach Satz 1 folgt, zu vernichten.

1265 § 39 a Nds.SOG; § 39 Abs. 2 und 3; § 31 Abs. 8 POG; § 27 Abs. 2 HSOG.

1266 Schutzwürdige Belange liegen nach dieser Regelung insbesondere dann vor, wenn der Betroffene über die Maßnahme noch nicht unterrichtet wurde und die Daten für die Erfolgsaussichten eines Rechtsbehelfs gegen die Maßnahme von Bedeutung sein können. Eine allgemeingültige und abschließende Aussage scheidet jedoch aus, da die schutzwürdigen Belange durch die vom Grundgesetz geschützte Persönlichkeit geprägt werden und sich daher von Person zu Person unterscheiden, vgl. *Meixner/Fredrich*, § 27 HSOG, Rn. 20.

1267 D.h. sie dürfen nicht genutzt und verarbeitet werden, sondern erhalten eine Kennzeichnung, vgl. *Unger/Siefken*, in: Böhrenz/Unger/Siefken,§ 39 a Nds.SOG, Anm. 3.

Regelungen zur Sperrung und Löschung von Daten finden sich für Rheinland-Pfalz in § 39 Abs. 2 und 3 POG, speziell für Telekommunikationsdaten in § 31 Abs. 8 POG[1268]. Wie das Verhältnis dieser Regelungen zu einander zu bestimmen ist, sagt das Gesetz nicht. § 31 Abs. 8 POG ist aber als zeitlich späteres Gesetzes und nach Sinn und Zweck als lex specialis zu § 39 Abs. 2 Nr. 3 POG anzusehen, so dass nicht erst nach Ablauf von Überprüfungsfristen[1269] oder einer (zufälligen) Einzelfallbearbeitung eine Löschung stattzufinden hat. Die Regelung des § 39 Abs. 3 Nr. 1 POG über die Sperrung von Daten anstatt deren Löschung, wenn Tatsachen die Annahme rechtfertigen, dass schutzwürdige Interessen des Betroffenen beeinträchtigt würden, dürfte dagegen weiter anzuwenden sein, da nur so dem Betroffenen ein effektiver Rechtsschutz gewährleistet werden kann.[1270]

Gemäß § 27 Abs. 7 Nr. 2 HSOG dürfen Daten nicht gelöscht werden, sondern sind zu sperren, solange noch keine Unterrichtung der betroffenen Personen erfolgt ist. Gesperrte Daten dürfen ausschließlich zur Unterrichtung der betroffenen Person und zur gerichtlichen Kontrolle verarbeitet werden.[1271] Nach der Unterrichtung bewahrt die Behörde die Unterlagen noch eine gewisse Zeit gemäß § 27 Abs. 6 Satz 1 Nr. 1 HSOG gesperrt auf, um sie dann, wenn die betroffenen Personen keinen Rechtsschutz in Anspruch nehmen, nach § 27 Abs. 2 HSOG zu löschen.[1272]

g) Die Dokumentationspflicht

Die Dokumentationspflicht, die das BVerfG als Vorkehrung zum Schutz des Fernmeldegeheimnisses aus der Verfassung herleitet, ist lediglich ansatzweise im ThPAG normiert, denn

---

[1268] § 31 Abs. 8 POG lautet: Sind durch die Maßnahmen erlangte Unterlagen nicht mehr erforderlich, so sind sie unverzüglich unter Aufsicht des behördlichen Datenschutzbeauftragten zu vernichten. Über die Vernichtung ist eine Niederschrift anzufertigen.

[1269] Vgl. §§ 33 Abs. 3; 41 Abs. 2 Nr. 10 POG.

[1270] Vgl. *Roos*, § 39 POG, Rn. 6. Keine Ausnahme ist dagegen für die Sperrung der Daten zur Behebung einer Beweisnot und deren einhergehende Nutzung zu diesem Zweck zu machen, da § 31 Abs. 7 iVm § 29 Abs. 5 POG speziell die Zweckbindung bzw. –änderung für Telekommunikationsdaten regelt und diese Möglichkeit nicht vorsieht. Eine Sperrung zur Nutzung zu wissenschaftlichen Zwecken ist nur vertretbar, wenn die Daten anonymisiert werden.

[1271] § 27 Abs. 7, Satz 2 HSOG.

[1272] Vgl. LT-Drucks. Hessen 16/2352, S. 23. Eine weitere Ausnahme vom Löschungsgebot wird gemacht, wenn die erhobenen Daten zu Beweiszwecken unerlässlich sind. In Beweisnot kann sich die speichernde Gefahrenabwehr- oder Polizeibehörde oder die betroffene Person befinden. Beweisnot liegt vor, wenn ein entscheidungserheblicher Beweis in einem an Beweisgrundsätze gebundenen Verfahren ohne Verwendung der gespeicherten Daten nicht erbracht werden kann, ihre Verarbeitung also unerlässlich ist, vgl. *Meixner/Fredrich*, § 27 HSOG, Rn. 21. Diese Regelung dürfte nicht auf Daten aus einer präventiven Telekommunikationsüberwachung anzuwenden sein. Denn diese sind zweckgebunden sowohl was ihre Verarbeitung, als auch ihre Übermittlung angeht, § 20 Abs. 3, § 21 Abs. 3 HSOG.

§ 44 Abs. 3 ThPAG sieht die Anfertigung einer Niederschrift über die Löschung der Daten und Vernichtung der Unterlagen vor.[1273]

In § 40 Abs. 1, Satz 2 Nds.SOG ist nur geregelt, dass die Übermittlung personenbezogener Daten zu einem anderen Zweck aktenkundig zu machen ist. Für Kommunikationsdaten, die den Kernbereich privater Lebensgestaltung betreffen, gilt jedoch eine Dokumentationspflicht bezüglich der Erhebung und Löschung dieser Daten.[1274]

Nach § 29 Abs. 9, Satz 4 POG muss die Zweckänderung der Daten im Einzelfall festgestellt und dokumentiert werden.[1275] Über die Löschung der Telekommunikationsdaten ist gemäß § 31 Abs. 8 POG eine Niederschrift zu fertigen.

§ 21 Abs. 1, Satz 2 HSOG sieht vor, dass die Gefahrenabwehr- und Polizeibehörden bei der Datenübermittlung den Empfänger, Tag und wesentlichen Inhalt der Übermittlung festzuhalten haben. Werden Daten gesperrt, ist ein gemäß § 27 Abs. 3, Satz 3 HSOG entsprechender Vermerk anzubringen.[1276] Nach § 27 Abs. 2, Satz 1 Nr. 3 HSOG ist über die Löschung von Daten, die durch eine verdeckte Datenerhebung gewonnen wurden, eine Niederschrift anzufertigen.

3. Fazit

Die Polizeigesetze der hier untersuchten Länder enthalten zwar differenzierte Regelungen für die Datenverarbeitung, allerdings wurde bei der Einführung der präventiven Telekommunikationsüberwachung versäumt, diese (vollständig) den spezifischen verfassungsrechtlichen Anforderungen anzupassen, die an die Verarbeitung von Daten zu stellen sind, die durch einen Eingriff in das Fernmeldegeheimnis erlangt wurden.

1273 Die lediglich für die Vernichtung vorgesehene Protokollierung reicht für die rechtsstaatlich gebotene Kontrolle nicht aus. Sie erlaubt keine Kontrolle der Datenübermittlung durch die dafür bestimmten Gremien oder im Wege des Gerichtsschutzes, vgl. BVerfGE 110, 33 (75).

1274 § 33 a Abs. 3, Satz 3 iVm § 35 a Abs. 2, Satz 3 Nds.SOG.

1275 Dadurch soll ein missbräuchlicher Umgang mit den Daten vermieden werden, vgl. *Roos*, § 29 POG, Rn. 11; so auch LT-Drucks. 14/2287, S. 46.

1276 Stellt die Gefahrenabwehr- oder die Polizeibehörde fest, dass unrichtige oder nach § 27 Abs. 2, Satz 1 Nr. 1 HSOG zu löschende oder nach § 27 Abs. 3, Satz 1 zu sperrende personenbezogene Daten übermittelt worden sind, ist dem Empfänger die Berichtigung, Löschung und Sperrung mitzuteilen.

Die (teilweise) unzureichende Umsetzung der Rechtsprechung des BVerfG ist umso überraschender, da das BND-Urteil über zwei Jahre vor der Änderung des ThPAG, das als erstes Landespolizeigesetz eine präventive Telekommunikationsüberwachung vorsah, erlassen wurde.[1277] Die Gesetzesbegründungen der Länder Thüringen und Niedersachsen erwähnen diese Entscheidung auch mit keinem Wort, sondern beziehen sich lediglich auf die Entscheidungen des SächsVerfGH[1278] und des BayVerfGH[1279], welche die Vereinbarkeit der jeweiligen landespolizeigesetzlichen Datenschutzregelungen – u.a. vor dem Hintergrund der Wohnraumüberwachung – mit der für sie einschlägigen Landesverfassung überprüfen.[1280] Auch die anderen Gesetzgeber betonen zwar in den Gesetzesbegründungen immer wieder, dass insbesondere auch die Vorgaben des BVerfG zur Datenverarbeitung eingearbeitet und berücksichtigt worden seien[1281], in den Gesetzestexten schlägt sich dies aber kaum nieder. In dieser Hinsicht besteht Handlungsbedarf des Gesetzgebers. Zwar darf der Datenschutz nicht zum Täterschutz werden[1282], doch sind den Grundrechtseingriffen durch die verdeckte Datenerhebung Rechnung zu tragen. Dies proklamieren auch die Entscheidungen der Landesverfassungsgerichte.[1283]

1277 Das BND-Urteil wurde am 14.07.1999 erlassen. Der Gesetzentwurf für das ThPAG stammt vom 15.01.2002, der Gesetzentwurf aus Niedersachsen vom 07.06.2003.

1278 SächsVerfGH DVBl. 1996, 1423 ff. = JZ 1996, 957 ff. = LKV 1996, S. 273 ff.

1279 BayVerfGH JZ 1995, 299 ff. = BayVBl. 1995, 143 ff.

1280 Der niedersächsische Landesgesetzgeber führt die Entscheidungen als Argumente an, um die im NGefAG vorhandenen Datenschutzregelungen aufzuweichen, LT-Drucks. 15/240, S. 21. Der thüringer Gesetzgeber erwähnt die Entscheidungen im Rahmen des § 34 ThPAG, LT-Drucks. 3/2128, S. 30.

1281 Vgl. LT-Drucks. RhPf 14/2287, S. 31; LT-Drucks. Hessen 16/2352, S. 11.

1282 Vgl. BVerfGE 65, 1 (44); BVerfG EuGRZ 2001, 249 (252); BayVerfGH BayVBl. 1995, 143 (144); *Di Fabio*, in: Maunz/Dürig, Art. 2 Abs. 1 GG, Rn. 181; *Starck*, in: v.Mangoldt/Klein/Starck (Hrsg.), Art. 2 Abs. 1 GG, Rn. 116; *Murswiek*, in: Sachs (Hrsg.), Art. 2 Abs. 1 GG Rn. 121.

1283 So lautet LS 11 des SächsVerfGH, JZ 1996, 957: „Soweit die Polizei mit verdecktem Einsatz besonderer Mittel, insbesondere in oder aus Wohnungen, Daten erhebt und damit heimlich in die Grundrechte auf informationelle Selbstbestimmung und auf Unverletzlichkeit der Wohnung eingreift, reicht der herkömmliche Grundrechtsschutz nicht aus. Daher bedarf es insoweit einer besonderen Ausgestaltung des Grundrechtsschutzes durch Verfahrensregeln, die den individualrechtlichen wie den strukturellen Schutzbedürfnissen gerecht werden müssen."

Kapitel 7: Zusammenfassung der Thesen

Mit der Einführung der präventiven Telekommunikationsüberwachung haben sich die Landesgesetzgeber den jüngsten Herausforderungen an eine effektive Gefahrenabwehr gestellt. Ist es dabei für den Schutz der Bürger notwendig Grundrechte einzuschränken, so ist stets zu beachten, dass „der Zweck nicht jedes Mittel heiligt". Auch wenn zur Sicherheit der Bürger entschieden gegen die Gefahren der Organisierten Kriminalität und des internationalen Terrorismus vorgegangen werden muss, sind die verfassungsrechtlichen Grenzen zu beachten und die Ermächtigungsgrundlagen unter Berücksichtigung dieser Vorgaben sorgfältig zu überprüfen. Keines der hier untersuchten Landesgesetze entspricht bislang vollständig den Vorgaben des Grundgesetzes und der verfassungsgerichtlichen Rechtsprechung.

I. Das Erfordernis einer eigenen Datenerhebung

Mit den hier untersuchten §§ 34 a ThPAG; 33 a – 33 c Nds.SOG; Art. 34 a – 34 c PAG; §§ 31 POG und 15 a HSOG ist den jeweiligen Landespolizeibehörden die Telekommunikationsüberwachung als Maßnahme zur Gefahrenabwehr eröffnet worden.

Obgleich (übermittelte) Telekommunikationsdaten den Gefahrenabwehrbehörden auch schon zur Verfügung stehen, wenn die Landespolizeigesetze das Zitiergebot beachten[1284] und spezielle Ermächtigungsgrundlagen für die Datenübermittlung vorsehen[1285], ist eine originäre Datenerhebung nicht überflüssig. Die präventive Telekommunikationsüberwachung ist eingeführt worden, um der Organisierten Kriminalität, dem internationalen Terrorismus aber auch Selbstgefährdungen wirksam begegnen zu können.[1286] Um auf diese konkreten Gefahrensituationen reagieren zu können, ist eine eigene Datenerhebung notwendig. Für eine effektive Gefahrenwehr ist es nach der hier vertretenen Auffassung nicht ausreichend, lediglich auf übermittelte Daten angewiesen zu sein.[1287]

1284 So für § 38 PolG BW *Würtenberger/Heckmann*, 2005, Rn. 651; *W.-R. Schenke*, 2005, Rn. 209; *R.P. Schenke*, in: FG für Hilger, S. 221 f.

1285 Vgl. *R.P. Schenke*, in: FG für Hilger, S. 218 f.; *W.-R. Schenke*, JZ 2001, 997 (1002 ff.), die ausdrücklich auf die Anforderungen des BVerfG aus dem BND-Urteil verweisen (BVerfGE 100, 393 ff.).

1286 Vgl. LT-Drucks. Th. 3/2128, S. 1; LT-Drucks. Nds. 15/240, S. 8; LT-Drucks. Bayern 15/2096, S. 2; LT-Drucks. RhPf. 14/2287, S. 30.

1287 Zur Begründung vgl. das Kapitel „Entwicklung und bisherige gesetzliche Grundlagen der Telekommunikationsüberwachung in der Bundesrepublik Deutschland" unter V.

II. Die Gesetzgebungskompetenz der Länder

Mit der Aufnahme der Telekommunikationsüberwachung in die Polizeigesetze ist eine eigene Rechtsgrundlage für die Datenerhebung geschaffen worden, so dass sich der Zu- und Rückgriff auf einen polizeilichen Notstand erübrigt.[1288]

Die Anordnung gegenüber den Diensteanbietern auf Auskunftserteilung und Überwachungsermöglichung ist den Polizeibehörden möglich, da die einschlägigen Polizeigesetze Gesetze im Sinne des § 88 Abs. 3, Satz 3 TKG sind.[1289] Die Gesetzgebungskompetenz der Länder ist gegeben, da mit der Telekommunikationsüberwachung zu präventiven Zwecken materielles Polizeirecht geregelt wird. Von der Gesetzgebungskompetenz ist nicht nur die Telekommunikationsüberwachung zur Abwehr von Gefahren umfasst, sondern auch die Überwachung zur vorbeugenden Bekämpfung von Straftaten, zu der nicht nur die Verhinderungsvorsorge, sondern nach der hier vertretenen Auffassung auch die Verfolgungsvorsorge zählt.[1290]

Selbst wenn man mit dem BVerfG[1291] davon ausgehen wollte, dass die Verfolgungsvorsorge in den Bereich der konkurrierenden Gesetzgebung fällt, ist eine landesgesetzliche Regelung nicht ausgeschlossen, da der Bundesgesetzgeber durch die Vorschriften der §§ 100 a ff. StPO nicht abschließend von seiner Gesetzgebungskompetenz Gebrauch gemacht hat.[1292]

III. Die grenzüberschreitende Überwachung

Die präventive Telekommunikationsüberwachung ist durch die jeweilige landesgesetzliche Regelung nicht auf das „Anordnungsbundesland“ beschränkt, da den Ermächtigungsgrundlagen in den Landespolizeigesetzen bundesweite Geltung zukommt. Zweck der Maßnahme ist die Gefahrenabwehr im „Anordnungsland“. Dazu kann es aufgrund der technischen und tatsächlichen Gegebenheiten notwendig sein, auch Personen und Anschlüsse zu überwachen, die sich nicht im „Anordnungsland“ befinden.[1293]

1288 Vgl. das Kapitel „Entwicklung und bisherige gesetzliche Grundlagen der Telekommunikationsüberwachung in der Bundesrepublik Deutschland“ unter IV.
1289 Siehe dazu die Formulierungen in § 110 Abs. 1, Satz 6 TKG und § 1 Nr. 1 d) TKÜV.
1290 Vgl. das Kapitel „Der Zugriff auf die Telekommunikationsdaten“ unter IV. 1.
1291 Vgl. BVerfGE 113, 349 (369 f.).
1292 Vgl. Kapitel „Der Zugriff auf die Telekommunikationsdaten“ unter IV.1.
1293 Vgl. das Kapitel „Länderübergreifende Sachverhalte“.

