Stiftervereinigung der Presse e.V., Berlin

Gesellschaft für Datenschutz und Datensicherung e.V. (GDD), Bonn

(Hrsg.)

Gutachten:

Datenschutz- und presserechtliche Bewertung der „Vorratsdatenspeicherung“

Erstellt von

Professor Peter Gola
(Vorstandsvorsitzender der GDD e.V., Bonn)

Christoph Klug
(Rechtsanwalt, Köln)

Yvette Reif, LL.M.
(Rechtsanwältin, Bonn)

Gutachten: Datenschutz und presserechtliche Bewertung der „Vorratsdatenspeicherung“

Herausgeber: Stiftervereinigung der Presse e.V. und
Gesellschaft für Datenschutz und Datensicherung e.V. (GDD)

Inhaltsverzeichnis

A Zusammenfassung der Ergebnisse

Am 18. April 2007 hat das Bundeskabinett den Entwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ beschlossen. Die darin vorgesehene Umsetzung der EG-Richtlinie über die Vorratsdatenspeicherung in nationales Recht führt zu einem verfassungsrechtlichen Spannungsfeld zwischen der effektiven Verhütung und Verfolgung von Straftaten und der Wahrung des Rechts auf informationelle Selbstbestimmung und der Pressefreiheit.

Die Abkehr von einem grundsätzlichen Verbot anlassloser Vorratsspeicherung durch die gesetzliche Regelung einer Pflicht zur massenhaften Bevorratung mit Daten unbescholtener Nutzer bedeutet einen Paradigmenwechsel.

Nach dem Ergebnis der vorliegenden verfassungsrechtlichen Würdigung würden die Nutzer der betroffenen Kommunikationsformen (Telefonfestnetz und Mobilfunk, Internetzugang, Internet-E-Mail und Internet-Telefonie) durch die vorgesehene Richtlinienumsetzung in ihrem Grundrecht auf informationelle Selbstbestimmung in seiner speziellen Ausprägung als Fernmeldegeheimnis (Artikel 10 Abs. 1 Var. 3 GG) verletzt.

Daneben würde auch das staatspolitisch bedeutsame Grundrecht der Pressefreiheit (Artikel 5 Abs. 1 S. 2 Alt. 1 GG) unter dem Aspekt der vertraulichen Kommunikation zwischen Pressevertreter und Informant verletzt.

Die Bundesregierung beabsichtigt, die - gegebenenfalls europarechtswidrige - Richtlinie zur Vorratsdatenspeicherung gleichwohl umzusetzen.

Die materielle Grundrechtswidrigkeit der Vorratsdatenspeicherung verpflichtet den deutschen Gesetzgeber, alle sich aus der Richtlinie 2006/24/EG ergebenden Spielräume zum Schutz der Grundrechte auszuschöpfen (verfassungsschonende Regulierung). Insbesondere eine überobligatorische Richtlinienumsetzung ist zu vermeiden. Denn der Vorrang des Gemeinschaftsrechts kann als

„Rechtfertigung“ für Grundrechtsverletzungen in Deutschland nur insoweit tragen, als dieses dem nationalen Gesetzgeber zwingende Vorgaben macht.

Der oben genannte Regierungsentwurf geht über eine Umsetzung von Richtlinienvorgaben hinaus und trägt dem Gebot der Verfassungsschonung nicht hinreichend Rechnung.

Die Richtlinie knüpft die Speicherpflicht an die Ermittlung, Feststellung und Verfolgung von schweren Straftaten. Da sowohl die Bestimmung der schweren Straftat als auch das Verfahren des Zugriffs auf die bevorrateten Daten den Mitgliedstaaten überlassen ist, kann das Bundesverfassungsgericht die Verfassungsmäßigkeit diesbezüglicher nationaler Zweckbegrenzungsnormen - auch mit Blick auf den Vorrang des Gemeinschaftsrechts - überprüfen. Insbesondere wären die in dem Regierungsentwurf enthaltenen Regelungen vom Bundesverfassungsgericht insofern überprüfbar, als auch Straftaten erfasst werden, die nicht schwer sind, aber mittels einer Telekommunikationsendeinrichtung begangen werden (überobligatorische Umsetzung). Auch die nunmehr vorgesehene präventive Datenverwendung für Zwecke der Gefahrenabwehr geht über die Vorgaben der Richtlinie 2006/24/EG hinaus.

Das Gebot zur verfassungsschonenden Richtlinienumsetzung, die durch die Vorratsdatenspeicherung erheblich verstärkte Eingriffsintensität sowie die Vorgaben des Bundesverfassungsgerichts zum Schutz des Rechts auf informationelle Selbstbestimmung machen eine verfahrensrechtliche Sicherung des Fernmeldegeheimnisses erforderlich.

Der staatliche Zugriff auf „Vorratsdaten“ sollte - nicht zuletzt mit Blick auf den Bestimmtheits- und Verhältnismäßigkeitsgrundsatz - auf Straftaten nach § 139 StGB begrenzt werden. Hierzu bietet sich die Schaffung eines eigenständigen, speziell auf „Vorratsdaten“ bezogenen Zugriffstatbestands an.

Der festgestellte Paradigmenwechsel wirkt sich im Bereich der - zuletzt ohnehin verstärkt bedrohten - Pressefreiheit in besonderem Maße aus, denn mit der Vorratsdatenspeicherung wird auch jede elektronische Kontaktaufnahme per Telefon, E-Mail, SMS

und Internet von oder zu einem Pressevertreter für einen längeren Zeitraum rückverfolgbar. Dieser Umstand lässt befürchten, dass ein Einschüchterungseffekt eintritt und die Informationsquellen der Presse weniger werden.

Angesichts der verschärften Gefährdungslage bedarf es einer Anpassung der Verfahrensvorschriften, die der aktuellen Arbeitsweise der Presse und dem Informantenschutz unter den Bedingungen der Informationsgesellschaft angemessen Rechnung trägt. Insofern ist eine Einbeziehung der Pressevertreter in den Schutz des § 53b Abs. 1 StPO-E angezeigt. Damit wäre das Verlangen einer Auskunft über Telekommunikationsverbindungen, die von oder zu einem Pressevertreter hergestellt wurden, künftig nur zulässig, wenn gegen den Pressevertreter ein hinreichender Verdacht strafbarer Beteiligung gemäß § 53b Abs. 4 StPO-E besteht. Unter Missachtung dieses Schutzes erlangte Auskünfte dürften nicht verwertet werden (§ 53b Abs. 1 S. 2 StPO-E).

Im Rahmen der anstehenden Änderung des TKG sollte eine dahingehende gesetzliche Klarstellung erfolgen, dass auch die Verknüpfung einer dynamischen IP-Adresse mit den Bestandsdaten eines konkreten Nutzers dem Richtervorbehalt unterfällt.

Mit Blick auf die eventuelle Europarechtswidrigkeit der Richtlinie 2006/24/EG und zur Ermöglichung einer weitergehenden Evaluation der Speicherungs-, Verwendungs- und Zugriffsvorschriften durch eine unabhängige Stelle sollten die entsprechenden gesetzlichen Regelungen außerdem angemessen befristet werden.

B Gutachten

1. Ausgangslage

Im April 2006 wurde im Amtsblatt der Europäischen Union[1] die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG veröffentlicht. Die Richtlinie ist bis zum 15. September 2007 bzw. hinsichtlich der Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail spätestens bis zum 15. März 2009 in nationales Recht umzusetzen.

Seit April 2007 liegt ein Regierungsentwurf[2] für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ vor, welcher zum 1. Januar 2008 in Kraft treten soll (Artikel 16 des Entwurfs). Von der in der Richtlinie vorgesehenen Aufschubmöglichkeit hinsichtlich der Speicherung von Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail soll kein Gebrauch gemacht werden.

1.1. Duale Zielsetzung und Gegenstand der Richtlinie 2006/24/EG

Ziel der Richtlinie ist die Harmonisierung der mitgliedstaatlichen Vorschriften zu den Speicherpflichten von Providern der Informations- und Kommunikationsbranche im Hinblick auf die bei diesen anfallenden Verkehrs- und Standortdaten der Nutzer (Erwägungsgründe 5 und 6 der Richtlinie, Artikel 1 der Richtlinie).

1 Amtsblatt der Europäischen Union, L 105/54.
2 BR-Dr 275/07.

Daneben soll mit der Festlegung von Speicherfristen (gemäß Artikel 6 der Richtlinie mindestens sechs Monate und höchstens zwei Jahre) sichergestellt werden, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung schwerer Straftaten verfügbar sind. Die Definition dessen, was unter den Begriff der schweren Straftaten subsumierbar ist, überlässt die Richtlinie den nationalen Gesetzgebern.