Zwar verpflichtet der Grundsatz des bundesfreundlichen Verhaltens die Länder untereinander bei der Inanspruchnahme ihrer Rechte die gebotene Rücksicht auf die Belange der anderen Mitglieder der bundesstaatlichen Rechtsverhältnisse zu nehmen und nicht rücksichtslos ihre eigenen Rechtspositionen durchzusetzen.[1294] Die Hoheitsgewalt anderer Bundesländer wird durch die länderübergreifende Telekommunikationsüberwachung aber nicht beeinträchtigt.[1295] Vielmehr hat das betroffene Bundesland nach der hier vertretenen Auffassung die Telekommunikationsüberwachung zu dulden, da überwiegende Belange des „Anordnungsbundeslandes“ gegeben sind und die Versagung der länderübergreifenden Telekommunikationsüberwachung zu einer gravierenden Störung der bundesstaatlichen Ordnung führen würde.[1296] Das „Anordnungsbundeslandes“ nimmt mit der präventiven Telekommunikationsüberwachung den Schutzauftrag aus Art. 2 Abs. 2 GG gegenüber seinen Einwohnern wahr. Würde ihm die Telekommunikationsüberwachung bei einer Gefahrenlage innerhalb seines Territoriums versagt werden, da die Kommunikation in einem anderen Bundesland stattfindet, hätte es das andere Bundesland in der Hand, eine effektive Gefahrenabwehr zu verhindern und damit die Erfüllung einer durch das Grundgesetz auferlegten Pflicht zu vereiteln. Dem anderen Bundesland steht es aufgrund der telekommunikationsrechtlichen Regelungen dagegen offen, jederzeit selbst eine Überwachung des betroffenen Anschlusses zu verlangen.[1297] Auch ein körperliches Eindringen in sein Hoheitsgebiet findet nicht statt.[1298]

Der Überwachung in einem anderen Bundesland stehen auch nicht subjektive Rechte Dritter entgegen. Ist eine Person für eine Gefahr in einem Bundesland verantwortlich, so kann die zuständige Behörde gegen sie einschreiten unabhängig davon, ob die (verhältnismäßig) eingesetzten Mittel auch den Gefahrenabwehrbehörden seines „Wohnsitzlandes“ zur Verfügung stehen, da die demokratische Legitimation des Normgebers grundsätzlich für sein Hoheitsgebiet besteht [1299] und im diesem die Gefahrlage gegeben ist.

1294 Vgl. BVerfGE 34, 216 (232); BVerwGE 50, 137 (148);. *Bauer*, 1992, S. 356; *Isensee*, in: HStR IV, § 98, Rn. 157 f.

1295 Vgl. Kapitel „Länderübergreifende Sachverhalte“ unter V. 3. b) dd).

1296 Vgl. Kapitel „Länderübergreifende Sachverhalte“ unter V. 3. b) dd). Denn das eine Bundesland könnte dann die effektive Gefahrenabwehr durch ein anderes Bundesland verhindern.

1297 Sollte das betroffene Bundesland am überwachten Telekommunikationsanschluss Überwachungsmaßnahmen durchführen wollen, so ist ihm das – bei Vorliegen der jeweiligen Voraussetzungen – ohne weiteres möglich, vgl. § 6 Abs. 4 TKÜV.

1298 Dies gilt jedenfalls solange es nicht zum Einsatz des IMSI-Catchers auf fremden Territorium kommt.

1299 Vgl. Kapitel „Länderübergreifende Sachverhalte“ unter V. 3. c).

IV. Die verfassungsrechtlichen Vorgaben

1. Telekommunikationsüberwachung zur Gefahrenabwehr

Müssen den Polizeibehörden Maßnahmen für eine effektive Gefahrenabwehr zur Verfügung stehen, so darf nicht unbeachtet bleiben, dass die Aufzeichnung und Überwachung der Telekommunikation in die Grundrechte der von den Maßnahmen – auch unvermeidlich – Betroffenen eingreift. Die Telekommunikationsüberwachung ist daher nach der hier vertretenen Meinung nur bei einer gegenwärtigen Gefahrenlage für überragend wichtige Rechtsgüter zulässig.[1300] Dies sind Leben, Freiheit und Gesundheit einer Person, nicht aber bloße Sachgefahren, wie es die Regelung des Art. 34 a PAG vorsieht.

2. Telekommunikationsüberwachung zur Straftatenverhinderung

Auch die Telekommunikationsüberwachung zur Verhinderung bevorstehender Straftaten bedarf einschränkender Tatbestandsmerkmale sowohl im Hinblick auf den Begehungsverdacht, als auch hinsichtlich des Straftatenkataloges. Gerade im Bereich der Vorfeldermittlungen müssen Anhaltspunkte für das Zeitmoment der möglichen Tatbegehung gegeben sein, schon um den Anforderungen des Bestimmtheitsgrundsatzes zu genügen.[1301]

Darüber hinaus muss der Gesetzgeber eine eigene Entscheidung darüber treffen, welche Straftaten er als gewichtig genug ansieht, um das Fernmeldegeheimnis einzuschränken. Eine Orientierung kann dabei am Strafrahmen erfolgen, wie es das BVerfG für die strafprozessuale Wohnraumüberwachung vorgenommen hat (argumentum a maiore ad minus).[1302]

1300 Vgl. hierzu *Würtenberger/Heckmann*, 2005, Rn. 625 c für eine mögliche Regelung in Baden-Württemberg, welche die Ansicht vertreten, dass die polizeirechtliche Eingriffsermächtigung zur Telekommunikationsüberwachung ebenso wie die Ermächtigung zum Lauschangriff nach Art. 13 Abs. 4 GG ausgestaltet werden kann (argumentum a maiore ad minus).

1301 Vgl. BVerfGE 110, 33 (55 f.); BVerfGE 113. 349 (379).

1302 Vgl. BVerfGE 109, 279 (346 ff.). So orientierten sich auch die in Art. 30 Abs. 5 PAG aufgezählten Straftaten an einer höheren Höchststrafe als fünf Jahre, vgl. LT-Drucks. Bayern 15/2096, S. 31 mit dem Hinweis, dass wenn Straftaten aufgenommen wurden, die diesen Strafrahmen unterschreiten, es sich dabei um Straftaten handelt, die einen besonderen Bezug zur Organisierten Kriminalität aufweisen. Der Gesetzentwurf zur Telekommunikationsüberwachung und anderen verdeckten Ermittlungsmaßnahmen vom 18.04.2007 sieht vor, den Katalog von Straftaten, die Anlass für eine Telekommunikationsüberwachungsmaßnahme sein können, auf schwere Straftaten zu beschränken. Dabei orientiert sich der Gesetzesentwurf auch an einer Mindesthöchststrafe von 5 Jahren Freiheitsstrafe, vgl. BT-Drucks. 16/5846, S. 40 ff.

Gewichtige Rechtsgüter sind vor allem das Leben, die Gesundheit und die persönliche Freiheit.[1303] Da die Telekommunikationsüberwachung der Bekämpfung der Organisierten Kriminalität dienen soll, ist die banden- und gewerbsmäßige Begehung von Straftaten entsprechend zu berücksichtigen. [1304] Darüber hinaus darf nicht unberücksichtigt bleiben, dass nur Straftaten aufzuführen sind, bei denen die Telekommunikationsüberwachung ein erforderliches und angemessenes Mittel zur Verhütung oder Verfolgung von Straftaten sein kann.[1305]

Bei den polizeilichen Datenerhebungen ist zudem an die Möglichkeit zu denken, die unterschiedlichen Eingriffe in das Telekommunikationsgeheimnis – ähnlich der StPO – alternativ zu gestalten, wie es in Niedersachsen schon für die Aufzeichnung und Überwachung der Telekommunikation und den Einsatz des IMSI-Catchers vorgesehen ist.[1306] So könnten auch für die Inhaltsüberwachung und Auskunftserteilung differenzierte Eingriffsvoraussetzungen vorgesehen werden.[1307]

3. Überwachungsobjekt

Eine eindeutige Aussage ist darüber zu treffen, wer Betroffener im Sinne der präventivpolizeilichen Regelungen sein kann und welche Anschlüsse überwacht werden dürfen.[1308] Der Begriff der Kontakt- und Begleitpersonen ist nach der hier vertretenen Meinung dahin-

---

1303 Haben die Länder eine Kommunikationsüberwachung normiert, um dem Terrorismus und der Organisierten Kriminalität wirksam begegnen zu können, so muss sich dieser Gesetzeszweck auch im Katalog der zu verhütenden Straftaten widerspiegeln. Zulässig ist damit wie in Bayern eine Telekommunikationsüberwachung zur Verhinderung von Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaats oder des Landesverrates und der Gefährdung der äußeren Sicherheit, von Straftaten gegen die öffentliche Ordnung, von Straftaten gegen die sexuelle Selbstbestimmung, das Leben und die persönliche Freiheit und zur Verhinderung von Verbrechen gegen die Menschlichkeit und Kriegsverbrechen. Diese Normen schützen gewichtige Rechtsgüter wie die Funktionsfähigkeit des Staates, das Leben, die Gesundheit und die Freiheit seiner Bewohner. Dabei handelt es sich nahezu ausschließlich um Verbrechen, also Straftaten, die eine Mindeststrafe von einem Jahr Freiheitsstrafe vorsehen.

1304 Z.B. bei Straftaten nach dem Waffengesetz, dem Betäubungsmittelgesetz oder dem Gesetz über die Kontrolle von Kriegswaffen. Diese werden verstärkt durch kriminelle Organisationen begangen. So stellt auch Art. 30 Abs. 5 Nr. 8 – 10 PAG auf die banden- oder gewerbsmäßige Begehung ab. Die Organisierte Kriminalität zeigt sich nicht nur im Bereich des internationalen Rauschgifthandels, sondern in zahlreichen Kriminalitätsbereichen wie Waffenhandel, Falschgeldverbreitung, Glücksspiel, Prostitution und Menschenhandel, Schutzgelderpressung etc., vgl. *Körner/Scherp*, § 30 b BtMG, Rn. 10.

1305 Vgl. BVerfGE 113, 349 (388).

1306 § 33a Nds.SOG regelt die Überwachungsermöglichung und Auskunftserteilung, § 33 b Nds. SOG den Einsatz des IMSI-Catchers. Diese Ermächtigungsgrundlagen sehen unterschiedliche Voraussetzungen vor.

1307 Angedacht werden kann dabei, dass die Kenntnis über den Gesprächsinhalt einen intensiveren Eingriff in das Fernmeldegeheimnis bedeutet, als die bloße Auskunftserteilung über Verkehrsdaten und dementsprechend die jeweiligen Eingriffsvoraussetzungen gestaltet werden.

1308 Vgl. BVerfGE 113, 349 (380), welches bei Kontakt- und Begleitpersonen eine Konkretisierung dahin fordert, dass klar sein muss, wer im Vorfeld mit dem potenziellen Straftäter so in Verbindung steht, dass Hinweise über die angenommene Straftat gewonnen werden können.

gehend zu präzisieren, dass dies Personen sind, die für den potenziellen Täter oder Störer Nachrichten entgegennehmen oder weiterleiten und/oder deren Anschlüsse der potenzielle Straftäter oder Störer benutzt, so dass auch eine Gutgläubigkeit der Kontakt- und Begleitperson der Anordnung nicht entgegensteht. Nach dem Vorbild der Regelung in § 31 Abs. 2, Satz 2 POG sollte festgehalten werden, dass sich die Überwachung auf Anschlüsse bezieht, die von den zu überwachenden Personen mit überwiegender Wahrscheinlichkeit genutzt werden.

4. Verfahrenssicherung

Der Richtervorbehalt sollte für die präventive Telekommunikationsüberwachung vorgesehen werden. Die Überwachungsmaßnahmen stellen gravierende Grundrechtseingriffe dar, deren Überprüfung im Nachhinein den erfolgten Eingriff, war dieser auch rechtswidrig, weder zu verhindern noch zu beseitigen vermag. Die vorgeschaltete Kontrolle, die durch ein Organ erfolgt, dass außerhalb der Eingriffsverwaltung steht, kann die durch die Maßnahmen betroffenen Grundrechte des Betroffenen nach der hier vertretenen Ansicht am ehesten wahren. Die ebenfalls in Frage kommenden Behördenleitervorbehalte sehen eine Kontrolle durch Personen innerhalb des Verwaltungsapparates vor und die Unterrichtung des Parlaments bewirkt lediglich eine nachgeschaltete Kontrollmöglichkeit.[1309]

Für einen effektiven Rechtsschutz des Betroffenen durch die richterliche Kontrolle, sollte gesetzlich festgeschrieben sein, dass die Anordnungsbeschlüsse schriftlich ergehen müssen, den Namen, die Anschrift, die Rufnummer oder eine andere Kennung seines Telekommunikationsanschlusses angeben sowie den Grund der Überwachung und ihre Unentbehrlichkeit darlegen müssen, um sicherzustellen, dass sich der jeweilige Richter mit den (verfassungs-) rechtlichen Vorgaben an die Einschränkungsmöglichkeiten des Art. 10 GG auseinander gesetzt hat. Zudem ist die Dauer der Überwachung im Beschluss festzusetzen. Bei der Fernsprechüberwachung ist außer der Bezeichnung der Rufnummer oder der Kennung des Telekommunikationsanschlusses auch anzugeben, ob und in welchem Umfang die Gespräche aufzuzeichnen, welche von mehreren Anschlüssen zu überwachen sind und ob das durchgehend oder nur zu bestimmten Tageszeiten geschehen soll.

[1309] Vgl. zur parlamentarischen Kontrolle die Regelung in § 23 Abs. 5 PolG BW. Danach in der Landtag jährlich über die Datenerhebung durch den Einsatz technischer Mittel in oder aus Wohnungen zu unterrichten.

Auch wenn diese Anforderungen bereits aufgrund des Rechtsstaatsprinzips einzuhalten sind, so ist es doch jedenfalls im Hinblick auf die Rechtssicherheit erforderlich, diese Voraussetzungen gesetzlich zu fixieren, wie es der bayerische Gesetzgeber getan hat. Ist bei Gefahr in Verzug die Anordnung durch den Behördenleiter vorgesehen, so ist ausdrücklich im Gesetz festzuhalten, dass diese außer Kraft tritt, wenn sie nicht binnen einer bestimmten Frist[1310] bestätigt wird. Auch ist sicherzustellen, dass der Behördenleitervorbehalt nur unter engen Voraussetzungen in Betracht kommt und nicht dazu verwendet wird, die richterliche Anordnung zu umgehen.[1311]

Um den Stimmen zu begegnen, die dem Richtervorbehalt eine Effektivität absprechen, da die Überprüfung der Sachlage nur aufgrund Aktenlage und ohne Anhörung des Betroffenen erfolgt, könnte – ohne verfassungsrechtlich zwingen geboten zu sein – dem Betroffenen im Anordnungsverfahren „eine Stimme geliehen“ werden. Dies könnte z.B. durch Stärkung des Datenschutzbeauftragten geschehen.[1312]

Darüber hinaus ist im Hinblick auf den Grundrechtsschutz durch Verfahren festzuschreiben, dass das Fortbestehen der Überwachungsvoraussetzungen während des gesamten Anordnungszeitraums ständig überwacht werden muss. Nach ihrem Wegfall ist die Maßnahme unverzüglich zu beenden, z.B. wenn der Gefahrenverdacht entkräftet oder die Maßnahme nicht mehr unentbehrlich oder nicht mehr aussichtsreich ist.[1313]

5. Befristung

Um der hohen Einbuße grundrechtlicher Freiheiten Rechnung zu tragen, ist die Telekommunikationsüberwachung auf ein Mindestmaß zu beschränken. Das kann dadurch erreicht wer-

---

1310 § 100 b Abs. 1, Satz 3 StPO sieht eine Frist von drei Tagen vor.

1311 In Thüringen ist dies durch eine Dienstanweisung des Innenministeriums geschehen, da durch die Berichte der Landesregierung über die präventiv-polizeiliche Telekommunikationsüberwachung gemäß § 34 a Abs. 3 ThPAG offengelegt wurde, dass bei der Auslegung des Behördenleitervorbehalts bei polizeilichen Eilanordnungen, einschließlich der Form der Eilanordnung, Defizite bestehen, vgl. LT-Drucks. 4/249, S. 3 und LT-Drucks. 4/972, S. 3 f. Dies zeigt das Erfordernis einer klaren gesetzlichen Regelung.