Die Richtlinie bezieht sich auf folgende Datenkategorien:

- zur Rückverfolgung und Identifizierung der Quelle einer Nachricht benötigte Daten (Artikel 5 Abs. 1 lit. a der Richtlinie),
- zur Identifizierung des Adressaten einer Nachricht benötigte Daten (Artikel 5 Abs. 1 lit. b der Richtlinie),
- zur Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung benötigte Daten (Artikel 5 Abs. 1 lit. c der Richtlinie),
- zur Bestimmung der Art einer Nachrichtenübermittlung benötigte Daten (Artikel 5 Abs. 1 lit. d der Richtlinie),
- zur Bestimmung der Endeinrichtung oder der vorgeblichen Endeinrichtung von Benutzern benötigte Daten (Artikel 5 Abs. 1 lit. e der Richtlinie) sowie
- zur Bestimmung des Standorts mobiler Geräte benötigte Daten (Artikel 5 Abs. 1 lit. f der Richtlinie).

Im Einzelnen sind folgende Informationen zu speichern (vgl. Artikel 5 Abs. 1 der Richtlinie):

Im Hinblick auf das Telefonfestnetz und den Mobilfunk:

- Rufnummer des anrufenden/angerufenen Anschlusses
- Name und Anschrift des jeweiligen Teilnehmers oder registrierten Benutzers
- Datum und Uhrzeit des Beginns und des Endes eines Kommunikationsvorganges
- in Anspruch genommene Telefondienste

- internationale Mobilteilnehmerkennung (IMSI) des anrufenden/angerufenen Anschlusses
- internationale Mobilfunkgeräteerkennung (IMEI) des anrufenden/angerufenen Anschlusses
- im Falle vorbezahlter anonymer Dienste: Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Kennung des Standorts (Cell-ID), an dem der Dienst aktiviert wurde (Mobilfunk)

Im Hinblick auf Internetzugang, Internet-E-Mail und Internet-Telefonie:

- zugewiesene Benutzerkennungen bzw. Rufnummern (auch des vorgesehenen Empfängers eines Anrufs/einer Nachricht)
- Name und Anschrift des Teilnehmers oder registrierten Benutzers, dem eine IP-Adresse, Benutzerkennung oder Rufnummer zum Zeitpunkt der Nachricht zugewiesen war
- Datum und Uhrzeit der An- und Abmeldung beim Internetzugangsdienst auf der Grundlage einer bestimmten Zeitzone, zusammen mit der vom Internetzugangsanbieter einer Verbindung zugewiesenen dynamischen oder statischen IP-Adresse und die Benutzerkennung des Teilnehmers oder des registrierten Benutzers
- Datum und Uhrzeit der An- und Abmeldung beim Internet-E-Mail-Dienst oder Internet-Telefonie-Dienst auf der Grundlage einer bestimmten Zeitzone
- in Anspruch genommene Internetdienste
- Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss
- digitaler Teilnehmeranschluss (DSL) oder ein anderer Endpunkt des Urhebers des Kommunikationsvorgangs

Im Hinblick auf die Bestimmung des Standorts mobiler Geräte:

- Standortkennung (Cell-ID) bei Beginn der Verbindung
- Daten zur geografischen Ortung von Funkzellen durch Bezugnahme auf ihre Standortkennung (Cell-ID) während des Zeitraums, in dem die Vorratsspeicherung der Kommunikationsdaten erfolgt

Sofern die Voraussetzungen von Artikel 3 Abs. 2 der Richtlinie vorliegen, sind auch Daten zu speichern, die im Zusammenhang mit erfolglosen Anrufversuchen anfallen. Ausdrücklich nicht zu speichern sind nach der Richtlinie dagegen Daten, die Aufschluss über den Inhalt einer Kommunikation geben (Artikel 5 Abs. 2 der Richtlinie).

Adressaten der Verpflichtung zur Vorratsdatenspeicherung sind Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste und Betreiber öffentlicher Kommunikationsnetze (Artikel 3 Abs. 1 der Richtlinie).

In Bezug auf den staatlichen Zugriff auf die vorzuhaltenden Daten stellt die Richtlinie auf schwere Straftaten ab (Artikel 1 Abs. 1). Ein Spielraum verbleibt dem nationalen Gesetzgeber hinsichtlich der Definition der schweren Straftat (Artikel 1 Abs. 1) und des Verfahrens des staatlichen Zugriffs (Artikel 4).

1.2. Nationale Umsetzung der Richtlinie

Der Gesetzgeber hatte sich schon länger eine Reform der Regelungen über verdeckte Ermittlungsmaßnahmen in der Strafprozessordnung vorgenommen. Bereits anlässlich der Verlängerung der Geltungsdauer der §§ 100g, 100h StPO bis zum 31. Dezember 2007 hat die Bundesregierung darauf hingewiesen, dass umfassendere Änderungen im Bereich der Überwachung der Telekommunikation noch ausstehen und gleichzeitig festgestellt, dass sich die §§ 100g, 100h StPO im Zuge einer Gesamtnovellierung in ein harmonisches Gesamtsystem der strafprozessualen heimlichen

Ermittlungsmethoden einzugliedern haben[3].

Inzwischen hat die Bundesregierung den bereits angesprochenen Entwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ vorgelegt[4]. Danach regelt § 113a TKG-E die Speicherungspflichten der Provider und § 113b TKG-E die Verwendung der gespeicherten Daten.

1.3. Verfassungsrechtliches Spannungsfeld - Effektive Verhütung und Verfolgung von Straftaten unter Wahrung der Freiheitsrechte

Durch die Umsetzung der Richtlinie wird das Telekommunikationsverhalten eines jeden Nutzers unabhängig vom Bestehen eines konkreten Verdachts für einen längeren Zeitraum nachvollziehbar. Bereits allgemein stellt sich die Frage, inwieweit dies mit den Bestimmungen des Grundgesetzes (Fernmeldegeheimnis gemäß Artikel 10 Abs. 1 Var. 3 GG, Recht auf informationelle Selbstbestimmung gemäß Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 GG) vereinbar sein kann[5].

---

3 BT-Dr 15/3349, S. 6. Der Bundestag hat die Bundesregierung ferner aufgefordert, einen Erfahrungsbericht über die Anwendungspraxis der §§ 100g, 100h StPO anzufertigen. Zu diesem Zweck erteilte das Bundesministerium der Justiz dem Max-Planck-Institut für ausländisches und internationales Strafrecht den Auftrag zur Durchführung einer wissenschaftlichen Studie über die Rechtswirklichkeit der Auskunftserteilung nach §§ 100g, 100h StPO; die Ergebnisse einer bereits zuvor in Auftrag gegebenen Studie zu den §§ 100a, 100b StPO sowie anderer verdeckter Ermittlungsmaßnahmen liegen inzwischen vor (http://www.bmj.bund.de/files/-/134/Abschlussbericht.pdf).

4 BR-Dr 275/07.

5 BT-Dr 16/128 „Gegen eine europaweit verpflichtende Vorratsdatenspeicherung“; BT-Dr 16/237 „Freiheit des Telefonverkehrs vor Zwangsspeicherungen“; BITKOM-Stellungnahme vom 22.05.2007, S. 4 f. (http://www.bitkom.org/files/documents/Stellungnahme_BITKOM_RegE_ Neuregelung_TKUe_22_05_07.pdf); Stellungnahme des Unabhängigen Landeszentrums für den Datenschutz Schleswig-Holstein vom 27.06.2007, S. 18 ff. (https://www. da-

Eine besondere Gefährdungslage resultiert aus der Umsetzung der Richtlinie zur Vorratsdatenspeicherung im Bereich der Presse. Wenn jede elektronische Kontaktaufnahme mit einem Pressevertreter über einen längeren Zeitraum rückverfolgbar ist, ist nicht auszuschließen, dass potenzielle Informanten vor einer Kontaktaufnahme mit der Presse zurückschrecken und diese dadurch in der Wahrnehmung ihrer verfassungsrechtlich geschützten Aufgaben behindert wird[6].

Der Bundestag hat die Bundesregierung - nicht zuletzt mit Blick auf das Recht auf informationelle Selbstbestimmung - aufgefordert, mit den Regelungen zur Speicherungsdauer und den erfassten Datenarten nicht über die Mindestanforderungen der Richtlinie hinauszugehen[7]. Außerdem hat der Bundestag ausdrücklich darauf hingewiesen, dass die Abfrage der gespeicherten Daten die Presse- und Rundfunkfreiheit nach Artikel 5 Abs. 1 S. 2 GG berühren kann (Ziffer 10 der Drucksache) und gefordert, dass die

---

tenschutzzentrum.de/polizei/20070627-vorratsdatenspeicherung.pdf); Stellungnahme der Wissenschaftlichen Dienste des Deutschen Bundestages, S. 15 ff. (http://www.bundestag.de/bic/analysen/2006/zulaessigkeit_der_vorratsdatenspeicherung_nach_europaeischem_und_deutschem_recht.pdf); Leutheusser-Schnarrenberger, ZRP 2007, 9; Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (8.-9. März 2007) zur Vorratsdatenspeicherung (http://www.datenschutz. thueringen.de/veroeffentlichungen/entschliessungen/konferenz_73/Vorratsdatenspeicherung73.htm); Gemeinsame Stellungnahme des Arbeitskreises Vorratsdatenspeicherung, des Netzwerkes Neue Medien und der Neuen Richtervereinigung zum Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (http://www. vorratsdatenspeicherung.de/images/stellungnahme_vorratsdatenspeicherung. pdf); Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder in Deutschland, DuD 2004, 605; Breyer, S. 389 ff.; Ulmer/Schrief, DuD 2004, 593 ff.; Kühling, K&R 2004, 108 ff.; Vassilaki, MMR 2/2006, XIII.