1312 Dem Datenschutzbeauftragten steht u.a. das Recht zu, Maßnahmen zu beanstanden, vgl. § 25 BDSG.

1313 Sowohl bei staatlichen Eingriffen als auch dort, wo der Staat die durch Art. 10 GG gewährleistete Vertraulichkeit zu schützen hat, sind regelmäßig organisatorische und verfahrensmäßige Vorkehrungen erforderlich, die die Einhaltung materieller Regelungen sichern. Zur Wirksamkeit der Kontrolle gehört es, dass sich die Kontrolle auf alle Schritte des Prozesses der Fernmeldeüberwachung erstreckt. Kontrollbedürftig ist sowohl die Rechtmäßigkeit der Eingriffe als auch die Einhaltung der gesetzlichen Vorkehrungen zum Schutz des Fernmeldegeheimnisses, vgl. BVerfGE 100, 313 (362).Von der Beendigung sind das Gericht und das Telekommunikationsunternehmen zu unterrichten.

den, dass nur eine kurze Überwachungsfrist vorgesehen wird, um alle Beteiligten anzuhalten, die Maßnahmen in kurzen Zeitabständen zu überprüfen. Auch kann nach dem Vorbild des PAG die Befristung der Anordnung differenziert anhand der Schwere der Maßnahme vorgenommen werden. Verlängerungsmöglichkeiten stehen dem nicht entgegen, da für die Verlängerungsanordnung weiter die Voraussetzungen für die Überwachung vorliegen müssen.[1314]

V. Die Anforderungen an die Datenverarbeitung

Um den Schutz des Fernmeldegeheimnisses auch nach der Datenerhebung zu gewährleisten, ist eine entsprechende Ausgestaltung der Datenweitergabe- und Datenverarbeitungsvorschriften vorzunehmen. Unabdingbare Voraussetzung für einen Grundrechtsschutz ist die Kennzeichnung der Daten. Ist dies nicht der Fall, laufen die Schutzvorschriften für die Datenweitergabe und –verarbeitung ins Leere. Erforderlich ist nicht nur, dass die erhobenen Telekommunikationsdaten zu kennzeichnen sind, sondern auch die übermittelten Daten dahin gehend zu kennzeichnen sind, dass sie aus einer Telekommunikationsüberwachung stammen.[1315]

Die Weitergabe der Daten und ihre Verarbeitung ist stets an ihren Erhebungszweck gebunden.[1316] Eine Verarbeitung und Weitergabe ist dann möglich, wenn sie auch zu diesen Zwecken hätten erhoben werden können.[1317] Sehen die Polizeigesetze unterschiedliche Voraussetzungen vor, ist eine Weitergabe zulässig, wenn die Empfängerbehörde den Grundrechtseingriff ansonsten nochmals vornehmen müsste und dürfte.

Für rechtswidrig erlangte oder nicht (mehr) benötigte Daten sind Löschungs- bzw. Sperrungsvorschriften vorzusehen. Sicherzustellen ist, dass soweit Daten aus dem Kernbereich privater Lebensgestaltung erhoben worden sind, diese nicht gespeichert und verwertet, sondern unverzüglich gelöscht werden.[1318]

1314 § 34 a Abs. 2, Satz 10 ThPAG; § 33a Abs. 4, Satz 3 Nds.SOG; Art. 34 c Abs. 3, Satz 5 PAG; § 31 Abs. 5, Satz 3 POG; § 15 a Abs. 4, Satz 4 iVm § 15 Abs. 5, Satz 7 HSOG.

1315 Vgl. *Jarass*, in: Jarass/Pieroth, Art. 10 GG, Rn. 19; *Hermes*, in: Dreier (Hrsg.), Art.10 GG, Rn. 90; *Petri*, in: Lisken/Denninger, Kapitel H. Rn. 53.

1316 Vgl. BVerfE 100, 313 (360).

1317 Vgl. BVerfGE 100, 313 (360); E 110, 33 (74 f.).

1318 Vgl. BVerfGE 113, 349 (392); *Würtenberger/Heckmann*, 2005, Rn. 625 d.

Um einen effektiven Rechtsschutz der Betroffenen zu gewährleisten, ist das Datenverarbeitungsverfahren, insbesondere die Information und ihre Zurückstellung, der richterlichen Überprüfung zu unterstellen.[1319] Eine bloße Unterrichtung des Datenschutzbeauftragten ist nicht ausreichend, da diesem lediglich die Möglichkeit der Beanstandung zukommt.

Unter welchen Voraussetzungen eine Zurückstellung in Betracht kommt, muss der Gesetzgeber präzise bestimmen.[1320] Die Benachrichtigung kann unterbleiben, solange der Zweck der Maßnahme dadurch gefährdet würde oder eine Gefahr für Leib und Leben der eingesetzten Ermittler besteht. Die bloße Gefährdung der öffentlichen Sicherheit ist für eine Zurückstellung nicht ausreichend.[1321]

Wird die Telekommunikationsüberwachung als Gefahrenabwehrmaßnahme in die Polizeigesetze integriert, sind spezielle Datenverarbeitungsvorschriften mit aufzunehmen, da die allgemeinen Verarbeitungsvorschriften den verfassungsrechtlichen Vorgaben nicht gerecht werden. Da von der Überwachung auch unbeteiligte Dritte betroffen sind, sind für die bei der Durchführung der Maßnahme anfallenden Daten Dritter eigene Regelungen zu treffen. So ist explizit festzuhalten, dass diese Daten nur erhoben werden dürfen, wenn es technisch unvermeidbar ist, sie nicht weitergeben werden dürfen und unverzüglich zu löschen sind, wenn feststeht, dass sie zur Gefahrenabwehr nicht benötigt werden.[1322]

Mag eine parlamentarische Kontrolle der präventiven Telekommunikationsüberwachung nicht zwingend geboten sein, solange ein effektiver Rechtsschutz für die Betroffenen zu erlangen ist, so ist diese nach der hier vertretenen Auffassung dennoch als Kontrollmittel vorzusehen. Denn dem Gesetzgeber eröffnet sich damit die Möglichkeit überprüfen zu können, ob seine Maßnahmen die erhoffte Wirkung erzielen und als Mittel für die Gefahrenabwehr geeignet sind. Auch kann diese Berichtspflicht dazu dienen, Defizite bei der Anwendung der gesetzlichen Vorschriften aufzuzeigen.[1323]

1319 Siehe dazu *P.M. Huber*, ThürVBl. 2005, 33 (39), der eine dauerhafte personelle Überwachung der Informationserhebung fordert.

1320 Vgl. BVerfGE 109, 279 (366).

1321 Vgl. BVerfGE 109, 279 (366).

1322 Vgl. BVerfGE 110, 33 (75). In diesem Zusammenhang ist auch eine eindeutige Regelung über Zufallsfunde zu treffen

1323 Vgl. den Bericht der Landesregierung über die präventiv-polizeiliche Telekommunikationsüberwachung im Jahr 2003 gemäß § 34 a Abs. 3 ThPAG, LT-Drucks. 4/249, S. 3.

Anhang: Anordnungsvoraussetzungen

Voraussetzungen	**§ 34 a ThPAG**	**§§ 33 a – 33 c Nds.SOG**	**Art. 34 a – 34 c PAG**	**§ 31 POG**	**§ 15 a HSOG**
1. Gefahrenlage/Schutzgüter	Es muss eine Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person bestehen.	Es muss eine gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person bestehen.	Es muss eine dringende Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leben, Gesundheit oder Freiheit einer Person oder eine gemeine Gefahr für Sachen bestehen.	Es muss eine gegenwärtige Gefahr für Leib oder Leben einer Person bestehen.	Es muss eine gegenwärtige Gefahr für Leib, Leben oder Freiheit einer Person bestehen.
2. Straftatenverhütung - Straftatenverdacht - Straftatenkatalog	Tatsachen müssen die Annahme rechtfertigen, dass Personen Straftaten im Sinn des § 100 a StPO begehen wollen.	Tatsachen müssen die Annahme rechtfertigen, dass Personen Straftaten von erheblicher Bedeutung (§ 2 Nr. 10 Nds.SOG 2005) begehen werden.	Konkrete Vorbereitungshandlungen müssen für sich oder zusammen mit weiteren bestimmten Tatsachen die begründete Annahme rechtfertigen, dass Personen schwerwiegende Straftaten (§ 30 V, 1 PAG) begehen werden.	Nicht im POG vorgesehen.	Nicht im HSOG vorgesehen.
3. Kontakt- und Begleitpersonen	Dies sind Personen, die zum potenziellen Straftäter in näherer persönlicher oder geschäftlicher Beziehung stehen oder zu ihm über einen längeren Zeitraum eine Verbindung unterhalten oder unter konspirativen Umständen hergestellt haben oder pflegen.	Dies sind nach dem Nds.SOG 2005 Personen, die mit dem potenziellen Straftäter in einer Weise in Verbindung stehen, die erwarten lässt, dass durch sie Hinweise über die angenommene Straftat gewonnen werden	Dies sind Personen, die für den potenziellen Straftäter Mitteilungen entgegennehmen oder weitergeben oder deren Kommunikationseinrichtungen der potenzielle Straftäter benutzt.	Nicht im POG vorgesehen.	Nicht im HSOG vorgesehen.

		können.			
4. IMSI-Catcher	Der Einsatz des IMSI-Catchers ist nicht vorgesehen.	Der Einsatz des IMSI-Catchers ist vorgesehen zur Abwehr einer gegenwärtigen Gefahr für Leib und Leben.	Der Einsatz des IMSI-Catchers ist unter den gleichen Voraussetzungen wie die Auskunftserteilung und Inhaltsüberwachung zulässig.	Der Einsatz des IMSI-Catchers ist unter den gleichen Voraussetzungen wie die Auskunftserteilung und Inhaltsüberwachung zulässig, es ist jedoch eine strengere Subsidiaritätsklausel vorgesehen.	Der Einsatz des IMSI-Catchers ist unter den gleichen Voraussetzungen wie die Auskunftserteilung und Inhaltsüberwachung zulässig.
5. Richtervorbehalt	Die Anordnung untersteht dem Richtervorbehalt. Bei Gefahr im Verzug entscheidet der Leiter des Landeskriminalamts oder einer Polizeidirektion.	Die Anordnung untersteht dem Richtervorbehalt. Bei Gefahr in Verzug kann die Polizei die Anordnung treffen.	Die Anordnung untersteht dem Richtervorbehalt. Bei Gefahr in Verzug genügt die Anordnung durch die in Art. 33 V, 1 PAG genannten Personen. Soll lediglich der Aufenthalt ermittelt werden, kann die Anordnung durch die Leiter der in Art. 4 II, 1 Nr. 1 – 3 POG genannten Dienststellen oder das Landeskriminalamt erfolgen.	Die Anordnung untersteht dem Richtervorbehalt. Bei Gefahr in Verzug kann die (Polizei-) Behördenleitung die Anordnung treffen.	Die Anordnung steht außer bei Gefahr in Verzug unter Richtervorbehalt.
6. Befristung	Die Auskunft über Verbindungsdaten ist rückwirkend für einen Zeitraum von 2 Monaten zulässig. Die Maßnahmen sind auf 3 Monate zu befristen.	Die Auskunft über die Verbindungsdaten ist rückwirkend für einen Zeitraum von 6 Monaten zulässig. Die Maßnahmen sind auf 3 Monate zu befristen.	Die Auskunft über die Verbindungsdaten ist rückwirkend für einen Zeitraum von 6 Monaten zulässig. Die Maßnahmen sind je nach Art auf 3 Tage bis zu einem Monat zu befristen.	Die Auskunft über die Verbindungsdaten ist rückwirkend für einen Zeitraum von 6 Monaten zulässig. Die Maßnahmen sind auf 3 Monate zu befristen.	Die Auskunft über die Verbindungsdaten ist rückwirkend für einen Zeitraum von 6 Monaten zulässig. Die Maßnahmen sind auf 3 Monate zu befristen. Es gilt eine Obergrenze von 12 Monaten.

Literaturverzeichnis

Achterberg, Norbert/Püttner, Günter/Würtenberger, Thomas (Hrsg.): Besonderes Verwaltungsrecht, Band I, Wirtschafts-, Umwelt-, Bau-, Kultusrecht, 2. Auflage, Heidelberg: C.F. Müller 2000, (zitiert: *Bearbeiter*, in: Achterberg/Püttner/Würtenberger, Band I)

- Besonderes Verwaltungsrecht, Band II, Kommunal-, Haushalts-, Abgaben-, Ordnungs-, Sozial-, Dienstrecht, 2. Auflage, Heidelberg: C.F. Müller 2000, (zitiert: *Bearbeiter*, in: Achterberg/Püttner/Würtenberger, Band II)

Albrecht, Hans-Jörg, Dorsch, Claudia, Krüpe, Christiane: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, b StPO und anderer verdeckter Ermittlungsmaßnahmen, Eine rechtstatsächliche Untersuchung im Auftrag des Bundesministeriums der Justiz (Kriminologische Forschungsberichte aus dem Max-Planck-Institut für ausländisches und internationales Strafrecht, Band 115, hrsg. von Albrecht, Hans-Jörg/Kaiser, Günther), Freiburg: edition iuscrim 2003, (zitiert: *Albrecht/Dorsch/Krüpe*, 2003)

- Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, b StPO und anderer verdeckter Ermittlungsmaßnahmen, Eine rechtstatsächliche Untersuchung (forschung aktuell – research in brief/17, hrsg. von Albrecht, Hans-Jörg/Eser, Albin), Freiburg: edition iuscrim 2003, (zitiert: *Albrecht/Dorsch/Krüpe*, Kurzbericht)

Ahlf, Ernst-Heinrich: Rechtsprobleme der polizeilichen Kriminalaktenführung, KritV 1988, S. 136 - 156

Amelung, Knut: Die Entscheidung des BVerfG zur „Gefahr im Verzug“ i.S. des Art. 13 II GG, NStZ 2001, S. 337 - 343

- Erweitern allgemeine Rechtfertigungsgründe, insbesondere § 34 StGB, hoheitliche Eingriffsbefugnisse des Staates? NJW 1977, S. 833 - 844

Amelung, Knut/Pauli, Gerhard: Einwilligung und Verfügungsbefugnis bei staatlichen Beeinträchtigungen des Fernmeldegeheimnisses i.S.d. Art. 10 GG, MDR 1980, S. 801 - 803

Arloth, Frank: Grundlagen und Grenzen des Untersuchungsrechts parlamentarischer Untersuchungsausschüsse, NJW 1987, S. 808- 812

Arndt, Claus: Zum Abhörurteil des BVerfG, NJW 2000, S. 47 - 49

- Grundrechtsschutz bei der Fernmeldeüberwachung, DÖV 1996, S. 459 - 463

Asbrock, Bernd: Der Richtervorbehalt – prozedurale Grundrechtssicherung oder rechtsstaatliches Trostpflaster? ZRP 1998, S. 17 - 19

Aschmann, Tjark Erich: Der Richtervorbehalt im deutschen Polizeirecht, Dissertation (Würzburger rechtswissenschaftliche Schriften, Band 11, hrsg. von der Juristischen

Fakultät der Universität Würzburg), Würzburg: Ergon Verlag 1999, (zitiert: *Aschmann*, 1999)

Bachmann, Gregor: Probleme des Rechtsschutzes gegen Grundrechtseingriffe im strafrechtlichen Ermittlungsverfahren, Dissertation (Schriften zum Prozessrecht, Band 121), Berlin: Duncker & Humblot 1994, (zitiert: *Bachmann*, 1994)

Backes, Otto/Gusy, Christoph/Bergemann, Maik/Doka, Siiri/Finke, Anja: Wirksamkeitsbedingungen von Richtervorbehalten bei Telefonüberwachungen, Kurzfassung des Abschlussberichts zum Forschungsprojekt der Universität Bielefeld, Betrifft JUSTIZ 2003, S. 14 - 17

Baldus, Manfred: Nachrichtendienste – Beobachtungen völkerverständigungswidriger Bestrebungen, ZRP 2002, S. 400 - 404

- Transnationales Polizeirecht, Baden-Baden: Nomos 2001, (zitiert: *Baldus*, 2001)

- Die Einheit der Rechtsordnung, Bedeutungen einer juristischen Formel in Rechtstheorie, Zivil- und Staatsrechtswissenschaft des 19. und 20. Jahrhunderts, (Schriften zur Rechtstheorie, Heft 168), Berlin: Duncker & Humblot 1995 (zitiert: *Baldus*, 1995)

Balzert, Helmut: Lehrbuch der Software-Technik, Band 1, Software-Entwicklung, 2. Auflage, Heidelberg und Berlin: Spektrum Akademischer Verlag 2001, (zitiert: *Balzert*, 2001)

Bär, Wolfgang: Anmerkung zu BGH: >>Durchsuchung<< einer Mailbox, Beschluss vom 31.07.1995 – 1 BGs 625/95 – , CR 1996, S. 490 - 491