6 Gemeinsame Stellungnahme von ARD, BDZV, DJV, Deutscher Presserat, VDZ, Ver.di, VPRT und ZDF vom 19.01.2007 (http://www.presserat.de/fileadmin/download/Stellungnahme_Telekommunikationsueberwachung.pdf).

7 Beschlussempfehlung „Speicherung mit Augenmaß - Effektive Strafverfolgung und Grundrechtswahrung“ vom 07.02.2006, BT-Dr 16/545, S. 4 (auch abgedruckt in RDV 2006, 86 ff.). Zur Annahme der Empfehlung vgl. Plenarprotokoll 16/19 vom 16.02.2006, S. 1430 (B).

Verfassungsgrundsätze und insbesondere das Berufsgeheimnis bei der Anwendung der Richtlinie gewahrt bleiben müssen (Ziffer 15 der Drucksache).

1.4. Vorrang des Gemeinschaftsrechts: „Solange II"-Entscheidung des Bundesverfassungsgerichts

Mit der „Solange II"-Entscheidung[8] hat das Bundesverfassungsgericht im Jahr 1986 den Vorrang des Gemeinschaftsrechts anerkannt und auf eine nationale Prüfung der Konformität des sekundären Gemeinschaftsrechts mit den deutschen Grundrechten verzichtet, „solange" nicht die EG die wesentlichen Strukturen des GG aushöhlt und an dem inzwischen erreichten europäischen Grundrechtsstandard festhält.

1992 wurde sodann Art. 23 GG neu geschaffen. Nach dieser Regelung kommt eine nationale Kontrolle des Gemeinschaftsrechts nur im Hinblick auf die Achtung der Grundprinzipien des GG (Demokratie, Rechts- und Sozialstaat, Föderalismus) und des Grundsatzes der Subsidiarität des Gemeinschaftsrechts in Betracht. Weiterhin wird klargestellt, dass der europäische Grundrechtsschutz dem deutschen Schutz nur „im Wesentlichen" vergleichbar sein muss. In der „Bananenmarkt"-Entscheidung[9] hat das Bundesverfassungsgericht dann erklärt, dass derartige Gefahren für die deutsche Verfassung nach dem derzeitigen Stand des Gemeinschaftsrechts kaum zu befürchten seien.

Dementsprechend erachtet das Bundesverfassungsgericht Verfassungsbeschwerden und Vorlagebeschlüsse, die aus abgeleitetem Gemeinschaftsrecht resultierende Grundrechtsverletzungen rügen, im Regelfall als „von vorneherein unzulässig".

Zu beachten ist allerdings, dass der Vorrang des Gemeinschaftsrechts als „Rechtfertigung" für Grundrechtsverletzungen in

---

8 Urteil des Bundesverfassungsgerichts vom 22.10.1986 - 2 BvR 197/83, NJW 1987, 577.

9 Urteil des Bundesverfassungsgerichts vom 07.06.2000 - 2 BvL 1/97, NJW 2000, 3124.

Deutschland nur insoweit tragen kann, als dieses dem nationalen Gesetzgeber zwingende Vorgaben macht. Hieraus folgt zum einen, dass das Bundesverfassungsgericht eine verfassungsrechtliche Überprüfung von überobligatorischen Umsetzungsmaßnahmen vornehmen kann. Zum anderen ergibt sich, dass der deutsche Gesetzgeber verpflichtet ist, alle sich aus dem jeweiligen Gemeinschaftsrecht ergebenden Spielräume zum Schutz der Grundrechte auszuschöpfen[10]. Auch insofern ist das Bundesverfassungsgericht prüfungsbefugt.

Sollte das Bundesverfassungsgericht Zweifel an der Gültigkeit der Richtlinie selbst haben, so ist gemäß Artikel 234 des Vertrages zur Gründung der Europäischen Gemeinschaft das so genannte Vorabentscheidungsverfahren durchzuführen.

1.5. Europarechtswidrigkeit der Richtlinie?

Nicht unumstritten ist bereits, ob die Richtlinie mit höherrangigem Gemeinschaftsrecht vereinbar ist. Insoweit werden Bedenken sowohl in formeller wie auch in materieller Hinsicht geäußert[11].

Eine verpflichtende Vorratsdatenspeicherung ist auf Initiative von Frankreich, Irland, Schweden und Großbritannien zunächst in der so genannten dritten Säule der Europäischen Union (polizeiliche und justizielle Zusammenarbeit in Strafsachen) vorgeschlagen worden. Am 28. April 2004 legten die genannten Staaten insoweit einen auf Artikel 31 Abs. 1 lit. c und Artikel 34 Abs. 2 lit. b des Vertrags über die Europäische Union gestützten Entwurf eines Rahmenbeschlusses vor[12]. Ziel war die angemessene Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, um ein hohes Maß an Schutz in einem Raum der Sicherheit, der Frei-

10 Vgl. hierzu im Einzelnen S. 49.

11 Vgl. Gemeinsame Stellungnahme des Arbeitskreises Vorratsdatenspeicherung, des Netzwerkes Neue Medien und der Neuen Richtervereinigung zum Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (Fn. 5).

12 Ratsdokument 8958/04.

heit und des Rechts zu erreichen (Erwägungsgrund 1 des Rahmenbeschlussentwurfs). Nach verschiedenen Kontroversen ist das Vorhaben allerdings schließlich als Richtlinie 2006/24/EG in der ersten Säule (Europäische Gemeinschaften) im Wege des Mitentscheidungsverfahrens nach Artikel 251 des Vertrags zur Gründung der Europäischen Gemeinschaft beschlossen worden. Zwar wird in den Erwägungsgründen 5 und 6 der Richtlinie auch die Beseitigung von Beeinträchtigungen des Binnenmarktes für elektronische Kommunikation angesprochen. Daneben ist aber auch die Verhütung bzw. Verfolgung schwerer Straftaten Regelungsgegenstand wie die Erwägungsgründe 5 bis 11 und insbesondere der Artikel 1 Abs. 1 der Richtlinie zeigen[13], so dass ein kompetenzgemäßer Richtlinienerlass teilweise angezweifelt wird[14]. Irland und die Slowakei haben mit der Begründung fehlender Zuständigkeit für den Richtlinienerlass Klage beim Europäischen Gerichtshof (EuGH) erhoben.

In materieller Hinsicht wird vielfach[15] angezweifelt, ob die Richt-

[13] Artikel 1 Abs. 1 der Richtlinie hat folgenden Inhalt: „Mit dieser Richtlinie sollen die Vorschriften der Mitgliedstaaten über die Pflichten von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes im Zusammenhang mit der Vorratsspeicherung bestimmter Daten, die von ihnen erzeugt oder verarbeitet werden, harmonisiert werden, um sicherzustellen, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden, zur Verfügung stehen."

[14] Vgl. etwa BT-Dr 16/1622 „Richtlinie zur Vorratsdatenspeicherung durch den Europäischen Gerichtshof prüfen lassen", S. 4 ff. Der Antrag wurde in der Bundestagssitzung vom 20.06.2006 mit den Stimmen der SPD- und Unionsfraktion abgelehnt, vgl. Plenarprotokoll 16/38 vom 20.06.2006, S. 3527 (D).

[15] Vgl. etwa Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (KOM(2005) 438 endg.), Amtsblatt der Europäischen Union, C 298/1, insbesondere Erwägungen Nr. 9, 10 und 24 ff.; Gemeinsame Stellungnahme des Arbeitskreises Vorratsdatenspeicherung, des Netzwerkes Neue Medien und der Neuen Richtervereinigung zum Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikati-

linie 2006/24/EG mit dem Recht auf Achtung des Privatlebens aus Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) vereinbar ist. Zwar ist die EG nicht Vertragspartner der EMRK, dennoch besteht voller Konventionsschutz gegenüber EG-Rechtsakten[16]. Unter anderem auf Artikel 8 EMRK stützt sich auch Artikel 8 der Grundrechte-Charta der Europäischen Union, der den Schutz personenbezogener Daten regelt. Die Charta entfaltet zwar zunächst keine unmittelbare Rechtswirkung[17], es wird aber erwartet, dass der EuGH sie in seine ständige Rechtsprechung miteinbeziehen wird[18].

1.6. Gegenstand der vorliegenden Untersuchung

Gegenstand der nachfolgenden Untersuchung ist nicht die Vereinbarkeit der Richtlinie mit dem Gemeinschaftsrecht. Nachgegangen wird vielmehr der Fragestellung, ob bzw. inwiefern die Richtlinienumsetzung mit dem Grundrecht auf informationelle Selbstbestimmung in seiner besonderen Ausprägung des Fernmeldegeheimnisses und der Pressefreiheit vereinbar ist.

Die Richtlinie enthält keine Pflicht zur automatischen Weiterleitung der Daten. Artikel 4 der Richtlinie sieht vielmehr vor, dass die Weiterleitung an die Behörden nur in bestimmten Fällen erfolgt und in Übereinstimmung mit dem innerstaatlichen Recht geregelt wird. Die Ausgestaltung der Voraussetzungen, unter denen die zuständigen Behörden Zugriff auf die Daten erhalten, ist also den nationalen Gesetzgebern überlassen. Nach dem inzwischen vorliegenden Regierungsentwurf soll die Speicherpflicht ihre Rechtsgrundlage im Telekommunikationsgesetz (TKG) er-

---

onsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (vgl. Fn. 5); Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder in Deutschland, Public consultation on traffic data retention, in: DuD 2004, 604 f.; Alvaro, RDV 2005, 49 f.; Breyer, S. 369 ff.

16 Streinz, Rdnr. 255.

17 Es bleibt abzuwarten, ob die Grundrechte-Charta tatsächlich bis 2009 von den einzelnen Mitgliedstaaten ratifiziert wird.

18 Gola/Klug, S. 30.

halten, während die staatlichen Zugriffsrechte wie bisher u. a. in der Strafprozessordnung (StPO) geregelt werden sollen.

Auf Grundlage der nachfolgenden verfassungsrechtlichen Würdigung der Vorratsdatenspeicherung werden dem Gesetzgeber Vorschläge für eine verfassungsschonende Richtlinienumsetzung unterbreitet.

2. Das Recht auf informationelle Selbstbestimmung und das BDSG als datenschutzrechtliches „Grundgesetz"

Grundlage des Anspruchs auf Gewährleistung des Datenschutzes bildet das dem Bürger vom Bundesverfassungsgericht[19] zuerkannte „Recht auf informationelle Selbstbestimmung". Danach setzt die verfassungsrechtlich gewährleistete freie Entfaltung der Persönlichkeit (Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 GG) angesichts der Gegebenheiten der modernen Datenverarbeitung den Schutz des Einzelnen gegen die unbegrenzte Erhebung, Verarbeitung und Nutzung seiner persönlichen Daten voraus[20]. Der Einzelne soll zunächst grundsätzlich selbst bestimmen, wer welche ihn betreffenden Daten zu welchen Zwecken verarbeitet. Das allgemeine Persönlichkeitsrecht aus Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 GG allerdings ergänzt

> *„die speziellen Freiheitsrechte, die ebenfalls konstituierende Elemente der Persönlichkeit schützen, nur insoweit, als Letztere keinen Schutz gewähren"*[21].

Soll in diese Freiheitsrechte seitens des Staates eingegriffen werden, sollen also Daten ohne oder sogar gegen den Willen des Betroffenen erhoben und verarbeitet werden, so bedarf es einer im

---

19 Urteil vom 15.12.1983 - 1 BvR 209, 269, 362, 420, 440, 484/83, NJW 1984, 419, 422.

20 Jarass/Pieroth, Artikel 2 Rdnr. 39.

21 Urteil des Bundesverfassungsgerichts vom 03.03.2004 - 1 BvR 2378/98 und 1084/99, NJW 2004, 999, 1005 („Großer Lauschangriff").

überwiegenden Allgemeininteresse und unter Beachtung des Verhältnismäßigkeitsprinzips ergangenen normenklaren Regelung[22]. Das Bundesverfassungsgericht[23] hat sich ausdrücklich gegen die Speicherung von Daten „auf Vorrat" ausgesprochen.

Der Verpflichtung zur Gewährleistung des informationellen Selbstbestimmungsrechts einerseits und den Bedürfnissen des Staates und der Privatwirtschaft, Daten Einzelner auch ohne bzw. gegen deren Willen verarbeiten zu können, andererseits, sind die Gesetzgeber auf Bundes- und Länderebene durch den Erlass allgemeiner und spezieller Datenschutzgesetze nachgekommen[24]. Gegenstand der Datenschutzgesetze sind Regelungen zum Umgang mit personenbezogenen Daten (§ 1 Abs. 1 Bundesdatenschutzgesetz - BDSG), d.h. „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)" (§ 3 Abs. 1 BDSG). Zu diesen Angaben zählt auch die Tatsache, ob und unter welchen näheren Umständen jemand mit einem anderen per Telekommunikation Kontakt hatte[25].

Für Datenverarbeitungen der Privatwirtschaft und damit auch für die künftigen Adressaten der Pflicht zur Vorratsdatenspeicherung bildet das BDSG die allgemeine Datenschutznorm. Der Datenschutz wird aber nicht nur oder zumindest nicht primär durch das BDSG, sondern vielfach durch bereichsspezifische, d.h. ganz bestimmte Bereiche der Verarbeitung personenbezogener Daten konkret betreffende Bestimmungen geregelt. Die Notwendigkeit derartiger Regelungen ergibt sich dann, wenn die allgemeinen Datenschutzgesetze mit ihren unbestimmten Rechtsbegriffen dem Schutzbedarf nicht Rechnung tragen können.

Demgemäß sind sowohl die allgemeinen Vorschriften des Grund-

---

22 Vgl. bei Gola/Schomerus, § 1 Rdnr. 17 und § 4 Rdnr. 7 f.

23 Urteil vom 15.12.1983 - 1 BvR 209, 269, 362, 420, 440, 484/83, NJW 1984, 419, 422.

24 Zum Charakter der Datenschutzgesetze als Schutz- und Eingriffsgesetze vgl. Gola/Schomerus, § 1 Rdnr. 4 ff., 16 ff.

25 Vgl. bereits zur betrieblichen Telefondatenerfassung: Beschluss des Bundesarbeitsgerichts vom 27.05.1986 - 1 ABR 48/84, RDV 1986, 199 = DB 1986, 2086.

gesetzes (Artikel 2 Abs. 1 und Artikel 1 Abs. 1 GG) als auch ihre allgemeine Umsetzung im BDSG (§§ 1 Abs. 4, 4 Abs. 1 BDSG) gegenüber so genannten speziellen Schutz- und Eingriffsnormen subsidiär.

Soweit die Speicherung von Telekommunikationsdaten und der staatliche Zugriff hierauf betroffen ist, findet sich im Grundgesetz eine spezielle Gewährleistung in Form des Fernmeldegeheimnisses (Artikel 10 Abs. 1 Var. 3 GG) und auf einfachgesetzlicher Ebene die Festlegung von konkreten Eingriffsbefugnissen des Staates u. a. im TKG und in der StPO.

3. Verfassungsrechtliche Würdigung der Vorratsdatenspeicherung

3.1. Artikel 10 Abs. 1 Var. 3 GG (Fernmeldegeheimnis)

3.1.1. Das Fernmeldegeheimnis als spezielle Ausgestaltung des Rechts auf informationelle Selbstbestimmung

Es wurde bereits dargelegt[26], dass das Fernmeldegeheimnis eine besondere Ausprägung des Rechts auf informationelle Selbstbestimmung (Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 GG) darstellt[27]. Wie auch Artikel 13 GG (Unverletzlichkeit der Wohnung) sichert nämlich Artikel 10 GG in einem Teilbereich Gehalte des Persönlichkeitsrechts und ist somit eine spezielle Gewährleistung[28].

---

[26] Vgl. die Ausführungen auf S. 21 f.

[27] Beschluss des Bundesverfassungsgerichts vom 04.04.2006 - 1 BvR 518/02, NJW 2006, 1939, 1942. Vgl. dazu auch Roßnagel/Groß, S. 1261.