- Der Zugriff auf Fernmeldedaten der Bundespost TELEKOM oder Dritter, CR 1993, S. 634 -643

Bauer, Hartmut, in: Dreier (Hrsg.), Grundgesetz Kommentar, Band II, Artikel 20 – 82 GG, 2. Auflage, Tübingen: Mohr Siebeck 2006, (zitiert: *Bauer*, in: Dreier)

- Die Bundestreue, zugleich ein Beitrag zur Dogmatik des Bundesstaatsrechts und zur Rechtsverhältnislehre, Habilitationsschrift, Jus Publicum Band 3, Tübingen: J.C.B. Mohr (Paul Siebeck) 1992 (zitiert: *Bauer*, 1992)

Becker, Joachim: Der transnationale Verwaltungakt, Übergreifendes Rechtsinsitut oder Anstoß zur Entwicklung mitgliedstaatlicher Verwaltungskooperationsgesetze? DVBl. 2001, S. 855 - 866

Begemann, Arndt/Lustermann, Henning: Neue Rechtsprechung des EuGH zur grenzüberschreitenden Abfallverbringung, NVwZ 2005, S. 283 - 285

Beheim, Johannes: Sicherheit und Vertraulichkeit bei europaweiter Mobilkommunikation: Zellulare Digital-Mobilfunksysteme D900 und D1800 bieten sicheren Informationsschutz über GMS-Standards hinaus, DuD 1994, S. 327 - 331

Behrendes, Udo: Von der Eilzuständigkeit zur Allzuständigkeit? Die Polizei 1988, S. 220 - 228

Belz, Reiner/Mußmann, Eike: Polizeigesetz für Baden-Württemberg, 6.Auflage, Stand 2005, Stuttgart u.a.: Boorberg 2001, (zitiert: *Belz/Mußmann)*

Benda, Ernst, in: Leibolz u.a. (Hrsg.), Privatsphäre und „Persönlichkeitsprofil“, Ein Beitrag zur Datenschutzdiskussion, in: Festschrift für Willi Geiger zum 65. Geburtstag, Tübingen: J.C.B. Mohr (Paul Siebeck) 1974, S. 23 – 44, (zitiert: *Benda*, in: FS für Geiger)

Benfer, Jost: Verdeckte Ermittlungen durch Polizeibeamte, MDR 1994, S. 12 - 13

Bernsmann, Klaus/Jansen, Kirsten: Anmerkung zum Beschluss des LG Aachen vom 24.11.1998 – 64 Qs 78/98 – , StV 1999, S. 591 - 593

- Heimliche Ermittlungsmethoden und ihre Kontrolle – Ein systematischer Überblick, StV 1998, S. 217 -231

Bethge, Herbert, in: Sachs (Hrsg.), Grundgesetz Kommentar, 4. Auflage, München: C.H. Beck 2007, (zitiert: *Bethge*, in: Sachs)

Bizer, Johann: Begleitgesetz zum Telekommunikationsgesetz vom 30. Oktober 1997, DuD 1998, S. 42 - 44

- Anmerkung zu BGH Beschluss vom 31.07.1995 – 1 BGs 625/95 – , DuD 1996, S. 627

Bleckmann, Albert: Staatsrecht II – Die Grundrechte, 4. Auflage, Köln u.a.: Carl Heymanns Verlag 1997, (zitiert: *Bleckmann*, 1997)

- Die Anerkennung der Hoheitsakte eines anderen Landes im Bundesstaat, NVwZ 1986, S. 1 - 6

Bock, Michael, in: Beck`scher TKG-Kommentar, 3. Auflage, München: C.H. Beck 2006, (zitiert: *Bock*, in: BeckTKG-Komm)

Böhrenz, Gunter/Franke, Jürgen: Niedersächsisches Gefahrenabwehrgesetz mit Ausführungsbestimmungen und Erläuterungen für Praxis und Ausbildung, 5. Auflage, Hannover: Pinkvoss Verlag 1998, (zitiert: *Bearbeiter*, in: Böhrenz/Franke)

Böhrenz, Gunter/Unger, Christoph/Siefken, Peter: Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung mit Ausführungsbestimmungen und Erläuterungen für Praxis und Ausbildung, 8. Auflage, Hannover: Pinkvoss Verlag 2005, (zitiert: *Bearbeiter*, in: Böhrenz/Unger/Siefken)

Borgs- Maciejewski, Hermann: Nochmals: Grenzen informationeller Zusammenarbeit zwischen Polizei und Verfassungsschutz, I. Erwiderung auf die gleichnamige Abhandlung von Riegel, DVBl. 1988, S. 388 - 390

- in: Borgs-Maciejewski/Ebert: Das Recht der Geheimdienste, Kommentar zum Bundesverfassungsschutzgesetz sowie zum G-10-Gesetz, Stuttgart: Boorberg 1986, (zitiert: *Borgs*, in: Borgs-Maciejewski/Ebert)

Borgs- Maciejewski, Hermann/Ebert, Frank: Das Recht der Geheimdienste, Kommentar zum Bundesverfassungsschutzgesetz sowie zum G-10-Gesetz, Stuttgart u.a.: Boorberg 1986, (zitiert: *Bearbeiter*, in: Borgs-Maciejewski/Ebert)

Brandner, Hans Erich: Das allgemeine Persönlichkeitsrecht in der Entwicklung durch die Rechtsprechung, JZ 1983, S. 689 - 696

Braun, Frank: Der sogenannte „Lauschangriff“ im präventivpolizeilichen Bereich, NVwZ 2000, S. 375 - 382

Breyer, Jonas: Vorratsdatenspeicherung von IP-Adressen durch Access Provider, DuD 2003, S. 491 - 495

Brodersen, Kilian: Das Strafverfahrensänderungsgesetz 1999, NJW 2000, S. 2536 - 2542

Brüning, Christoph: Widerspruchsfreiheit der Rechtsordnung – Ein Topos mit verfassungsrechtlichen Konsquenzen?, NVwZ 2002, S. 33 - 37

Bubnoff, Eckhart von: Terrorismusbekämpfung – eine weltweite Herausforderung, NJW 2002, S. 2672 - 2676

Buergenthal, Thomas/Doehring, Karl/Kokott, Juliane/Maier, Harold G.: Grundzüge des Völkerrechts, 3. Auflage, Heidelberg: C.F. Müller 2003, (zitiert: *Buergenthal/Doehring/Kokott/Maier*, 2003)

Büchner, Wolfgang u.a. (Hrsg.): Beck`scher TKG-Kommentar, 2. Auflage, München: C.H. Beck 2000, (zitiert: *Bearbeiter*, in: BeckTKG-Komm)

Caemmerer, Ernst von: Der privatrechtliche Persönlichkeitsschutz nach deutschem Recht, in: Esser/Thieme (Hrsg.), Festschrift für Fritz von Hippel zum 70. Geburtstag, Tübingen: J.C.B. Mohr (Paul Siebeck) 1967, S. 27 – 40, (zitiert: *v. Caemmerer*, in: FS für v. Hippel)

Calliess, Christian/Ruffert, Matthias: EUV/EGV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, Kommentar, 3. Auflage, München: C.H. Beck 2007, (zitiert: *Bearbeiter*, in: Calliess/Ruffert)

- Kommentar des Vertrages über die Europäische Union und des Vertrages zur Gründung der Europäischen Gemeinschaften – EUV/EGV – , 2. Auflage, Neuwied und Kriftel: Luchterhand 2002 (zitert: *Bearbeiter*, in: Calliess/Ruffert, 2002)

Cornils, Karin/Greve, Vagn, Landesbericht Dänemark, in: Gropp/Huber (Hrsg.), Rechtliche Initiativen gegen organisierte Kriminalität (Beiträge und Materialien aus dem Max-Planck-Institut für ausländisches und internationales Strafrecht Freiburg, hrsg. von Eser, Albin), Freiburg i.Br.: edition iuscrim 2001, S. 3 - 68, (zitiert: *Cornils/Greve*, in: Gropp/Huber)

Dammann, Ulrich, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 6. Auflage, Baden-Baden: Nomos 2006, (zitiert: *Dammann*, in: Simitis)

Dau, Klaus: Rechtsgrundlagen für den MAD – Das Gesetz über den Militärischen Abschirmdienst – , DÖV 1991, S. 661 - 670

Degenhart, Christoph: Das allgemeine Persönlichkeitsrecht, Art. 2 I i.V. mit Art. 1 I GG, JuS 1992, S. 361 - 368

Demko, Daniela: Die Erstellung von Bewegungsbildern mittels Mobiltelefonen als neuartige strafprozessuale Observationsmaßnahme, NStZ 2004, S. 57 - 64

Denninger, Erhard: in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, Gefahrenabwehr, Strafverfolgung, Rechtsschutz, 4. Auflage, München: C.H. Beck 2007, (zitiert: *Denninger*, in: Lisken/Denninger)

- Lauschangriff – Anmerkungen eines Verfassungsrechtlers, StV 1998, S. 401 - 406

- Verfassungsrechtliche Grenzen polizeilicher Datenverarbeitung insbesondere durch das Bundeskriminalamt, CR 1988, S. 51 - 60

Deutsch, Markus: Die heimliche Erhebung von Informationen und deren Aufbewahrung durch die Polizei, Dissertation, (Mannheimer rechtswissenschaftliche Abhandlungen, Band 12, hrsg. von der Fakultät für Rechtswissenschaft der Universität Mannheim), Heidelberg: C.F. Müller 1992, (zitiert: *Deutsch*, 1992)

Dierstein, Rüdiger/Fiedler, Herbert/Schulz, Arno (Hrsg.): Datenschutz und Datensicherung, Referate der gemeinsamen Fachtagung der Österreichischen Gesellschaft für Information (ÖGI) und der Gesellschaft für Informatik (GI), Johannes-Kepler-Universität, Linz/Österreich, 21. bis 23. September 1976, Köln: J.P. Bachem Verlag 1976, (zitiert: *Bearbeiter*, in: Dierstein/Fiedler/Schulz)

Di Fabio, Udo, in: Maunz-Dürig, Grundgesetz Kommentar, Band I, Art. 1 – 5, Loseblattsammlung, Stand: Dezember 2007, 51. Ergänzungslieferung zur 1. Auflage, München: C.H. Beck 2008, (zitiert: *Di-Fabio*, in: Maunz/Dürig)

Dix, Alexander: Informations-und Kommunikationskriminalität, Teil 2: Zwölf Thesen aus der Sicht eines Landesdatenschutzbeauftragten, Kriminalistik 2004, S. 81 - 85

- Vorratsspeicherung von IP-Adressen? Anmerkungen zur Bewertung der Praxis der T-Online International AG durch das Regierungspräsidium Darmstadt, DuD 2003, S. 234 - 236

- Rechtsfragen der Polizeilichen Datenverarbeitung, Jura 1993, S. 571 - 578

Dörr, Erwin/Schmidt, Dietmar: Neues Bundesdatenschutzgesetz, Handkommentar, Die Arbeitshilfe für Wirtschaft und Verwaltung, 3. Auflage, Frechen: Datakontext Verlag 1997 (zitiert: *Dörr/Schmidt*, 1997)

Dreier, Horst (Hrsg.): Grundgesetz Kommentar, Band II, Art. 20 – 82 GG, 2. Auflage, Tübingen: Mohr Siebeck 2006, (zitiert: *Bearbeiter*, in: Dreier)

- Grundgesetz Kommentar, Band I, Präambel, Art. 1 – 19 GG, 2. Auflage, Tübingen: Mohr Siebeck 2004, (zitiert: *Bearbeiter*, in: Dreier)

- in: Dreier (Hrsg.), Grundgesetz Kommentar, Band I, Art. 1 – 19, 2. Auflage, Tübingen: Mohr Siebeck 2004, (zitiert: *Dreier*, in: Dreier)

- Erkennungsdienstliche Maßnahmen im Spannungsfeld von Gefahrenabwehr und Strafverfolgung, JZ 1987, S. 1009 - 1017

Drews, Bill/Wacke, Gerhard/Vogel, Klaus/Martens, Wolfgang: Gefahrenabwehr, 9. Auflage, Köln u.a.: Carl Heymanns Verlag 1986, (zitiert: *Drews/Wacke/Vogel/Martens*, 1986)

Dronsch, Gerhard: Anmerkung zum Urteil des VGH Baden-Württemberg vom 26.05.1992 – 1 S 668/90 – , DVBl. 1992, S. 1314 - 1315

Droste, Bernadette: Handbuch des Verfassungsschutzrechts, Stuttgart u.a.: Boorberg Verlag 2007 (zitiert: *Droste*, 2007)

Ebert, Frank/Honnacker, Heinz/Seel, Lothar: Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei, Polizeiaufgabengesetz – PAG -, 4. Auflage, Stuttgart u.a.: Boorberg 2005

Eckhardt, Jens: Neue Entwicklungen der Telekommunikationsüberwachung, CR 2002, S. 770 - 775

- Neue Regelungen der TK-Überwachung, DuD 2002, S. 197 - 201

Ehlers, Dirk: Die Europäisierung des Verwaltungsprozessrechts (Völkerrecht Europarecht Staatsrecht, Schriftenreihe, Band 26, hrsg. von Bleckmann, Albert), Köln u.a.: Carl Heymanns Verlag 1999, (zitiert: *Ehlers*, 1999)

Ehmann, Horst: Zur Struktur des Allgemeinen Persönlichkeitsrechts, JuS 1997, S. 193 - 203

- Zur Zweckbindung privater Datennutzung – Zugleich ein Beitrag zum Rechtsgut des Datenschutzrechts mit einer Stellungnahme zu den Entwürfen zur Änderung des Bundesdatenschutzgesetzes, RDV 1988, S. 221 - 241

Ehmer, Jörg, in: Büchner u.a. (Hrsg.), Beck`scher TKG-Kommentar, 2. Auflage, München: C.H. Beck 2000, (zitiert: *Ehmer*, in: BeckTKG-Komm)

Elbel, Thomas: Die datenschutzrechtlichen Vorschriften für Diensteanbieter im neuen Telekommunikationsgesetz auf dem Prüfstand des europäischen und deutschen Rechts, Dissertation (Rechtswissenschaftliche Forschungsberichte), Berlin: Mensch & Buch Verlag 2005, (zitiert: *Elbel*, 2005)

Engisch, Karl: Einführung in das juristische Denken, herausgegeben und bearbeitet von Würtenberger, Thomas und Otto, Dirk, 10. Auflage, Stuttgart: Kohlhammer 2005 (zitiert: *Engisch*, 2005)

Erichsen, Hans-Uwe, in: Erichsen/Ehlers (Hrsg.), Allgemeines Verwaltungsrecht, 12. Auflage, Berlin: De Gruyter 2002, (zitiert: *Erichsen*, in: Erichsen/Ehlers)

Erichsen, Hans-Uwe/Ehlers, Dirk (Hrsg.): Allgemeines Verwaltungsrecht, 12. Auflage, Berlin: De Gruyter 2002, (zitiert: *Bearbeiter*, in: Erichsen/Ehlers)

Etling-Ernst, Martina: Praxiskommentar zum Telekommunikationsgesetz TKG, 2. Auflage, Ratingen: Eutelis Consult GmbH Eigenverlag 1999

Esser, Josef/Thieme, Hans (Hrsg.): Festschrift für Fritz von Hippel zum 70. Geburtstag, Tübingen: J.C.B. Mohr (Josef Siebeck) 1967, (zitiert: *Bearbeiter,* in: FS für v.Hippel)

Fastenrath, Ulrich: Die veränderte Stellung der Verwaltung und ihr Verhältnis zum Bürger unter dem Einfluss des europäischen Gemeinschaftsrechts, Die Verwaltung 31 (1998), S. 277 - 306

Felix, Dagmar: Einheit der Rechtsordnung: Zur verfassungsrechtlichen Relevanz einer juritischen Argumentationsfigur, Jus Publicum; Beiträge zum Öffentlichen Recht, Bd. 34, Habilitationsschrift, Tübingen: Mohr Siebeck 1998 (zitiert: *Felix*, 1998)

Fincke, Martin: Zum Begriff des Beschuldigten und den Verdachtsgraden, ZStW 95 (1983), S. 918 - 972

Fox, Dirk: Der IMSI-Catcher, DuD 2002, S. 212 - 215

- IMSI-Catcher, DuD 1997, S. 539

Franke, Jürgen/Unger, Christoph, in: Böhrenz/Franke, Niedersächsisches Gefahrenabwehrgesetz mit Ausführungsbestimmungen und Erläuterungen für Prxis und Ausbildung, 5. Auflage, Hannover: Pinkvoss Verlag 1998, (zitiert: *Franke/Unger*, in: Böhrenz/Franke)

Fugmann, Annette: Erkennungsdienstliche Maßnahmen zu präventiv-polizeilichen Zwecken, NJW 1981, S. 2227 - 2230

Gallwas, Hans-Ullrich: Grundrechte, 2. Auflage, Neuwied/Kriftel/Berlin: Luchterhand, 1995, (zitiert: *Gallwas*, 1995)

Geerds, Friedrich: Strafprozessuale Personenidentifizierung – Juristische und kriminalistische Probleme der §§ 81 b, 163 b und 163 c StPO, Jura 1986, S. 7 - 19

Gehde, Frank: Verfolgung von Straftaten im Internet, DuD 2003, S. 496 - 502

Geiger, Rudolf: Grundgesetz und Völkerrecht, 3. Auflage, München: C.H. Beck 2002, (zitiert: *Geiger*, 2002)

Geppert, Martin u.a. (Hrsg.): Beck`scher TKG-Kommentar, 3. Auflage, München: C.H. Beck 2006, (zitiert: *Bearbeiter*, in: BeckTKG-Komm)

Globig, Klaus: Die Verwertung von Abhörerkenntnissen aus einer Telefonüberwachung gemäß § 100 a StPO zu Zwecken der Gefahrenabwehr, ZRP 1991, S. 81 - 85

- Replik: Gefahrenabwehr durch Verwertung von Erkenntnissen aus Telefonabhörmaßnahmen gem. § 100 a StPO, ZRP 1991, S. 289 - 291

Gnirck, Karen/Lichtenberg, Jan: Internetprovider im Spannungsfeld staatlicher Auskunftsersuchen, DuD 2004, S. 598 - 602

Gola, Peter/Klug, Christoph: Die Entwicklung des Datenschutzrechts in den Jahre 2006/2007, NJW 2007, S. 2452 - 2459

- Die Entwicklung des Datenschutzrechts in den Jahren 2004/2005, NJW 2005, S. 2434 - 2440

- Grundzüge des Datenschutzrechts, München: C.H. Beck 2003, (zitiert: *Gola/Klug*, 2003)

Gola, Peter/Müthlein, Thomas: Neuer Tele-Datenschutz – bei fehlender Koordination über das Ziel hinausgeschossen? RDV 1997, S. 193 - 197

Gola, Peter/Schomerus, Rudolf: Bundesdatenschutzgesetz Kommentar, 9. Auflage, München: C.H. Beck 2007

Götz, Volkmar: Allgemeines Polizei- und Ordnungsrecht, 13. Auflage, Göttingen: Vandenhoeck & Ruprecht 2001, (zitiert: *Götz*, 2001)

- Die Entwicklung des allgemeinen Polizei- und Ordnungsrechts (1990 – 1993), NVwZ 1994, S. 652 - 661

Grabenwarter, Christoph: Europäische Menschenrechtskonvention, 2. Auflage, München: C.H. Beck/Manz 2005, (zitiert: *Grabenwarter*, 2005)

- Die Charta der Grundrechte für die Europäische Union, DVBl. 2001, S. 1 - 13

Graulich, Kurt: Die Novellierung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung im Jahr 2004, NVwZ 2005, S. 271 - 275

Gröpl, Christoph: Das Fernmeldegeheimnis des Art. 10 GG vor dem Hintergrund des internationalen Aufklärungsauftrages des Bundesnachrichtendienstes, ZRP 1995, S. 13 - 18

Gropp, Walter/Huber, Barbara (Hrsg.): Rechtliche Initiativen gegen organisierte Kriminalität (Beiträge und Materialien aus dem Max-Planck-Institut für ausländisches und internationales Strafrecht Freiburg, hrsg. von Eser, Albin), Freiburg i.Br.: edition iuscrim 2001, (zitiert: *Bearbeiter*, in: Gropp/Huber)

Groß, Thomas: Die Schutzwirkung des Brief-, Post- und Fernmeldegeheimnisses nach der Privatisierung der Post, JZ 1999, S. 326 - 335

Gubelt, Manfred in: von Münch/Kunig, Band 2: Art. 20 bis Art. 69, 4./5. Auflage, München: C.H. Beck 2001, (zitiert: *Gubelt*, in: v.Münch/Kunig)

Gusy, Christoph: in: von Mangoldt/Klein/Starck (Hrsg.), Kommentar zum Grundgesetz, Band 1: Präambel, Artikel 1 – 19, 5. Auflage, München: Verlag Franz Vahlen 2005, (zitiert: *Gusy*, in: v.Mangoldt/Klein/Starck)

- Lauschangriff und Grundgesetz, JuS 2004, S. 457 - 462

- Überwachung der Telekommunikation unter Richtervorbehalt – Effektiver Grundrechtsschutz oder Alibi?, ZRP 2003, S. 275 - 278

- Organisierte Kriminalität zwischen Polizei und Verfassungsschutz, GA 1999, S. 319 - 331

- Verfassungsfragen vorbeugenden Rechtsschutzes, JZ 1998, S. 167 - 174

- Das gesetzliche Trennungsgebot zwischen Polizei und Verfassungsschutz, Die Verwaltung 1991, S. 467 – 490

- Das Grundrecht des Post- und Fernmeldegeheimnisses, JuS 1986, S. 89 - 96

- Die Verwendung rechtmäßig erlangter Informationen durch die Nachrichtendienste, NVwZ 1983, S. 322 - 328

- Grundrechtsschutz vor staatlichen Informationseingriffen, VerwArch 74 (1983), S. 91 - 111

- Der Schutz vor Überwachungsmaßnahmen nach dem Gesetz zur Beschränkung von Art. 10 GG, NJW 1981, S. 1581 - 1586

Haas, Günter: Der „Große Lauschangriff“ – klein geschrieben, NJW 2004, S. 3082 - 3084

Habscheid, Walther J./Seidl-Hohenveldern, Ignaz, in: Seidl-Hohenveldern (Hrsg.), Völkerrecht – Lexikon des Rechts, 3. Auflage, Neuwied und Kriftel: Luchterhand 2001, (zitiert: *Habscheid/Seidl-Hohenveldern*, in: Seidl-Hohenveldern)

Haedge, Karl-Ludwig: Das neue Nachrichtendienstrecht für die Bundesrepublik Deutschland, Ein Leitfaden mit Erläuterungen, Heidelberg: Kriminalistik Verlag 1998, (zitiert: *Haedge*, 1998)

Hanack, Ernst-Walter/Mehle, Volkmar/Hilger, Hans/Widmaier, Gunter (Hrsg.): Festschrift für Peter Rieß zum 70. Geburtstag, Berlin und New York: De Gruyter 2002, (zitiert: *Bearbeiter*, in: FS für Rieß)

Hansen-Oest, Stephan, in: Schmidt/Königshofen/Zwach, Telekommunikationsrecht der Bundesrepublik Deutschland – TKR – , Rechtsvorschriften und Erläuterungen, Ordner 2, Stand 2003, Heidelberg: R.v. Decker 2003 ,(zitiert: *Hansen/Oest*, in: Schmidt/Königshofen/Zwach)

Hartung, Jürgen, in: Wilms/Masing/Jochum, Telekommunikationsgesetz, Kommentar und Vorschriftensammlung, Loseblattsammlung, 4. Lieferung Juli 2006, Stuttgart: Kohlhammer 2007, (zitiert: *Hartung*, in: Wilms/Masing/Jochum)

Hassemer, Winfried: Telefonüberwachung und Gefahrenabwehr, ZRP 1991, S. 121 - 125

Hassemer, Winfried/Starzacher, Karl: Organisierte Kriminalität – geschützt vom Datenschutz? (Forum Datenschutz, Band 2, hrsg. von Hassemer, Winfried/Starzacher, Karl), Baden-Baden: Nomos 1993, (zitiert: *Hassemer/Starzacher*, 1993)

Hefendehl, Roland: Die neue Ermittlungsgeneralklausel der §§ 161, 163 StPO: Segen oder Fluch?, StV 2001, S. 700 - 706

Heidrich, Joerg: Die T-Online-Entscheidung des RP Darmstadt und ihre Folgen, DuD 2003, S. 237 - 238

Henneke, Hans-Günter, in: Knack (Hrsg.), Verwaltungsverfahrensgesetz Kommentar, 8. Auflage, Köln u.a.: Carl Heymanns Verlag 2004, (zitiert: *Henneke*, in: Knack)

Hermes, Georg, in: Dreier (Hrsg.), Grundgesetz Kommentar, Band I, Präambel, Art. 1 – 19, 2. Auflage, Tübingen: Mohr Siebeck 2004, (zitiert: *Hermes*, in: Dreier)

Herzog, Roman/Herdegen, Matthias/Scholz, Rupert u.a. (Hrsg.): Grundgesetz Kommentar, begründet von Maunz, Theodor und Dürig, Günter, Bände I - V, Loseblattsammlung, Stand: Dezember 2007, 51. Ergänzungslieferung zur 1. Auflage, München: C.H. Beck 2008, (zitiert: *Bearbeiter*, in: Maunz/Dürig)

Heun, Sven-Erik: Das neue Telekommunikationsgesetz 2004, CR 2004, S. 893 - 907

Hilf, Meinhard: Untersuchungsausschüsse vor Gerichten, Zur neueren Rechtsprechung zum Recht der Untersuchungsausschüsse, NVwZ 1987, S. 537 - 545

Hilger, Hans: Gesetzgebungsbericht: Über den neuen § 100 i StPO, GA 2002, S. 557 - 559

- Neues Strafverfahrensrecht durch das OrgKG –1. Teil – , NStZ 1992, S. 457 - 463

- Über den „Richtervorbehalt im Ermittlungsverfahren, JR 1990, S. 485 - 489

Hirsch, Burkhard: Leserbrief zu Haas, NJW 2004, 3082, Der „Große Lauschangriff“, NJW 2004, Heft 49, S. XX

Hirsch, Günter: Der EuGH im Spannungsverhältnis zwischen Gemeinschaftsrecht und nationalem Recht, NJW 2000, S. 1817 - 1822

Hirsch, Hans Joachim, in: Jähnke/Laufhütte/Odersky (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Großkommentar, Zweiter Band, §§ 32 bis 60, 11. Auflage, Berlin: De Gruyter Recht 2003 , (zitiert: *H.J. Hirsch*, in: LK)

Hoeren, Thomas: Das Telemediengesetz, NJW 2007, S. 801 - 806

Hofmann, Hans, in: Schmidt-Bleibtreu/Klein, Kommentar zum Grundgesetz, 10. Auflage, München: Luchterhand 2004, (zitiert: *Hofmann*, in: Schmidt-Bleibtreu/Klein)

Holznagel, Bernd/Nelles, Ursula/ Sokol, Bettina: Die neue TKÜV (Telekommunikations-Überwachungsverordnung), Die Probleme in Recht und Praxis (Schriftenreihe Information und Recht, Band 27), München: C.H. Beck 2002, (zitiert: *Bearbeiter*, in: Holznagel/Nelles/Sokol)

Holznagel, Bernd/Enaux, Christoph/Nienhaus, Christian: Telekommunikationsrecht, Rahmenbedingungen – Regulierungspraxis, 2. Auflage, München: C.H. Beck 2006 (zitiert: *Holznagel/Enaux/Nienhaus*, 2006)

Honnacker, Heinz: Rechtsgrundlagen für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS), CR 1986, S. 287 - 291

Honnacker, Heinz/Beinhofer, Paul: Polizeiaufgabengesetz – PAG –, Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei, 18.Auflage, Stuttgart u.a.: Boorberg 2004

Huber, Bertold: Das Bankgeheimnis der Nachrichtendienste, NJW 2007, S. 881 - 883

- Das neue G-10-Gesetz, NJW 2001, S. 3296 - 3302

Huber, Peter M.: Verdeckte Datenerhebung, präventive Telekommunikationsüberwachung und der Einsatz technischer Mittel in Wohnungen nach dem Thüringer Verfassungsschutzgesetz und dem Thüringer Polizeiaufgabengesetz (Teil I), ThürVBl. 2005, S. 1 – 7

- Verdeckte Datenerhebung, präventive Telekommunikationsüberwachung und der Einsatz technischer Mittel in Wohnungen nach dem Thüringer Verfassungsschutzgesetz und dem Thüringer Polizeiaufgabengesetz (Teil II), ThürVBl. 2005, S. 33 - 39

- in: von Mangoldt/Klein/Starck (Hrsg.), Kommentar zum Grundgesetz, Band 1: Präambel, Artikel 1 – 19, 5. Auflage, München: Verlag Franz Vahlen 2005, (zitiert: *Huber P.M.*, in: v.Mangoldt/Klein/Starck)

Hufen, Friedhelm, in: Schmidt-Aßmann/Hoffmann-Riem (Hrsg.), Strukturen des Europäischen Verwaltungsrechts (Schriften zur Reform des Verwaltungsrechts, Band 6, hrsg. von Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard), Baden-Baden: Nomos 1999, (zitiert: *Hufen*, in: Schmidt-Aßmann/Hoffmann-Riem)

Ipsen, Jörn: Staatsrecht II, Grundrechte, 10. Auflage, Köln: Luchterhand 2007 (zitiert: *Ipsen*, 2007)

Ipsen, Knut: Völkerrecht, 5. Auflage, München: C.H. Beck 2004, (zitiert: *K. Ipsen*, 2004)

Isensee, Josef/Kirchhof, Paul (Hrsg.): Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band IV, Finanzverfassung – Bundesstaatliche Ordnung, 2. Auflage, Heidelberg: C.F. Müller 1999, (zitiert: *Bearbeiter*, in: HStR IV)

- Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band VI, Freiheitsrechte, 2. Auflage, Heidelberg: C.F. Müller 2001, (zitiert: *Bearbeiter*, in: HStR VI)

Jähnke, Burkhard/Laufhütte, Heinrich Wilhelm/Odersky, Walter (Hrsg.): Strafgesetzbuch, Leipziger Kommentar, Großkommentar, Zweiter Band, §§ 32 bis 60, 11. Auflage, Berlin: De Gruyter 2003, (zitiert: *Bearbeiter*, in: LK)

Jahn, Joachim: Verschärfte Finanzkontrollen nach Terroranschlägen, ZRP 2002, S. 109 - 111

Jarass, Hans D., in: Jarass/Pieroth, Grundgesetz für die Bundesrepublik Deutschland, 9. Auflage, München: C.H. Beck 2007, (zitiert: *Jarass*, in: Jarass/Pieroth)

- Das allgemeine Persönlichkeitsrecht im Grundgesetz, NJW 1989, S. 857 - 862

Jarass, Hans D./Pieroth, Bodo: Grundgesetz für die Bundesrepublik Deutschland, 9. Auflage, München: C.H. Beck 2007, (zitiert: *Bearbeiter*, in: Jarass/Pieroth)

Jauernig, Othmar (Hrsg.): Bürgerliches Gesetzbuch mit Allgemeinem Gleichbehandlungsgesetz (Auszug), Kommentar, 12. Auflage, München: C.H. Beck 2007, (zitiert: *Bearbeiter*, in: Jauernig)

Karpen, Ulrich/von Rönn, Matthias: Bericht über die Rechtsprechung des Bundesverfassungsgerichtes und der Landesverfassungsgerichte zum Bundesstaatsprinzip (seit 1980), JZ 1990, S. 579 -585

Kingreen, Thorsten, in: Calliess/Ruffert (Hrsg.), EUV/EGV, Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta, Kommentar, 3. Auflage, München: C.H.Beck 2007, (zitiert: *Kingreen*, in: Calliess/Ruffert)

- in: Callies/Ruffert (Hrsg.), Kommentar des Vertrages über die Europäische Union und des Vertrages zur Gründung der Europäischen Gemeinschaft, 2. Auflage, Neuwied und Kriftel: Luchterhand 2002, (zitiert: *Kingreen*, in: Calliess/Ruffert)

Kley, Max Dietrich/Sünner, Eckart/Willemsen, Arnold (Hrsg.): Festschrift für Wolfgang Ritter zum 70. Geburtstag, Steuerrecht, Steuer- und Rechtspolitik, Wirtschaftsrecht und Unternehmensverfassung, Umweltrecht, Köln: Verlag Dr. Otto Schmidt, 1997, (zitiert: *Bearbeiter*, in: FS für Ritter)

Klesczewski, Diethelm: Das Ende des Auskunftsersuchens nach § 12 FAG, JZ 1997, S. 719 - 721

- Das Auskunftsersuchen an die Post: die wohlfeile Dauerkontrolle von Fernmeldeanschlüssen, StV 1993, S. 382 - 389

Kloepfer, Michael/Bröcker, Klaus: Das Gebot der widerspruchsfreien Normgebung als Schranke der Ausübung einer Steuergesetzgebungskompetenz nach Art. 105 GG, DÖV 2001, S. 1 - 12

Knack, Hans-Joachim (Hrsg.): Verwaltungsverfahrensgesetz Kommentar, 8. Auflage, Köln u.a.: Carl Heymanns Verlag 2004, (zitiert: *Bearbeiter*, in: Knack)

Kniesel, Michael: Neue Polizeigesetze contra StPO?, ZRP 1987, S. 377 - 383

Kniesel, Michael/Tegtmeyer, Henning/Vahle, Jürgen: Handbuch des Datenschutzes für Sicherheitsbehörden, Datenschutz und Informationsverarbeitung in der sicherheitsbehördlichen Praxis, Stuttgart u.a.: Kohlhammer 1986, (zitiert: *Kniesel/Tegtmeyer/Vahle*, 1986)