[28] Jarass/Pieroth, Artikel 2 Rdnr. 40; Urteil des Bundesverfassungsgerichts vom 14.07.1999 - 1 BvR 2226/94, 2420/95 und 2437/95, NJW 2000, 55, 56;

Aus dem Umstand, dass das Fernmeldegeheimnis eine besondere Ausprägung des Rechts auf informationelle Selbstbestimmung ist, ergibt sich, dass sich im Hinblick auf den zu Grunde zu legenden Prüfungsmaßstab keine wesentlichen Unterschiede ergeben können. So hat auch das Bundesverfassungsgericht[29] erst im März 2006 im Rahmen einer Entscheidung zur Sicherung von im Herrschaftsbereich des Teilnehmers gespeicherten Telekommunikationsverbindungsdaten festgestellt:

> *„Soweit der Eingriff in das Fernmeldegeheimnis die Erlangung personenbezogener Daten betrifft, sind dabei die Maßgaben, die das Bundesverfassungsgericht im Volkszählungsurteil aus Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 GG entwickelt hat, grundsätzlich auch auf die speziellere Garantie in Artikel 10 Abs. 1 GG zu übertragen."*

3.1.2. Schutzbereich

3.1.2.1. Allgemeines

Die spezielle Kodifikation des Rechts auf informationelle Selbstbestimmung in Artikel 10 Abs. 1 Var. 3 GG hat den Schutz personenbezogener Daten im Zusammenhang mit einem räumlich distanzierten Kommunikationsvorgang (Fernkommunikation) zum Gegenstand. Das Fernmeldegeheimnis bezieht sich dabei zum einen auf den Inhalt der Kommunikation[30]. Erfasst werden zum anderen auch Informationen über den Ort und die Zeit sowie die Art und Weise der Kommunikation[31] (nähere Umstände der Kommunikation). Geschützt werden insbesondere Daten über die an der Kommunikation beteiligten Personen[32], über die Dauer und

Urteil des Bundesverfassungsgerichts vom 12.03.2003 - 1 BvR 330/96 und 348/99, NJW 2003, 1787, 1788.

29 Urteil vom 02.03.2006 - 2 BvR 2099/04, NJW 2006, 976, 979 f.

30 Jarass/Pieroth, Artikel 10 Rdnr. 9; MKS/Gusy, Artikel 10 Rdnr. 58.

31 Jarass/Pieroth, Artikel 10 Rdnr. 9.

32 Urteil des Bundesverfassungsgerichts vom 12.03.2003 - 1 BvR 330/96 und 348/99, NJW 2003, 1787, 1788.

Häufigkeit der Kommunikation, über den Ort, von dem aus kommuniziert wird, und über die Kennung des Endgeräts[33]. Nicht erforderlich ist, dass Telekommunikationsverkehr tatsächlich stattgefunden hat; vielmehr genügt es für das Eingreifen des Grundrechts, dass ein solcher versucht worden ist[34].

Mit der grundrechtlichen Verbürgung der Unverletzlichkeit des Fernmeldegeheimnisses soll insbesondere vermieden werden, dass der Meinungs- und Informationsaustausch mittels Telekommunikationsanlagen deswegen unterbleibt oder nach Form und Inhalt anders verläuft, weil die Beteiligten damit rechnen müssen, dass staatliche Stellen sich in die Kommunikation einschalten und Kenntnisse über die Kommunikationsbeziehungen oder Kommunikationsinhalte gewinnen[35].

3.1.2.2. Von § 113a TKG-E erfasste Datenkategorien

Die von § 113a TKG-E erfassten Datenkategorien unterfallen grundsätzlich dem Schutzbereich des Fernmeldegeheimnisses. Denn sie beziehen sich auf die Identifikation der am Kommunikationsvorgang beteiligten Personen bzw. Endeinrichtungen (§ 113a Abs. 2 Nr. 1, Nr. 4 a), b), d) und Nr. 5, Abs. 3 Nr. 1 bis 3, Abs. 4 Nr. 1 und Nr. 2 TKG-E), die Ermittlung von Zeit und Ort der Kommunikation (§ 113a Abs. 2 Nr. 2, Abs. 3 Nr. 4, Abs. 4 Nr. 3 TKG-E; § 113a Abs. 2 Nr. 4 c, Abs. 7 TKG-E) bzw. die Bestimmung der Art und Weise der Kommunikation (§ 113a Abs. 2 Nr. 3 TKG-E) und damit auf Umstände, bezüglich derer bereits festgestellt wurde, dass sie prinzipiell dem Schutzbereich des Fernmeldegeheimnisses unterfallen.

Auch sind die nach § 113a Abs. 5 TKG-E zu speichernden Informationen über erfolglose Anrufversuche durch das Fernmeldegeheimnis geschützt.

---

33 Jarass/Pieroth, Artikel 10 Rdnr. 9.

34 Beschluss des Bundesverfassungsgerichts vom 25.03.1992 - 1 BvR 1430/88, NJW 1992, 1875; Beschluss des Bundesverfassungsgerichts vom 20.06.1984 - 1 BvR 1494/78, NJW 1985, 121, 122.

35 Beschluss des Bundesverfassungsgerichts vom 30.04.2007 - 2 BvR 2151/06.

3.1.2.3. Von § 113a TKG-E erfasste Kommunikationsformen

Fraglich ist jedoch, ob auch alle von § 113a TKG-E umfassten Kommunikationsformen dem Schutzbereich des Fernmeldegeheimnisses unterfallen. Die in § 113a TKG-E enthaltenen Speicherungspflichten betreffen Anbieter von Telefondiensten einschließlich der Mobilfunk- und Internet-Telefonie (Abs. 2) sowie Angebote im Bereich der elektronischen Post (Abs. 3) und Internetzugangsdienste (Abs. 4).

Unproblematisch ist die Geltung des Fernmeldegeheimnisses im Hinblick auf die klassische Festnetztelefonie und den Mobilfunk[36]. Auch dass die E-Mail-Kommunikation dem Fernmeldegeheimnis unterfällt, ist mittlerweile anerkannt[37]. Für die Einordnung der Internet-Telefonie (Voice over IP) muss das Gleiche gelten wie im Hinblick auf die E-Mail-Kommunikation, denn Internet-Telefonie und E-Mail-Kommunikation sind insofern identisch, als in beiden Fällen eine individuelle Kommunikation über das Medium Internet bezweckt wird.

Ob auch der reine Internetzugang vom Fernmeldegeheimnis erfasst wird, ist indessen umstritten. Hintergrund des Streits ist, dass das Fernmeldegeheimnis grundsätzlich nur solche Informationen erfassen soll, die an einen bestimmten Adressatenkreis gerichtet sind; beim „Surfen“ im Internet werde aber auf öffentlich zugängliche Informationen zugegriffen[38]. Insoweit ist festzustellen, dass es zwar richtig ist, dass sich im Internet meist frei für jedermann verfügbare Informationen befinden; über das Internet können aber auch viele nicht öffentliche Informationen angesprochen werden[39]. So können etwa in einem geschützten Bereich Informationen für eine andere Person abgelegt werden. Ein weiteres Argument für die Einordnung des „Surfens“ unter den Schutzbereich des Artikels 10 GG ergibt sich aus der technischen

---

36 Vgl. etwa Jarass/Pieroth, Artikel 10 Rdnr. 5; Ipsen, Rdnr. 287.

37 Jarass/Pieroth, Artikel 10 Rdnr. 5; Ipsen, Rdnr. 287; MüKu/Löwer, Artikel 10 Rdnr. 18; Breyer, S. 78.

38 Hierzu und zum Streitstand im Einzelnen: Breyer, S. 78 ff.

39 Sievers, S. 130.

Funktionsweise des Internet: Auch der Abruf von Informationen von einem für jedermann frei zugänglichen Web- oder FTP-Server veranlasst den Aufbau einer individuellen Verbindung; ohne Kenntnisnahme vom Inhalt der konkreten Verbindung ist nicht zu ermitteln, welche Inhalte ausgetauscht worden sind[40]. Eine Trennung von Individual- und Massenkommunikation wäre lediglich über die Kenntnisnahme der übermittelten Informationen zu erreichen. Da hiermit aber unvermeidbar auch die Kenntnisnahme von - unbestritten geschützter - Individualkommunikation verbunden wäre, liefe eine derartige Trennung dem Schutzzweck des Artikel 10 Abs. 1 Var. 3 GG zuwider[41]. Die Internetkommunikation muss demzufolge insgesamt dem Schutzbereich des Fernmeldegeheimnisses unterstellt werden[42].

Damit unterfallen alle vorliegend betroffenen Kommunikationsformen und Datenkategorien dem (sachlichen) Schutzbereich des Fernmeldegeheimnisses. Vom persönlichen Schutzbereich des Grundrechts sind auch Pressevertreter erfasst.

3.1.3. Eingriff

Fraglich ist, ob alleine der Umstand der Datenspeicherung einen Eingriff in das Fernmeldegeheimnis begründen kann oder ob ein solcher nicht vielmehr erst dann vorliegt, wenn auf die Daten auch tatsächlich von staatlicher Seite zugegriffen wird.