Kniesel, Michael/Vahle, Jürgen: Fortentwicklung des materiellen Polizeirechts, DÖV 1987, S. 953 - 960

Koch, Martin: Datenerhebung und -verarbeitung in den Polizeigesetzen der Länder, Dissertation (Frankfurter Studien zum Datenschutz, Band 13, Veröffentlichungen der Forschungsstelle für Datenschutz an der Johann-Wolfgang-Goethe Universität, Frankfurt am Main, hrsg. von Simitis, Spiros), Baden-Baden: Nomos, 1999, (zitiert: *M. Koch*, 1999)

Koch, Hans-Joachim (Hrsg.): Terrorismus – Rechtsfragen der äußeren und inneren Sicherheit. Symposium für Hans Peter Bull und Helmut Ritterstieg am 31.05.2002, Baden-Baden: Nomos 2002 , (zitiert: *Bearbeiter*, in: H.J. Koch)

König, Marco: Trennung und Zusammenarbeit von Polizei und Nachrichtendiensten, Dissertation (Schriften zum Recht der Inneren Sicherheit, Band 7, hrsg. von Heckmann, Dirk/Würtenberger, Thomas), Stuttgart u.a.: Boorberg 2005, (zitiert: *König*, 2005)

Königshofen, Thomas: Telekommunikations – Datenschutzverordnung (TDSV) Kommentar, Heidelberg: R. v. Decker 2002

- Private Netze aus fernmelderechtlicher Sicht, Archiv PT 1994, S. 39 - 50

Kopp, Ferdinand/Ramsauer, Ulrich: Verwaltungsverfahrensgesetz Kommentar, 9. Auflage, München: C.H. Beck 2005

Körner, Harald Hans/Scherp, Dirk: Betäubungsmittelgesetz, Arzneimittelgesetz, 5. Auflage, München: C.H. Beck 2001

Kowalczyk, Anneliese: Datenschutz im Polizeirecht, Reaktionen der Gesetzgeber auf das Volkszählungsurteil des Bundesverfassungsgericht, Dissertation (Schriften zur öffentlichen Verwaltung, Band 29, hrsg. von Knemeyer, Franz-Ludwig), Köln: Kohlhammer und Deutscher Gemeindeverlag 1990 (zitiert: *Kowalczyk*, 1990)

Kramer, Bernhard: Grundfragen der Erkennungsdienstlichen Behandlung nach § 81 b StPO, JR 1994, S. 224 - 231

Krüger, Ralf: Informationelle Selbstbestimmung und Kriminalaktenführung, DÖV 1990, S. 641 - 646

Kubicek, Herbert: Der Schutz des Fernmeldegeheimnisses auf dem Telekommunikationsmarkt, DuD 1995, S. 656 - 663

Kubicek, Herbert/Bach, Knud: Neue TK-Datenschutzverordnung – Fortschritt für den Datenschutz? CR 1991, S. 489 - 496

Kudlich, Hans: Der heimliche Zugriff auf Daten in einer Mailbox: ein Fall der Überwachung des Fernmeldeverkehrs? – BGH, NJW 1997, 1934 – , JuS 1998, S. 209 - 214

Kühne, Hans-Heiner: Telefonüberwachung von Rechtsanwälten, Fall Kopp – EMGR-Urteil vom 25.03.1998, Übersetzung und Zusammenfassung des Sachverhalts sowie Anmerkung, StV 1998, S. 683 - 686

Kunig, Philip, in: von Münch/Kunig (Hrsg.), Grundgesetz-Kommentar, Band 1, 5. Auflage, München: C.H. Beck 2000

- Der Grundsatz informationeller Selbstbestimmung, Jura 1993, S. 595 - 604

Kutscha, Martin: Verfassungsrechtlicher Schutz des Kernbereichs privater Lebensgestaltung – nichts Neues aus Karlsruhe? NJW 2005, S. 20 - 22

- Rechtsschutzdefizite bei Grundrechtseingriffen von Sicherheitsbehörden, NVwZ 2003, S. 1296 - 1300

- Novellierung des Thüringer Polizeiaufgabengesetzes – Mehr Sicherheit durch weniger Grundrechtsschutz, LKV 2003, S. 114 - 118

Kutscha, Martin/Möritz, Marion: Lauschangriffe zur vorbeugenden Straftatenbekämpfung? – Ein Beitrag zu den Eingriffsvoraussetzungen nach dem neuen Art. 13 GG – , StV 1998, S. 564 - 568

Lackner, Karl/Kühl, Kristian: Strafgesetzbuch Kommentar, 26. Auflage, München: C.H. Beck 2007

Lammich, Klaus: Telekommunikationsgesetz Kommentar, Loseblattausgabe, einschließlich 5. Ergänzung – September 2001, Neuwied u.a.: Luchterhand 2001

Lang, Gernot: Zur Frage, ob (private) Anbieter von Telekommunikationsdiensten aus Gründen des Jugendschutzes das Fernmeldegeheimnis durchbrechen können, Archiv PT 1997, S. 298 - 302

Lange, Richard: Terrorismus kein Notstandsfall? Zur Anwendung des § 34 StGB im öffentlichen Recht, NJW 1978, S. 784 - 786

- Der „gezielte Todesschuss“, JZ 1976, S. 546 - 548

Leibholz, Gerhard u.a. (Hrsg.): Menschenwürde und freiheitliche Rechtsordnung, Festschrift für Willi Geiger zum 65. Geburtstag, Tübingen: J.C.B. Mohr (Paul Siebeck) 1974, (zitiert: *Bearbeiter*, in: FS für Geiger)

Lemke, Hanno-Dirk: Verwaltungsvollstreckungsrecht des Bundes und der Länder, Eine systematische Darstellung, Baden-Baden: Nomos 1997, (zitiert: *Lemke*, 1997)

Lenckner, Theodor, in: Schönke/Schröder, Strafgesetzbuch, Kommentar, 27. Auflage, München: C.H. Beck 2006, (zitiert: *Lenckner*, in: Schönke/Schröder)

Lerche, Peter, in: Maunz/Dürig, Grundgesetz Kommentar, Band V, Art. 70 – 99, Loseblattsammlung, Stand: Dezember 2007, 51. Ergänzungslieferung zur 1. Auflage, München: C.H. Beck 2008, (zitiert: *Lerche*, in: Maunz/Dürig)

Leutheusser-Schnarrenberger, Sabine: Vorratsdatenspeicherung – Ein vorprogrammierter Verfassungskonflikt, ZRP 2007, S. 9 - 13

Lisken, Hans: Polizeibefugnis zum Töten? DRiZ 1989, S. 401 – 404

- Neue polizeiliche Ermittlungsverfahren im Rechtsstaat des Grundgesetzes, DRiZ 1987, S. 184 - 188.

Lisken, Hans/Denninger, Erhard (Hrsg.): Handbuch des Polizeirechts, Gefahrenabwehr, Strafverfolgung, Rechtsschutz, 4. Auflage, München: C.H. Beck 2007, (zitiert: *Bearbeiter*, in: Lisken/Denninger)

- in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, Gefahrenabwehr, Strafverfolgung, Rechtsschutz, 4. Auflage, München: C.H. Beck 2007, (zitiert: *Lisken/Denninger*, in: Lisken/Denninger)

Lisken, Hans/Mokros, Reinhard: Richter- und Behördenleitervorbehalte im neuen Polizeirecht, NVwZ 1991, 609 - 614

Loewer, Wolfgang, in: von Münch/Kunig (Hrsg.), Grundgesetzkommentar Band 1, Art. 1 – 19, 5. Auflage, München: C.H. Beck 2000, (zitiert: *Loewer*, in: v.Münch/Kunig)

Lorenz, Dieter, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band VI, Freiheitsrechte, 2. Auflage, Heidelberg: C.F. Müller 2001, (zitiert: *Lorenz*, in: HStR VI)

Lorz, Ralph Alexander: Interorganrespekt im Verfassungsrecht: Funktionenzuordnung, Rücksichtnahmegebote und Kooperationsverpflichtungen; eine rechtsvergleichende Analyse anhand der Verfassungssysteme der Bundesrepublik Deutschland, der Europäischen Union und der Vereinigten Staaten, Habilitationsschrift, Jus Publicum, Bd. 70, Tübingen: Mohr Siebeck 2001 (zitiert: *Lorz*, 2001)

Löwnau-Iqbal, Gabriele, in: Scheurle/Mayen (Hrsg.), Telekommunikationsgesetz (TKG), München: C.H. Beck 2002, (zitiert: *Löwnau-Igbal*, in: Scheurle/Mayen)

Lutz, Dieter S.: Was ist Terrorismus? Definitionen, Wandel, Perspektiven, in: Koch (Hrsg.), Terrorismus – Rechtsfragen der äußeren und inneren Sicherheit, Symposium für Hans Peter Bull und Helmut Ritterstieg am 31.05.2002, Baden-Baden: Nomos 2002, S. 9 – 27, (zitiert: *Lutz*, in: Koch)

Magiera, Siegfried: Die Grundrechtecharta der Europäischen Union, DÖV 2000, S. 1017 – 1026

Mallmann, Christoph: Datenschutz in Verwaltungs-Informationssystemen, Zur Verhältnismäßigkeit des Austausches von Individualinformationen in der normvollziehenden Verwaltung, Dissertation (Rechtstheorie und Informationsrecht,

hrsg. von Podlech, Adalbert und Steinmüller, Wilhelm, Band 2), München und Wien: R. Oldenbourg Verlag 1976, (zitiert: *Mallmann*, 1976)

Mangoldt, Hermann von/Klein, Friedrich/Starck, Christian (Hrsg.): Kommentar zum Grundgesetz, Band 1: Präambel, Art. 1 – 19, 5. Auflage, München: Verlag Franz Vahlen 2005, (zitiert: *Bearbeiter*, in: v.Mangoldt/Klein/Starck)

- Kommentar zum Grundgesetz, Band 2: Artikel 20 bis 82, 5. Auflage, München: Verlag Franz Vahlen 2005, (zitiert: *Bearbeiter*, in: v.Mangoldt/Klein/Starck)

Mann, Thomas/Müller, Rolf-Georg: Präventiver Lauschangriff via Telefon? ZRP 1995, S. 180 - 185

Mansel, Heinz-Peter, in: Jauernig (Hrsg.), Bürgerliches Gesetzbuch mit Allgemeinem Gleichbehandlungsgesetz (Auszug), Kommentar, 12. Auflage, München: C.H. Beck 2007, (zitiert: *Bearbeiter*, in: Jauernig)

Manssen, Gerrit: Staatsrecht II, Grundrechte, 4. Auflage, München: C.H. Beck 2005 (zitiert: *Manssen*, 2005)

- Staatsrecht I, Grundrechtsdogmatik, München: Verlag Franz Vahlen 1995, (zitiert: *Manssen*, 1995)

März, Wolfgang, in: von Mangoldt/Klein/Starck (Hrsg.), Kommentar zum Grundgesetz, Band 2: Art. 20 bis 82, 5. Auflage, München: Verlag Franz Vahlen 2005, (zitiert: *März*, in: v.Mangoldt/Klein/Starck)

Maunz, Theodor, in: Maunz/Dürig, Grundgesetz Kommentar, Band IV, Art. 28 – 69, Loseblattsammlung, Stand: Dezember 2007, 51. Ergänzungslieferung zur 1. Auflage, München: C.H. Beck 2008, (zitiert: *Maunz*, in: Maunz/Dürig)

Meister, Matthias/Laun, Stefan, in: Wissmann, Martin (Hrsg.): Telekommunikationsrecht, Praxishandbuch (Schriftenreihe Kommunikation & Recht, Band 8, hrsg. von: Holznagel, Bernd/Koenig, Christian/Scherer, Joachim u.a.), 2. Auflage, Frankfurt am Main, Verlag Recht und Wirtschaft GmbH 2006, (zitiert: *Meister/Laun*, in: Wissmann)

Meixner, Kurt/Fredrich, Dirk: Hessisches Gesetz über die öffentliche Sicherheit und Ordnung, HSOG, mit Erläuterungen und ergänzenden Vorschriften, 10. Auflage, Stuttgart u.a.: Boorberg 2005

Meyer, Hubert, in: Knack (Hrsg.), Verwaltungsverfahrensgesetz Kommentar, 8.Auflage, Köln u.a.: Carl Heymanns Verlag 2004, (zitiert: *H. Meyer*, in: Knack)

Meyer-Goßner, Lutz: Strafprozessordnung, 50. Auflage, München: C.H. Beck 2007

Meyer-Ladewig, Jens: Europäische Menschenrechtskonvention, Handkommentar, 2. Auflage, Baden-Baden: Nomos 2006

Michel, Helmut: Die verfassungskonforme Auslegung, Korreferat, JuS 1961, S. 274 - 281

Möhrenschlager, Manfred: Das OrgKG – eine Übersicht nach amtlichen Materialien (Teil 2), wistra 1992, S. 326 - 333

Möstl, Markus: Verfassungsrechtliche Vorgaben für die strategische Fernmeldeaufklärung und die informationelle Vorfeldarbeit im allgemeinen, DVBl. 1999, S. 1394 -1403

Momsen, Carsten: Der „große Lauschangriff", ZRP 1998, S. 459 - 463

Münch, Ingo von: Staatsrecht, Band 2, 5. Auflage, Stuttgart u.a.: Kohlhammer 2002, (zitiert: *v.Münch*, 2002)

Münch, Ingo von/Kunig, Philip (Hrsg.): Grundgesetz-Kommentar, Band 1, Präambel bis Art. 19, 5. Auflage, München: C.H. Beck 2000, (zitiert: *Bearbeiter*, in: v.Münch/Kunig)

- Grundgesetz-Kommentar, Band 2, Art. 20 bis Art. 69, 4./5. Auflage, München: C.H. Beck 2001, (zitiert: *Bearbeiter*, in: v.Münch/Kunig)

Murswiek, Dietrich, in: Sachs (Hrsg.), Grundgesetz Kommentar, 4. Auflage, München: C.H. Beck 2007, (zitiert: *Murswiek*, in: Sachs)

Mußmann, Eike: Allgemeines Polizeirecht in Baden-Württemberg, Systematische Darstellung, 4. Auflage, Stuttgart u.a.: Boorberg 1994, (zitiert: *Mußmann*, 1994)

Nachbaur, Andreas: Standortfeststellung und Art. 10 GG – Der Kammerbeschluss des BVerfG zum Einsatz des „IMSI-Catchers", NJW 2007, S. 335 - 337

Nack, Armin, in: Pfeiffer (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung und zum Gerichtsverfassungsgesetz mit Einführungsgesetz, 5. Auflage, München: C.H. Beck 2003, (zitiert: *Nack*, in: KK)

Nedden, Burckhard: Thesen und Anmerkungen des Landesbeauftragten für den Datenschutz in Niedersachsen insbesondere zur präventiven Telekommunikationsüberwachung in § 33 a des Entwurfs eines Gesetzes zur Änderung des Niedersächsischen Gefahrenabwehrgesetzes (NGefAG), http://www.lfd.niedersachsen.de/master/C2216997_N2216723_L20_D0_I560.html

Nehm, Kay: Das nachrichtendienstliche Trennungsgebot und die neue Sicherheitsarchitektur, NJW 2004, S. 3289 - 3295

Neßler, Volker: Der transnationale Verwaltungsakt – Zur Dogmatik eines neuen Rechtsinstituts, NVwZ 1995, S. 863 - 866

- Europäisches Richtlinienrecht wandelt deutsches Verwaltungsrecht, Ein Beitrag zur Europäisierung des deutschen Rechts (Berliner Europa-Studien, Politik, Recht und Wirtschaft in Europa, Band 1, hrsg. von Neßler, Volker), Berlin: Verlag Dr. Köster 1994, (zitiert: *Neßler*, 1994)

Neuhaus, Ralf, in: Hanack/Mehle/Hilger/Widmaier (Hrsg.), Festschrift für Peter Rieß zum 70. Geburtstag, Berlin und New York: De Gruyter 2002, (zitiert: *Neuhaus*, in: FS für Rieß)

Oldiges, Martin: Verbandskompetenz, DÖV 1989, S. 873 - 884

Oppermann, Thomas: Europarecht, ein Studienbuch, 3. Auflage, München: C.H.Beck 2005 (zitiert: *Oppermann*, 2005)

Pagenkopf, Martin, in: Sachs (Hrsg.), Grundgesetz Kommentar, 4. Auflage, München: C.H. Beck 2007, (zitiert: *Pagenkopf*, in: Sachs)

Pallasky, *Ansgar*: USA Patriot Act: Neues Recht der TK-Überwachung, DuD 2002, S. 221 - 215

Palm, Franz/Roy, Rudolf: Mailboxen: Staatliche Eingriffe und andere rechtliche Aspekte, NJW 1996, S. 1791 - 1797