---

40 Sievers, S. 130. Ähnlich wie dieser auch Breyer, S. 79 f. und Pieroth/Schlink, Rdnr. 773.

41 Germann, S. 118.

42 Wie hier Sievers, S. 130; Breyer, S. 78 ff.; Pieroth/Schlink, Rdnr. 773; Germann, S. 118. Wollte man dieser Ansicht nicht folgen, griffe im Hinblick auf das „Surfen“ im Internet jedenfalls das (allgemeine) Recht auf informationelle Selbstbestimmung aus Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 GG und damit der gleiche Prüfungsmaßstab (vgl. S. 23). Eine entsprechende Klarstellung fordert der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Zehn Thesen für eine datenschutzfreundliche Informationstechnik: „Im Zeitalter des Internet, in dem neben die Individualkommunikation vielfältige andere Formen der elektronischen Kommunikation treten, muss das Fernmeldegeheimnis zu einem umfassenden Mediennutzungsgeheimnis ausgebaut werden“.

Nach den Feststellungen des Bundesverfassungsgerichts[43] in der Entscheidung Verbrechensbekämpfungsgesetz/G 10 liegt ein Eingriff in das Fernmeldegeheimnis nicht erst in der Kenntnisnahme von erfassten Fernmeldevorgängen durch die Mitarbeiter staatlicher Stellen[44]. Vielmehr, so das Bundesverfassungsgericht, müssten auch die vorangehenden Arbeitsschritte in ihrem durch den Überwachungs- und Verwendungszweck bestimmten Zusammenhang betrachtet werden. Ein Eingriff sei schon die Erfassung der Daten selbst, es sei denn, die Fernmeldevorgänge würden zunächst ungezielt und rein technisch bedingt miterfasst, aber unmittelbar nach der Signalaufbereitung wieder spurlos ausgesondert. Mit der Speicherung der erfassten Daten, durch die das Material aufbewahrt und für den Abgleich bereitgehalten werde, setze sich der Eingriff fort.

Der Annahme eines Eingriffs durch die Datenerfassung bzw. Datenspeicherung steht auch nicht entgegen, dass diese Vorgänge vorliegend anders als in der angesprochenen Entscheidung nicht durch staatliche Stellen selbst erfolgen. Zwar erfolgt die Grundrechtsbeeinträchtigung nur vermittelt durch das privatrechtlich organisierte Telekommunikationsunternehmen. Handelt das Telekommunikationsunternehmen allerdings auf Grund einer verbindlichen hoheitlichen Anordnung, wie sie § 113a TKG-E darstellen würde, muss das Verhalten des privaten Telekommunikationsunternehmens der öffentlichen Gewalt zugerechnet werden[45].

Um effektiven Grundrechtsschutz zu gewährleisten, muss sich dieser im Übrigen auch nach Ende der Kommunikation dort fortsetzen, wo kommunikationsbezogene Informationen in irgendeiner Form gespeichert oder auf sonstige Weise verarbeitet werden[46]. Danach unterliegen beispielsweise Daten, die in einem

---

43 Vgl. zum gesamten Absatz: Urteil des Bundesverfassungsgerichts vom 14.07.1999 - 1 BvR 2226/94, 2420/95 und 2437/95, NJW 2000, 55, 59.

44 Zur Eingriffsqualität der staatlichen Kenntnisnahme vgl. Jarass/Pieroth, Artikel 10 Rdnr. 11.

45 Zur Zurechnung der gerichtlich angeordneten Auskunftserteilung gegenüber der öffentlichen Gewalt vgl. Urteil des Bundesverfassungsgerichts vom 12.03.2003 - 1 BvR 330/96 und 348/99, NJW 2003, 1787, 1793.

46 Vgl. etwa die Anmerkung von Bär, MMR 2005, 523 f.

elektronischen Postfach oder einer Mailbox des jeweiligen TK-Betreibers gespeichert sind, weiterhin dem Schutzbereich von Artikel 10 GG.

Bereits in der Datenerhebung liegt damit ein staatlicher Eingriff[47], der sich zunächst durch die Datenspeicherung und schließlich durch den Datenzugriff weiter intensiviert.

3.1.4. Verfassungsrechtliche Rechtfertigung

3.1.4.1. Gesetzesvorbehalt des Artikel 10 Abs. 2 S. 1 GG

Nach Artikel 10 Abs. 2 S. 1 GG steht das Fernmeldegeheimnis allerdings unter Gesetzesvorbehalt. Der in der staatlich angeordneten Datenerhebung bzw. -speicherung liegende Eingriff könnte mithin gerechtfertigt sein.

Die Einschränkung des Fernmeldegeheimnisses kann auf Grund einer formell-gesetzlichen Ermächtigung, durch Rechtsverordnung, Satzung oder Verwaltungsakt erfolgen oder auch - über den Wortlaut des Artikel 10 Abs. 2 GG hinaus[48] - unmittelbar durch ein förmliches Gesetz[49].

Erforderlich ist, dass die Rechtsgrundlage für den Eingriff ausreichend bestimmt und die Grundrechtseinschränkung verhältnismäßig ist[50]. Die Verhältnismäßigkeit der Maßnahme setzt dabei zunächst voraus, dass mit der Maßnahme ein legitimer Zweck verfolgt wird und die vorgesehene Maßnahme zur Erreichung bzw. Förderung dieses Zwecks geeignet und erforderlich ist[51]. Weiterhin müssen die Beschränkung des Grundrechts und die mit ihr verbundenen Nachteile auf Seiten des Grundrechtsträgers in einem angemessenen Verhältnis zum verfolgten Zweck stehen (Verhältnismäßigkeit im engeren Sinne)[52].

---

47 Vgl. auch Leutheusser-Schnarrenberger, ZRP 2007, 10.
48 „Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden."
49 Jarass/Pieroth, Artikel 10 Rdnr. 16; MüKu/Löwer, Artikel 10 Rdnr. 28.
50 Jarass/Pieroth, Artikel 10 Rdnr. 16 ff.
51 Pieroth/Schlink, Rdnr. 279.
52 Pieroth/Schlink, Rdnr. 289.

3.1.4.2. Bestimmtheit der Ermächtigungsgrundlage

Die Ermächtigung für einen Eingriff in das Fernmeldegeheimnis muss ausreichend bestimmt sein[53]. Notwendig ist ein Gesetz, das den Freiheitseingriff *„ausdrücklich offen legt“*[54]. Voraussetzungen und Umfang der Beschränkungen müssen sich für den Einzelnen erkennbar aus dem Gesetz ergeben[55]; der Verwendungszweck muss *„bereichsspezifisch und präzise bestimmt werden“*[56], so dass der Betroffene die Rechtslage erkennen und sein Verhalten darauf ausrichten kann[57]. Auf einfachgesetzlicher Ebene ist zudem § 88 Abs. 3 S. 3 TKG zu beachten. Danach ist eine Verwendung von Kenntnissen über Tatsachen, die dem Fernmeldegeheimnis unterliegen, für andere Zwecke als die sichere Erbringung des Telekommunikationsdienstes, insbesondere die Weitergabe an andere, nur zulässig, soweit das TKG selbst oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht.

Bedenken im Hinblick auf § 88 Abs. 3 S. 3 TKG ergeben sich vorliegend nicht. An einer ausreichenden Bestimmtheit der geplanten Regelungen fehlt es jedoch[58]. Nach dem Volkszählungsurteil des Bundesverfassungsgerichts[59] setzt ein Zwang zur Angabe personenbezogener Daten voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich

---

53 Jarass/Pieroth, Artikel 10 Rdnr. 17.

54 Beschluss des Bundesverfassungsgerichts vom 25.03.1992 - 1 BvR 1430/88, NJW 1992, 1875, 1877.

55 Jarass/Pieroth, Artikel 10 Rdnr. 17; AK/Bizer, Artikel 10 Rdnr. 79.

56 Urteil des Bundesverfassungsgerichts vom 14.07.1999 - 1 BvR 2226/94, 2420/95 und 2437/95, NJW 2000, 55, 65.

57 Urteil des Bundesverfassungsgerichts vom 27.07.2005 - 1 BvR 668/04, NJW 2005, 2603, 2607.

58 Vgl. etwa Gemeinsame Stellungnahme von ARD u.a. (Fn. 6), S. 30; Stellungnahme des Verbandes der Anbieter von Telekommunikations- und Mehrwertdiensten (VATM) e.V. vom 19.01.2007, S. 1f., 12 (die Stellungnahme ist abrufbar unter http://www.vatm.de/content/stellungnahmen/inhalt/19-01-2007.pdf).