Papier, Hans-Jürgen, in: Maunz/Dürig, Grundgesetz Kommentar, Band II, Art. 6 – 16 a; Loseblattsammlung, Stand: Dezember 2007, 51. Ergänzungslieferung zur 1. Auflage, München: C.H. Beck 2008, (zitiert: *Papier*, in: Maunz/Dürig)

Paulick, Heinz: Das Steuerrecht als Teil der Gesamtrechtsordnung und die Rechtsprechung des Bundesfinanzhofs, DStR 1975, S. 564 - 577

Peitsch, Dietmar: Die Informationsbeschaffung im neuen Polizeirecht, ZRP 1992, S. 127 - 130

Pernice, Ina Maria: Die Telekommunikationsüberwachungsverordnung (TKÜV), DuD 2002, S. 207 - 211

Pernice, Ingolf, in: Dreier (Hrsg.), Grundgesetz Kommentar, Band II, Art. 20 – 82, 2. Auflage, Tübingen: Mohr Siebeck 2006, (zitiert: *I. Pernice*, in: Dreier)

- Gemeinschaftsverfassung und Grundrechtsschutz – Grundlagen, Bestand und Perspektiven, NJW 1990, S. 2409 - 2420

Petri, Thomas , in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, Gefahrenabwehr, Strafverfolgung, Rechtsschutz, 4. Auflage, München: C.H. Beck 2007, (zitiert: *Petri*, in: Lisken/Denninger)

Pfeiffer, Gerd (Hrsg.): Karlsruher Kommentar zur Strafprozessordnung und zum Gerichtsverfassungsgesetz mit Einführungsgesetz, 5. Auflage, München: C.H. Beck 2003, (zitiert: *Bearbeiter*, in: KK)

- Strafprozessordnung, 5. Auflage, München: C.H. Beck 2005

Pieroth, Bodo, in: Jarass/Pieroth, Grundgesetz für die Bundesrepublik Deutschland, 9. Auflage, München: C.H. Beck 2007, (zitiert: *Pieroth*, in: Jarass/Pieroth)

Pieroth, Bodo/Schlink, Bernhard: Grundrechte, Staatsrecht II, 23. Auflage, Heidelberg: C.F. Müller 2007, (zitiert: *Pieroth/Schlink*, 2007)

Pieroth, Bodo/Schlink, Bernhard/ Kniesel, Michael: Polizei-und Ordnungsrecht mit Versammlungsrecht, 4. Auflage. München: C.H. Beck 2007 (zitiert: *Pieroth/Schlink/Kniesel*, 2007)

Pitschas, Rainer/Aulehner, Josef: Informationelle Sicherheit oder „Sicherheitsstaat“? NJW 1989, S. 2353 - 2359

Podlech, Adalbert: Aufgaben und Problematik des Datenschutzes, DVR 1976, S. 23 - 39

- Gesellschaftstheoretische Grundlagen des Datenschutzes, in: Dierstein/Fiedler/Schulz (Hrsg.), Datenschutz und Datensicherung, Referate der gemeinsamen Fachtagung der Österreichischen Gesellschaft für Information (ÖGI) und der Gesellschaft für Informatik (GI), Johannes-Kepler-Universität, Linz/Österreich, 21. bis 23. September 1976, Köln: J.P. Bachem Verlag 1976, S. 311 – 326, (zitiert: *Podlech*, in: Dierstein/Fiedler/Schulz)

Prittwitz, Cornelius: Die Grenzen der Verwertbarkeit von Erkenntnissen aus der Telefonüberwachung gemäß § 100 a StPO, StV 1984, S. 302 - 311

Puschke, Jens/Singelnstein, Tobias: Verfassungsrechtliche Vorgaben für heimliche Informationsbeschaffungsmaßnahmen, NJW 2005, S. 3534 - 3538

Püttner, Günter/Rux, Johannes: Schulrecht, in: Achterberg/Püttner/Würtenberger (Hrsg.), Besonderes Verwaltungsrecht, Band I, 2.Auflage, Heidelberg: C.F Müller 2000, S. 1124 - 1185 (zitiert: *Püttner/Rux*, in: Achterberg/Püttner/Würtenberger, Band I)

Rabe von Kühlwein, Malte: Der Richtervorbehalt im Polizei- und Strafprozessrecht, Dissertation (Schriften zum Strafrecht und Strafprozessrecht, hrsg. von Maiwald, Manfred, Band 50), Frankfurt am Main u.a.: Peter Lang 2001, (zitiert: *Rabe von Kühlwein*, 2001)

Rachor, Frederik, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, Gefahrenabwehr, Strafverfolgung, Rechtsschutz, 4. Auflage, München: C.H. Beck 2007, (zitiert: *Rachor*, in: Lisken/Denninger)

Randl, Hans: Verfassungsrechtliche Aspekte des neuen Hamburger Polizeirechts, NVwZ 1992, S. 1070 - 1073

Reimann, Thomas: Datenschutz im neuen TKG, DuD 2004, S. 421 - 425

Rengeling, Hans-Werner, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band IV, Finanzverfassung – Bundesstaatliche Ordnung, 2. Auflage, Heidelberg: C.F. Müller 1999 , (zitiert: *Rengeling*, in: HStR IV)

Rengeling, Hans-Werner/Szczekalla, Peter: Grundrechte in der Europäischen Union, Charta der Grundrechte und Allgemeine Rechtsgrundsätze, Köln: Carl Heymanns Verlag 2004 (zitiert: *Rengeling/Szczekalla*, 2004)

Riegel, Reinhard: Datenschutzbeauftragte als Essentiale des informationelle Selbstbestimmungsrechts, BayVBl. 1998, S. 523 - 526

- Nochmals: Telefonüberwachung und Gefahrenabwehr, ZRP 1991, S. 286 – 288

- Polizeiliche Informationsverarbeitung für Gefahrenabwehr und Strafverfolgung, RDV 1990, S. 232 - 241

- Grenzen informationeller Zusammenarbeit zwischen Polizei und Verfassungsschutz, DVBl. 1988, S. 121 - 129

- Nochmals: Grenzen informationeller Zusammenarbeit zwischen Polizei und Verfassungsschutz, II. Stellungnahme zur Erwiderung von Borgs-Maciejewski, DVBl. 1988, S. 391 - 392

- §§ 32, 34 StGB als hoheitliche Befugnisgrundlage? NVwZ 1985, S. 639 - 641

- Zum Problem der Anfertigung und Vernichtung erkennungsdienstlicher Unterlagen, DÖV 1978, S. 17 - 21

Rieß, Peter (Hrsg.): Löwe-Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Großkommentar, Zweiter Band, §§ 72 – 136 a, 25. Auflage, Berlin: De Gruyter 2004, (zitiert: *Bearbeiter*, in: Löwe-Rosenberg)

Rimmele, Peter: Die Novellierung des sächsischen Polizeigesetzes, SächsVBl. 1996, S. 32 - 37

Robert, Anna, in: Geppert, Martin u.a. (Hrsg.), Beck`scher TKG-Kommentar, 3. Auflage, München: C.H. Beck 2006, (zitiert: *Robert*, in: BeckTKG-Komm)

Roessler, Thomas: Erweiterte Nutzung von WHOIS-Daten, DuD 2003, S. 239

- WHOIS: Datenschutz im DNS? DuD 2002, S. 666 - 671

Roewer, Helmut: Nachrichtendienstrecht der Bundesrepublik Deutschland: Kommentar und Vorschriftensammlung für die Praxis der Verfassungsschutzbehörden, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes, Köln u.a.: Carl Heymanns Verlag 1987

Roggan, Fredrik: Handbuch zum Recht der Inneren Sicherheit mit einem Nachwort von Christian Bommarius, Bonn: Pahl-Rugenstein 2003, (zitiert: *Roggan*, 2003)

Roggan, Fredrik/Bergemann, Nils: Die „neue Sicherheitsarchitektur“ der Bundesrepublik Deutschland, NJW 2007, S. 876 - 881

Ronellenfitsch, Michael: 33. Tätigkeitsbericht des Hessischen Datenschutzbeauftragen vorgelegt zum 31.12.2004, gemäß § 30 des Hessischen Datenschutzgesetzes, http://www.datenschutz.hessen.de/_old_content/tb32/inhalt.htm

Roos, Jürgen: Polizei- und Ordnungsbehördengesetz Rheinland-Pfalz – POG -, 3. Auflage, Stuttgart u.a.: Boorberg 2004

Rosenbaum, Christian: Der grundrechtlichen Schutz vor Informationseingriffen, Jura 1988, S. 178 - 185

Roßnagel, Alexander (Hrsg.): Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, München: C.H. Beck 2003, (zitiert: *Bearbeiter*, in: Roßnagel)

- in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, München: C.H. Beck 2003, (zitiert: *Roßnagel*, in: Roßnagel)

Rublack, Susanne: Terrorismusbekämpfungsgesetz: Neue Befugnisse für die Sicherheitsbehörden, DuD 2002, S. 202 - 206

Rudolf, Walter/Jutzi, Siegfrid: Verfassungspflicht zur Harmonisierung der Landesmediengesetze?, ZRP 1987, S. 2 - 4

Ruffert, Matthias: Der transnationale Verwaltungsakt, Die Verwaltung 31 (2001), S. 453 - 485

Ruthig, Josef: Die Unverletzlichkeit der Wohnung (Art. 13 GG n.F.), JuS 1998, S. 506 - 516

Sachs, Michael (Hrsg.): Grundgesetz Kommentar, 4. Auflage, München: C.H. Beck 2007, (zitiert: *Bearbeiter*, in: Sachs)

- in: Sachs (Hrsg.) Grundgesetz Kommentar, 4. Auflage, München: C.H. Beck 2007, (zitiert: *Sachs*, in: Sachs)

- Fernmeldeüberwachung durch den Bundesnachrichtendienst, Urteilsanmerkung zu BVerfG, Urteil vom 14.07.1999, JuS 2000, S. 597 - 599

- Die dynamische Verweisung der Ermächtigungsnorm, NJW 1981, S. 1651 - 1652

Sannwald, Rüdiger, in: Schmidt-Bleibtreu/Klein, Kommentar zum Grundgesetz, 10. Auflage, München: Luchterhand 2004, (zitiert: *Sannwald*, in: Schmidt-Bleibtreu/Klein)

Saurer, Johannes: Grundrechtskonkurrenzen bei der Mobilfunküberwachung – insbesondere beim Einsatz des IMSI-Catchers, RDV 2007, S. 100 - 103

Schäfer, Gerhard, in: Rieß (Hrsg.), Löwe-Rosenberg, Die Strafprozeßordnung und das Gerichtsverfassungsgesetz, Großkommentar, Zweiter Band, §§ 72 – 136 a, 25. Auflage, Berlin: De Gruyter 2004, (zitiert: *Schäfer*, in: Löwe-Rosenberg)

Schatzschneider, Wolfgang: Telefondatenverarbeitung und Fernmeldegeheimnis, NJW 1993, S. 2029 - 2031

Schenke, Ralf P.: Verfassungsfragen einer Nutzung repressiver Daten zu Zwecken der Gefahrenabwehr am Beispiel der Überwachung der Telekommunikation, in: Wolter u.a. (Hrsg.), Datenübermittlungen und Vorermittlungen, Festgabe für Hans Hilger, Heidelberg: C.F. Müller 2003, S. 211 – 223, (zitiert: *R.P. Schenke*, in: FG für Hilger)

- Exekutive Rechtssetzung bei der strafprozessualen Überwachung der Telekommunikation – Ein Verstoß gegen den Vorbehalt des Gesetzes? MMR 2002, S. 8 - 10

- Verfassungsrechtliche Probleme einer präventiven Überwachung der Telekommunikation, AöR 125 (2000), S. 1 - 44

Schenke, Wolf-Rüdiger: Polizei- und Ordnungsrecht, 5. Auflage, Heidelberg: C.F. Müller 2007 (zitiert: *W.-R. Schenke*, 2007)

- Probleme der Übermittlung und Verwendung strafprozessual erhobener Daten für präventivpolizeiliche Zwecke, in: Wolter u.a. (Hrsg.), Datenübermittlungen und Vorermittlungen, Festgabe für Hans Hilger, Heidelberg: C.F. Müller 2003, S. 225 – 245, (zitiert: *W.-R. Schenke*, in: FG für Hilger)

- Die Verwendung der durch strafprozessuale Überwachung der Telekommunikation gewonnenen personenbezogenen Daten zur Gefahrenabwehr, JZ 2001, S. 997 - 1004

- Verfassungskonformität der Volkszählung, NJW 1987, S. 2777 – 2786

- Die Verfassungsorgantreue, Schriften zum Öffentlichen Recht, Band 325, Berlin: Duncker & Humblot 1977 (zitiert: *W.-R. Schenke*, 1977)

Schenke, Wolf-Rüdiger/Schenke, Ralf Peter: Polizei- und Ordnungsrecht, in: Steiner (Hrsg.), Besonderes Verwaltungsrecht, Ein Lehrbuch, 8. Auflage, Heidelberg: C.F: Müller 2006, S. 171 - 362, (zitiert: *W.-R. Schenke/R.P.Schenke*, in: Steiner)

Scherer, Joachim: Das neuen Telekommunikationsgesetz, NJW 2004, S. 3001 - 3010

Scheurle, Klaus-Dieter, in: Scheurle/Mayen (Hrsg.), Telekommunikationsgesetz (TKG), München: C.H. Beck 2002, (zitiert: *Scheurle*, in: Scheurle/Mayen)

Scheurle, Klaus-Dieter/Mayen/Thomas (Hrsg.): Telekommunikationsgesetz (TKG), München: C.H. Beck, 2002, (zitiert: *Bearbeiter*, in: Scheurle/Mayen)

Schild, Hans-Hermann: Die Verwertung von Abhörerkenntnissen aus einer Telefonüberwachung gem. § 100 a StPO zu Zwecken der Gefahrenabwehr, ZRP 1991, S. 311

Schily, Otto: Nachbesserungsbedarf bei der Wohnraumüberwachung? ZRP 1999, S. 129 - 132

Schmidbauer, Wilhelm, in: Schmidbauer/Steiner/Roese, Bayerisches Polizeiaufgabengesetz und bayerisches Polizeiorganisationsgesetz, 2. Auflage, München: C.H. Beck 2006, (zitiert: *Schmidbauer*, in: Schmidbauer/Steiner/Roese)

Schmidbauer, Wilhelm/Steiner, Udo/Roese, Eberhard: Bayerisches Polizeiaufgabengesetz und bayerisches Polizeiorganisationsgesetz, 2. Auflage, München: C.H. Beck 2006, (zitiert: *Bearbeiter*, in: Schmidbauer/Steiner/Roese)

Schmidt-Aßmann, Eberhard: in: Maunz/Dürig, Grundgesetz Kommentar, Band III, Art. 17 – 27, Loseblattsammlung, Stand: Dezember 2007, 51. Ergänzungslieferung zur 1. Auflage, München: C.H. Beck 2008, (zitiert: *Schmidt-Aßmann*, in: Maunz/Dürig)

- Deutsches und Europäisches Verwaltungsrecht – Wechselseitige Einwirkungen – , DVBl. 1993, S. 924 - 936

Schmidt-Aßmann, Eberhard/Hoffmann-Riem, Wolfgang (Hrsg.): Strukturen des Europäischen Verwaltungsrechts, (Schriften zur Reform des Verwaltungsrechts, Band 6, hrsg. von Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard), Baden-Baden: Nomos 1999, (zitiert: *Bearbeiter*, in: Schmidt-Aßmann/Hoffmann-Riem)

Schmidt-Bleibtreu, Bruno/Klein, Franz: Kommentar zum Grundgesetz, 10. Auflage, München: Luchterhand 2004, (zitiert: *Bearbeiter*, in: Schmidt-Bleibtreu/Klein)

Schmidt, Joachim/Königshofen, Thomas/Zwach, Ulrich: Telekommunikationsrecht der Bundesrepublik Deutschland – TKR - , Rechtsvorschriften und Erläuterungen, Ordner 2, Stand: 2003, Heidelberg, R.v. Decker 2003, (zitiert: *Bearbeiter*, in: Schmidt/Königshofen/Zwach)

Schmitt Glaeser, Walter, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Band VI, Freiheitsrechte, 2. Auflage, Heidelberg: C.F. Müller 2001, (zitiert: *Schmitt Glaeser*, in: HStR VI)

Schmitt Glaeser, Walter/Degenhart, Christoph: Koordinationspflicht der Länder im Rundfunkwesen – Zur Einspeisung herangeführter privater Programme in Kabelanlagen, AfP 17 (1986), S. 173 - 187

Schneider, Werner: Verwaltungsvollstreckungsgesetz für Baden-Württemberg, Taschenkommentar, Stuttgart u.a.: Boorberg 1974

Schoch, Friedrich, in: Schmidt-Aßmann/Hoffmann-Riem (Hrsg.), Strukturen des Europäischen Verwaltungsrechts, (Schriften zur Reform des Verwaltungsrechts, Band 6, hrsg. von Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard), Baden-Baden: Nomos 1999, (zitiert: *Schoch*, in: Schmidt-Aßmann/Hoffman-Riem)

- Grundfälle zum Polizei- und Ordnungsrecht, Jus 1994, S. 391 - 397

Schönke, Adolf/Schröder, Horst/Cramer, Peter: Strafgesetzbuch, Kommentar, 27. Auflage, München: C.H. Beck 2006 (zitiert: *Bearbeiter*, in: Schönke/Schröder)

Schoreit, Armin: Polizeiliche Kriminalakten als Grundlage der Informationsverarbeitung, KritV 1988, S. 157 - 177

Schröder, Meinhard: Der Vollzug der Europäischen Abfallverbringungsverordnung als Rechtsproblem, in: Kley/Sünner/Willemsen (Hrsg.), Festschrift für Wolfgang Ritter zum 70. Geburtstag, Steuerrecht, Steuer- und Rechtspolitik, Wirtschaftsrecht und Unternehmensverfassung, Umweltrecht, Köln: Verlag Dr. Otto Schmidt, 1997, S. 957 – 971, (zitiert: *Schröder*, in: FS für Ritter)

Schulze-Fielitz, Helmuth, in: Dreier (Hrsg.), Grundgesetz Kommentar, Band II, Art. 20 – 82, 2. Auflage, Tübingen: Mohr Siebeck 2006, (zitiert: *Schulze-Fielitz*, in: Dreier)

Schuppert, Gunnar Folke, in: Wassermann (Hrsg.), Kommentar zum Grundgesetz für die Bundesrepublik Deutschland, Reihe Alternativkommentare, Band 1, Art. 1 – 37, 2. Auflage, Neuwied: Luchterhand 1989, (zitiert: *Schuppert*, in: AK-GG)

Schwabe, Jürgen: Die polizeiliche Datenerhebung in oder aus Wohnungen mit Hilfe technischer Mittel, JZ 1993, S. 867 - 874

Schwagerl, H. Joachim: Verfassungsschutz in der Bundesrepublik Deutschland, Heidelberg: C.F. Müller 1985, (zitiert: *Schwagerl*, 1985)

Schwarze, Jürgen: Der Schutz der Grundrechte durch den EuGH, NJW 2005, S. 3459 - 3466

Schweckendieck, Helmut: Dateien zur „vorbeugenden Verbrechensbekämpfung" im Lichte der Rechtsprechung zu § 81 b Alt. 2 StPO, ZRP 1989, S. 125 - 127

Seibert, Max-Jürgen: Die Bindungswirkung von Verwaltungsakten, Baden-Baden: Nomos 1989, (zitiert: *Seibert*, 1989)

Seidl-Hohenveldern, Ignaz (Hrsg.): Völkerrecht – Lexikon des Rechts, 3. Auflage, Neuwied und Kriftel: Luchterhand 2001, (zitiert: *Bearbeiter*, in: Seidl-Hohenveldern)

Siebrecht, Michael: Die polizeiliche Datenverarbeitung im Kompetenzstreit zwischen Polizei- und Prozessrecht, JZ 1996, S. 711 - 714

Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz, 6. Auflage, Baden-Baden: Nomos 2006, (zitiert: *Bearbeiter*, in: Simitis)

Sommermann, Karl-Peter, in: von Mangoldt/Klein/Starck (Hrsg.), Bonner Grundgesetz Kommentar, Band 2: Art. 20 bis 78, 5. Auflage, München: Verlag Franz Vahlen 2005, (zitiert: *Sommermann*, in: v.Mangoldt/Klein/Starck)

Spendel, Günter, in: Jähnke/Laufhütte/Odersky (Hrsg.), Strafgesetzbuch, Leipziger Kommentar, Großkommentar, Zweiter Band, §§ 32 bis 60, 11. Auflage, Berlin: De Gruyter 2003 , (zitiert: *Spendel*, in: LK)

Spiegel, Gerald: Spuren im Netz, DuD 2003, S. 265 - 269

Sproß, Joachim: Das Hamburgische Sicherheits- und Polizeigesetz in einer verfassungsrechtlichen Würdigung, NVwZ 1992, S. 642 - 645

Starck, Christian, in: von Mangoldt/Klein/Starck (Hrsg.), Kommentar zum Grundgesetz, Band 1: Präambel, Art. 1 – 19, 5. Auflage, München: Verlag Franz Vahlen 2005, (zitiert: *Starck*, in: v.Mangoldt/Klein/Starck)

Stein, Torsten/Buttlar, Christian von: Völkerrecht, 11. Auflage, Köln u.a.: Carl Heymanns Verlag: 2005, (zitiert: *Stein/v.Buttlar*, 2005)

Steinberger, Rudolf: Grenzüberschreitende Informationsansprüche im Bundesstaat – untersucht am Beispiel des innerstaatlichen atomrechtlichen Nachbarrechts, NJW 1987, S. 2345 - 2351

Steiner, Udo (Hrsg.): Besonderes Verwaltungsrecht, Ein Lehrbuch, 8. Auflage, Heidelberg: C.F. Müller 2006, (zitiert: *Bearbeiter*, in: Steiner)

Stenger, Hans-Jürgen: Mailboxen, Probleme im Beweissicherungsverfahren, CR 1990, S. 786 - 794

Stern, Klaus: Das Staatsrecht der Bundesrepublik Deutschland, Band III, Allgemeine Lehren der Grundrechte, 2. Halbband, München: C.H. Beck 1994, (zitiert: *Stern*, Staatsrecht, Band III/2)

- Das Staatsrecht der Bundesrepublik Deutschland, Band III, Allgemeine Lehren der Grundrechte, 1. Halbband, München: C.H. Beck 1988, (zitiert: *Stern*, Staatsrecht, Band III/1)

- Das Staatsrecht der Bundesrepublik Deutschland, Band I, Grundbegriffe und Grundlagen des Staatsrechts, Strukturprinzipien der Verfassung, München: C.H. Beck 1984, (zitiert: *Stern*, Staatsrecht, Band I)

Streinz, Rudolf: Europarecht, 7. Auflage, Heidelberg: C.F. Müller 2005, (zitiert: *Streinz*, 2005)

Stümper, Alfred: Rechtspolitische Nachlese zum „Großen Lauschangriff“, ZRP 1998, S. 463 - 465

Summa, Harald A.: Was sagen die Internetprovider? in: Holznagel/Nelles/Sokol, Die neue TKÜV (Telekommunikations-Überwachungsverordnung), Die Probleme in Recht und Praxis (Schriftenreihe Information und Recht, Band 27, hrsg. von Hoeren, Thomas u.a.), München: C.H. Beck 2002, S. 23 – 33, (zitiert: *Summa*, in: Holznagel/Nelles/Sokol)

Sydow, Gernot: Verwaltungskooperation in der Europäischen Union. Zur horizontalen und vertikalen Zusammenarbeit der europäischen Verwaltungen am Beispiel des Produktzulassungsrechts, Jus Publicum, Beiträge zum Öffentlichen Recht Band 118, Tübingen: Mohr Siebeck 2004 (zitiert: *Sydow*, 2004)

Tinnefeld, Marie-Theres/Schuster, Heidi: Mangel an Vertrauen in die Telekommunikation, DuD 2005, S. 78 - 83.

Tröndle, Herbert/Fischer, Thomas: Strafgesetzbuch und Nebengesetze, 54. Auflage, München: C.H. Beck 2007

Trute, Hans-Heinrich, in: Trute/Spoerr/Bosch, Telekommunikationsgesetz mit FTEG, Kommentar, Berlin und New York: De Gruyter 2001; (zitiert: *Trute*, in: Trute Spoerr/Bosch)

Trute, Hans Heinrich/Spoerr, Wolfgang/Bosch, Wolfgang: Telekommunikationsgesetz mit FTEG, Kommentar, Berlin und NewYork: De Gruyter 2001, (zitiert: *Bearbeiter*, in: Trute/Spoerr/Bosch)

Ule, Carl Hermann: Zur räumlichen Geltung von Verwaltungsakten im Bundesstaat, JZ 1961, S. 622 - 624

Ulmer, Claus D./Schrief, Dorothee: Vorratsdatenspeicherung durch die Hintertür, DuD 2004, S. 591 - 597

Unger, Christoph/Siefken, Peter, in: Böhrenz/Unger/Siefken, Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung mit Ausführungsbestimmungen und Erläuterungen für Praxis und Ausbildung, 8. Auflage, Hannover: Pinkvoss Verlag 2005, (zitiert: *Unger/Siefken*, in: Böhrenz/Unger/Siefken)

Vassilaki, Irini E.: Die Überwachung des Fernmeldeverkehrs nach der Neufassung der §§ 100 a, 100 b StPO - Erweiterung von staatlichen Grundrechtseingriffen? JR 2000, 446 - 451

Villiger, Mark E.: Handbuch der Europäischen Menschenrechtskonvention (EMRK), 2. Auflage, Zürich: Schulthess Polygraphischer Verlag 1999, (zitiert: *Villinger*, 1999)

Walden, Marcus: Zweckbindung und –änderung präventiv und repressiv erhobener Daten im Bereich der Polizei, Dissertation (Schriften zum Recht des Informationsverkehrs und der Informationstechnik, Band 14, hrsg. von Ehmann, Horst/Pitschas, Rainer), Berlin: Duncker & Humblot 1996, (zitiert: *Walden*, 1996)

Walz, Stefan: Datenschutz und Telekommunikation (II) – Konsequenzen des Poststrukturgesetzes, CR 1990, S. 138 - 142

Wassermann, Rudolf (Hrsg.): Kommentar zum Grundgesetz für die Bundesrepublik Deutschland, Reihe Alternativkommentare, Band 1, Art. 1 – 37, 2. Auflage, Neuwied: Luchterhand 1989, (zitiert: *Bearbeiter*, in: AK-GG)

Weber, Albrecht: Die Europäische Grundrechtscharta – auf dem Weg zu einer europäischen Verfassung, NJW 2000, S. 537 - 544

Weitemeier, Ingmar/Große, Wolfgang: Telefonüberwachung aus präventivpolizeilichen Gründen – oder: Irritationen beim Eingriffsrecht müssen beseitigt werden, Kriminalistik 1997, S. 335 - 338

Welp, Jürgen: Verbindungsdaten, Zur Reform des Auskunftsrechts (§§ 100 g, 100h StPO), GA 2002, S. 535 – 556

- Anmerkung zum Urteil des BGH vom 08.10.1993 – 2 StR 400/93 – , NStZ 1994, S. 294 - 295

- Zufallsfunde bei der Telefonüberwachung, Jura 1981, S. 472 - 484

Wilms, Heinrich/Masing, Johannes/Jochum, Georg (Hrsg.): Telekommunikationsgesetz, Kommentar und Vorschriftensammlung, 4. Lieferung Juli 2006, Stuttgart: Kohlhammer 2007, (zitiert: *Bearbeiter*, in: Wilms/Masing/Jochum)

Wissmann, Martin (Hrsg.): Telekommunikationsrecht, Praxishandbuch (Schriftenreihe Kommunikation & Recht, Band 8, hrsg. von: Holznagel, Bernd/Koenig, Christian/Scherer, Joachim u.a.), 2. Auflage, Frankfurt am Main: Verlag Recht und Wirtschaft GmbH 2006, (zitiert: *Bearbeiter*, in: Wissmann)

Wittern, Felix, in: Geppert u.a. (Hrsg.), Beck`scher TKG – Kommentar, 3. Auflage, München: C.H. Beck 2006, (zitiert: *Wittern*, in: BeckTKG-Komm)

Wittern, Felix/Schuster, Fabian, in: Geppert u.a. (Hrsg.), Beck`scher TKG – Kommentar, 3. Auflage, München: C.H. Beck 2006, (zitiert: *Wittern/Schuster*, in: BeckTKG-Komm)

Wolf, Heinz/Stephan, Ulrich: Polizeigesetz für Baden-Württemberg, 5. Auflage, Stuttgart u.a.: Boorberg 1999, (zitiert: *Wolf/Stephan*)

Wolter, Henner: Die Richtervorbehalte im Polizeirecht, DÖV 1997, S. 939 - 948

Wolter, Jürgen: Polizeiliche und justitielle Datenübermittlungen in Deutschland und der Europäischen Union – Polizei und Europol, Staatsanwaltschaft und Eurojust, in: Wolter u.a. (Hrsg.), Datenübermittlungen und Vorermittlungen, Festgabe für Hans Hilger, Heidelberg: C.F. Müller 2003, S. 275 – 323, (zitiert: *Wolter*, in: FG für Hilger)

- 35 Jahre Verfahrensrechtskultur und Strafprozeßverfassungsrecht in Ansehung von Freiheitsentziehung, (DNA-)Identifizierung und Überwachung, Hans Joachim Hirsch zum 70. Geburtstag, GA 1999, S. 158 - 181

Wolter, Jürgen u.a. (Hrsg.): Datenübermittlungen und Vorermittlungen, Festgabe für Hans Hilger, Heidelberg: C.F. Müller 2003, (zitiert: *Bearbeiter*, in: FG für Hilger)

Wuermeling, Ulrich/Felixberger, Stefan: Staatliche Überwachung der Telekommunikation, CR 1997, S. 555 - 561

- Fernmeldegeheimnis und Datenschutz im Telekommunikationsgesetz, CR 1997, S. 230 – 238

Würkner, Joachim: Effektivierung des Grundrechtsschutzes durch Grundrechtskumulation? DÖV 1992, S. 150 - 154

Würtenberger, Thomas: Verwaltungsprozessrecht, Ein Studienbuch, 2. Auflage, München: C.H. Beck 2006, (zitiert: *Würtenberger*, 2006)

- Übermittlung und Verwendung strafprozessual erhobener Daten für präventivpolizeiliche Zwecke, in: Wolter u.a. (Hrsg.), Datenübermittlungen und Vorermittlungen, Festgabe für Hans Hilger, Heidelberg: C.F. Müller 2003, S. 263 - 274, (zitiert: *Würtenberger*, in: FG für Hilger)

- Polizei- und Ordnungsrecht, in: Achterberg/Püttner/Würtenberger (Hrsg.), Besonderes Verwaltungsrecht, Band II, Kommunal-, Haushalts-, Abgaben-, Ordnungs-, Sozial-, Dienstrecht, 2. Auflage, Heidelberg: C.F. Müller 2000, S. 381 – 534, (zitiert: *Würtenberger*, in: Achterberg/Püttner/Würtenberger, Band II)

Würtenberger, Thomas/Heckmann, Dirk: Polizeirecht in Baden-Württemberg, 6. Auflage, Heidelberg: C.F. Müller 2005, (zitiert: *Würtenberger/Heckmann*, 2005)

Würtenberger, Thomas/Heckmann, Dirk/Riggert, Rainer: Polizeirecht in Baden-Württemberg, 3. Auflage, Heidelberg: C.F. Müller 1993, (zitiert: *Würtenberger/Heckmann/Riggert*, 1993)

Würz, Karl: Polizeiaufgaben und Datenschutz in Baden-Württemberg, Stuttgart u.a.: Boorberg 1993 (zitiert: *Würz*, 1993)

Zeitler, Stefan: Allgemeines und Besonderes Polizeirecht für Baden-Württemberg, Stuttgart u.a.: Kohlhammer 1998, (zitiert: *Zeitler*, 1998)

Zerres, Achim, in: Scheurle/Mayen (Hrsg.), Telekommunikationsgesetz (TKG), München: C.H. Beck 2002, (zitiert: *Zerres*, in: Scheurle/Mayen)

Zippelius, Reinhold/Würtenberger, Thomas: Deutsches Staatsrecht, Ein Studienbuch, 31. Auflage, München: C.H. Beck 2005 (zitiert: *Zippelius/Würtenberger*, 2005)

Zöller, Mark Alexander: Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten, Zur Vernetzung von Strafverfolgung und Kriminalitätsverhütung im Zeitalter von multimedialer Kommunikation und Persönlichkeitsschutz, Dissertation (Mannheimer rechtswissenschaftliche Abhandlungen, Band 27, hrsg. von der Fakultät für Rechtswissenschaft der Universität Mannheim), Heidelberg: C.F. Müller, 2002, (zitiert: *Zöller*, 2002)

Zwiehoff, Gabriele (Hrsg.): Großer Lauschangriff, Die Entstehung des Gesetzes zur Änderung des Grundgesetzes vom 26. März 1998 und des Gesetzes zur Änderung der Strafprozessordnung vom 04. Mai 1998 in der Presseberichterstattung 1997/98 mit einer Einleitung von Bundestagsvizepräsident a.D. Burkhard Hirsch und einem Kommentar von Prof. Dr. Jürgen Welp (Juristische Zeitgeschichte, Band 6, hrsg. von Vormbaum, Thomas, Abteilung 5: Juristisches Zeitgeschehen, Rechtspolitik und Justiz aus zeitgenössischer Perspektive, hrsg. von Huff, Martin W./Salditt, Franz/Vormbaum, Thomas), Baden-Baden: Nomos 2000, (zitiert: *Zwiehoff*, 2000)