59 Urteil des Bundesverfassungsgerichts vom 15.12.1983 - 1 BvR 209, 269, 362, 420, 440, 484/83, NJW 1984, 419.

sind. Die in § 113b Nr. 1 TKG-E enthaltene pauschale Formulierung „zur Verfolgung von Straftaten“ wird diesem Erfordernis einer bereichsspezifischen und präzise bestimmten Zweckangabe nicht gerecht[60]. Gerade im Hinblick auf die immer vielfältigeren staatlichen Eingriffsbefugnisse bedarf es einer klaren gesetzlichen Zweckbestimmung. Insoweit ist eine exakte Bestimmung derjenigen Straftatbestände erforderlich, die zu einem Datenzugriff berechtigen würden[61]. Im Hinblick auf die notwendige Bestimmtheit von gesetzlichen Eingriffsbefugnissen sei auch auf die jüngste verfassungsgerichtliche Rechtsprechung zur präventiven polizeilichen Rasterfahndung[62], zum Niedersächsischen Polizeigesetz[63] sowie zur spezialgesetzlichen Regelung von Videoüberwachungsmaßnahmen[64] hingewiesen. Bestimmtheitsbedenken unterliegen im Übrigen auch die Vorschriften über die Zugriffsberechtigung[65].

Soweit der in § 113b Nr. 2 TKG-E genannte Verwendungszweck der „Abwehr von erheblichen Gefahren für die öffentliche Sicherheit“ betroffen ist, wird es zwar nicht an der erforderlichen Bestimmtheit fehlen, denn sowohl der Begriff der öffentlichen Sicherheit als auch derjenige der erheblichen Gefahr haben durch die Rechtsprechung eine entsprechende Konturierung erhalten. Im Rahmen der Prüfung der Verhältnismäßigkeit wird allerdings die Frage zu beantworten sein, ob eine entsprechend weitreichende Eingriffsbefugnis vor dem Hintergrund der betroffenen Grundrechtspositionen gerechtfertigt sein kann.

---

60 Gemeinsame Stellungnahme von ARD u.a. (Fn. 6), S. 30; ähnlich: Stellungnahme des VATM (Fn. 58), S. 1f., 12. Vgl. auch S. 10 der Stellungnahme, die der Arbeitskreis Vorratsdatenspeicherung, das Netzwerk Neue Medien e.V. und die Neue Richtervereinigung e.V. gemeinsam zum Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung abgegeben haben (Fn. 5): „Eine allgemeine Aufgabenbeschreibung (z.B. „zu Strafverfolgungszwecken“, „zu Zwecken der Gefahrenabwehr“) stellt keine hinreichende Zweckbestimmung in diesem Sinne dar.“ Siehe ferner BITKOM-Stellungnahme vom 22.05.2007 (Fn. 5), S. 14.

61 Simitis, RDV 2007, 146.

62 Beschluss vom 04.04.2006 - 1 BvR 518/02, NJW 2006, 1939.

63 Urteil vom 27.07.2005 - 1 BvR 668/04, NJW 2005, 2603.

64 Beschluss vom 23.02.2007 - 1 BvR 2368/06, RDV 2007, 115.

65 Siehe hierzu S. 58 ff.

3.1.4.3. Legitimer Zweck

Mit den geplanten Regelungen zur Vorratsdatenspeicherung soll zum einen sichergestellt werden, dass die von der Vorratsdatenspeicherung betroffenen Telekommunikationsdaten zum Zwecke der Verfolgung von Straftaten zur Verfügung stehen (§ 113b Nr. 1 TKG-E). Daran, dass die Verfolgung von Straftaten als legitimer öffentlicher Zweck anzusehen ist, besteht kein Zweifel[66]. Allerdings wird die Auffassung vertreten, dass die Effektivität der Verbrechensbekämpfung allein keinen legitimen Zweck zur Rechtfertigung von Eingriffen darstellen könne, da dies zwingend in die Maßlosigkeit führe[67].

Anders als noch der Referentenentwurf lässt es der jetzige Regierungsentwurf zudem zu, dass die Vorratsdaten „zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit“ (§ 113b Nr. 2 TKG-E) bzw. zur Erfüllung der Aufgaben der Nachrichtendienste (§ 113b Nr. 3 TKG-E) übermittelt werden. Auch dies ist als legitimer Zweck anzusehen[68].

3.1.4.4. Geeignetheit der Maßnahme

Ob die Einführung einer Vorratsdatenspeicherung geeignet ist, um Straftaten effektiver bekämpfen und verfolgen zu können, wird vielfach angezweifelt[69].

Insoweit wird vor allem auf die zahlreichen Möglichkeiten hin-

---

66 Urteil des Bundesverfassungsgerichts vom 27.07.2005 - 1 BvR 668/04, NJW 2005, 2603, 2610.

67 So Simitis, RDV 2007, 145.

68 Zum legitimen Interesse an der Verhütung von Straftaten von erheblicher Bedeutung vgl. Urteil des Bundesverfassungsgerichts vom 27.07.2005 - 1 BvR 668/04, NJW 2005, 2603, 2610.

69 Vgl. etwa Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (KOM(2005) 438 endg.), Amtsblatt der Europäischen Union, C 298/1, Erwägungen Nr. 25 und 77.

gewiesen, die potenzielle Straftäter haben, um einer Entdeckung mittels der Vorratsdatenspeicherung zu entgehen. So können sie etwa anonyme Kommunikationsmittel (wie z.B. Telefonzellen) nutzen oder ihre Spuren durch Nutzung von Anonymisierungsdiensten, wechselnd eingesetzte Mobiltelefone von unterschiedlichen ausländischen Mobilfunkanbietern oder Fälschung der elektronischen Adresse verwischen[70]. Es kann auch auf Provider außerhalb der EU zurückgegriffen werden, die von der Verpflichtung zur Vorratsdatenspeicherung nicht erfasst werden[71]. Die Gefahr von Umgehungen dürfte dabei umso größer sein, je besser die Tat geplant ist. Mittels der Vorratsdatenspeicherung sollen jedoch insbesondere Straftaten im Bereich des Terrorismus und der organisierten Kriminalität bekämpft werden[72] und damit Taten, die durch einen besonders hohen Grad an Organisation gekennzeichnet sind.

Im Hinblick auf über das Internet begangene Straftaten ist zudem zu berücksichtigen, dass insbesondere größere Unternehmen bzw. Institutionen zunehmend eine einzige statische IP-Adresse verwenden. Zwar könnte beim Provider die zu der IP-Adresse gehörige Institution in Erfahrung gebracht werden. Letztlich kann die konkret verantwortliche Person aber nur über die Log-Dateien der die IP-Adresse verwendenden Stelle ermittelt werden. Diese Daten werden dort auf Grund entsprechender Löschroutinen aber vielfach nicht mehr vorhanden sein. Mithin ist die Vorratsdatenspeicherung in derartigen Fällen nicht geeignet, Straftaten zu verhüten oder aufzudecken.

Für den Bereich der Internetdaten ist weiterhin fraglich, ob bei dem Ausmaß an zu speicherndem Datenvolumen eine zielführen-

---

70 Vgl. etwa Vassilaki, MMR 2/2006, XIII; Büllingen, DuD 2005, 350; Ulmer/Schrief, DuD 2004, 595; BDI, DuD 2004, 607.

71 Vassilaki, MMR 2/2006, XIII; Ulmer/Schrief, DuD 2004, 595; BDI, DuD 2004, 607.

72 Vgl. Erwägungsgründe 7 bis 10 der Richtlinie.

de Auswertung überhaupt möglich ist[73]. Laut dem Ausschuss des Europäischen Parlaments für bürgerliche Freiheiten, Justiz und Inneres fällt im Netz eines großen Internet-Providers bereits bei heutigem Verkehrsaufkommen eine Datenmenge von 20.000 - 40.000 Terabyte an[74]. Diese Datenmenge soll 4 Mio. km gefüllter Aktenordner entsprechen[75].

Ergänzend sei auf die folgende Feststellung von Weichert[76] verwiesen:

> *„Eine nüchterne Analyse muss zu dem Ergebnis kommen, dass mit den gewaltigen Massen an Datenschrott, der bei einer anlasslosen Überwachung anfällt, kein wesentlicher Sicherheitsgewinn erzielt werden kann."*

Im Hinblick auf Datenzugriffe zu Zwecken der Gefahrenabwehr (§ 113b Nr. 2 TKG-E) ist schließlich zu berücksichtigen, dass die Vorratsdatenspeicherung im Bereich der Gefahrenabwehr ohnehin nur eine untergeordnete Rolle spielen kann, da sie sich nur auf Telekommunikationsvorgänge bezieht, die in der Vergangenheit stattgefunden haben[77]. Insoweit stellt sich die Frage nach der Geeignetheit also in besonderer Weise.

Trotz der dargestellten Zweifel an der Effektivität der Regelungen zur Vorratsdatenspeicherung wird die Geeignetheit der Maßnahme allerdings letztlich zu bejahen sein. Insofern ist zu beachten, dass das Gebot der Geeignetheit lediglich verlangt, dass der Staat

---

73 Bericht des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments (A6-0174/ 2005), S. 8; BT-Dr 16/128 „Antrag gegen eine europaweit verpflichtende Vorratsdatenspeicherung", S. 2; Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (8.-9. März 2007) zur Vorratsdatenspeicherung (vgl. Fn. 5); BDI, DuD 2004, 607.

74 Bericht des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments (A6-0174/ 2005), S. 8.

75 Bericht des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments (A6-0174/ 2005), S. 8.

76 Weichert, Sonderbeilage zu RDV 1/2005, 10 f.

77 Leutheusser-Schnarrenberger, ZRP 2007, 9, 11; Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (vgl. Fn. 5), S. 23 f.

nur solche Mittel zum Einsatz bringt, mit deren *„Hilfe der gewünschte Erfolg gefördert werden kann“*[78], bzw. Mittel, die die *„Möglichkeit der Zweckerreichung“*[79] implizieren. Das benutzte Mittel muss nicht das bestmöglichste oder geeigneteste sein[80] und nicht in jedem Einzelfall Wirkung entfalten[81]; es genügt ein Beitrag zur Zielerreichung[82]. Dass auf Basis einer Vorratsdatenspeicherung zusätzliche Taten verhindert bzw. verfolgt werden können, erscheint jedoch nicht per se ausgeschlossen.

Auf die zahlreichen Möglichkeiten zur Umgehung einer Vorratsdatenspeicherung wird aber später noch zurückzukommen sein: Ist der Ertrag eines Mittels gering, die Belastung für den Betroffenen hingegen hoch, kann es an der Angemessenheit der Maßnahme fehlen[83].

3.1.4.5. Erforderlichkeit der Maßnahme

Eine staatliche Maßnahme ist lediglich dann erforderlich, wenn der verfolgte Zweck nicht durch ein gleich wirksames, aber weniger belastendes Mittel erreicht werden kann[84].

Zweifelhaft ist schon, ob die in § 113a TKG-E vorgesehene Speicherfrist von sechs Monaten zur Zweckerreichung erforderlich sind. Aus den Analysen schwedischer und britischer Stellen ergibt sich, dass sich die Datenabfragen der Behörden zu 80-85% auf den Zeitraum der letzten drei Monate beziehen, so dass die Erfor-

---

78 Beschluss des Bundesverfassungsgerichts vom 03.04.2001 - 1 BvL 32/97, NZA 2001, 777, 779; Beschluss des Bundesverfassungsgerichts vom 10.04.1997 - 2 BvL 45/92, NVwZ 1997, 1109, 1111; Beschluss des Bundesverfassungsgerichts vom 20.06.1984 - 1 BvR 1494/78, NJW 1985, 121, 122.

79 Beschluss des Bundesverfassungsgerichts vom 10.04.1997 - 2 BvL 45/92, NVwZ 1997, 1109, 1111; Beschluss des Bundesverfassungsgerichts vom 20.06.1984 - 1 BvR 1494/78, NJW 1985, 121, 123.

80 Sachs/Sachs, Artikel 20 Rdnr. 150; ähnlich: Stern, S. 776 f.

81 Beschluss des Bundesverfassungsgerichts vom 20.06.1984 - 1 BvR 1494/78, NJW 1985, 121, 123.

82 MD/Herzog, VII, Rdnr. 74.

83 Jarass/Pieroth, Artikel 20 Rdnr. 84.

84 Pieroth/Schlink, Rdnr. 285.

derlichkeit einer längeren Frist fraglich ist[85].

Gegen die Erforderlichkeit der Regelungen zur Vorratsdatenspeicherung wird weiter eingewandt, dass mit dem sog. „Quick Freeze[86]“-Verfahren ein wesentlich milderes und grundrechtsschonenderes Mittel existiere[87]. „Quick Freeze“ ist ein Konzept, mit dem Telekommunikationsverkehrsdaten vorübergehend gesichert werden können[88]. Vorgebeugt werden soll der Gefahr, dass von den Ermittlungsbehörden benötigte Daten möglicherweise bereits durch den Provider gelöscht sind, bevor der für den Zugriff erforderliche richterliche Beschluss vorliegt. Im Rahmen des „Quick Freeze“ ordnen die Ermittlungsbehörden in einem ersten Schritt an, dass bei Vorliegen eines konkreten Tatverdachts die routinemäßige Datenlöschung durch den Anbieter blockiert und die vorhandenen Daten damit "eingefroren" werden (so genannte Speicheranordnung bzw. anlassbezogene Speicherung). In einem zweiten Schritt können die Daten dann durch eine nachfolgende richterliche Anordnung "aufgetaut" und den Ermittlungsbehörden zur Verfügung gestellt werden. Das „Quick Freeze“-Verfahren wird auch in der Cybercrime-Konvention des Europarats vorgeschlagen[89].

Letztlich lässt allein die Möglichkeit der Einführung eines derartigen Verfahrens jedoch nicht die Erforderlichkeit der Vorratsdatenspeicherung entfallen. Die Erforderlichkeit einer Maßnahme entfällt nämlich nur dann, wenn das alternativ einsetzbare Mittel genauso wirksam ist wie das ursprünglich geplante. „Quick Freeze“ kann jedoch nur verhindern, dass vom Anbieter zunächst gespeicherte Daten aus Behördensicht verfrüht gelöscht werden. Soweit der Anbieter bestimmte Daten von Anfang nicht erhebt bzw. speichert, hilft den Behörden auch ein „Quick Freeze“ nicht

---

85 Büllingen, DuD 2005, 350.

86 Deutsch: Schockfrosten.

87 Vgl. etwa Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder in Deutschland, DuD 2004, 605; Büllingen, DuD 2005, 350.

88 Vgl. zum gesamten Absatz Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 27. Tätigkeitsbericht (2005), 4.2.3 Bekämpfung der Internetkriminalität - „quick freeze“, S. 29 f.

89 Artikel 16 der Cybercrime-Konvention.

weiter[90].

Die Möglichkeit des „Quick Freeze“ führt damit nicht zu einem Wegfall der Erforderlichkeit der Vorratsdatenspeicherung. Auch sie muss aber im Rahmen der nachfolgenden Prüfung der Verhältnismäßigkeit im engeren Sinne Berücksichtigung finden.

3.1.4.6. Verhältnismäßigkeit im engeren Sinne (Angemessenheit)

Das Vorliegen der Verhältnismäßigkeit im engeren Sinne setzt voraus, dass der Eingriff bzw. die Beeinträchtigung, die der Eingriff für den Einzelnen bedeutet, und der mit dem Eingriff verfolgte Zweck in recht gewichtetem und wohl abgewogenen Verhältnis zueinander stehen[91].

Insofern ist zunächst festzustellen, dass die Nutzer von moderner Informations- und Kommunikationstechnik[92] durch eine Vorratsdatenspeicherung in erheblichem Maße beeinträchtigt werden.

Die Belastung ergibt sich insbesondere daraus, dass von einer Vorratsdatenspeicherung nicht nur vermutete Straftäter oder deren Kontaktpersonen betroffen sind, sondern jeder Telekommunikationsnutzer unabhängig davon, ob er einen Grund für die Überwa-

---

90 Vgl. das Urteil des LG Darmstadt vom 25.01.2006 - 25 S 118/05, RDV 2006, 125, wonach bei einer „Flat-Rate“ die jeweils zugeordnete dynamische IP-Adresse unmittelbar nach dem Ende der jeweiligen Internetverbindung zu löschen ist, weil sie weder für die Entgeltermittlung noch die abrechnung erforderlich ist. Gegen das Urteil wurde Revision eingelegt, aber nicht zugelassen (vgl. Beschluss des Bundesgerichtshofs vom 26.10.2006 - III ZR 40/06, DuD 2006, 824 = MMR 2007, 37).

91 Pieroth/Schlink, Rdnr. 289; Stern, S. 782 ff.

92 Die besondere Interessenlage der Presse findet im Bereich des Artikel 10 GG noch keine Berücksichtigung, sondern ist der spezielleren Gewährleistung der Pressefreiheit vorbehalten, vgl. Frontal/Stern-Entscheidung des Bundesverfassungsgerichts (Urteil vom 12.03.2003 - 1 BvR 330/96 und 348/99, NJW 2003, 1787). Vgl. auch die Urteilsbesprechung von Kugelmann, NJW 2003, 1777: „Der Erste Senat sieht im Hinblick auf Artikel 10 GG Journalisten in der gleichen Gefährdungslage wie andere Nutzer und gibt pressespezifischen Erwägungen keinen Raum.“

chung geliefert hat oder in einer besonderen Nähebeziehung zu kriminellem Verhalten steht[93].

Insofern sei auch auf die Ausführungen des Bundesverfassungsgerichts[94] zum Niedersächsischen Gesetz über die öffentliche Sicherheit und Ordnung (Nds.SOG) verwiesen:

> *„Grundrechtlich bedeutsam ist ferner die große Streubreite der Eingriffe. Das Abhören und die Aufzeichnung der Gesprächsinhalte können eine große Zahl von Personen treffen. Erfasst sind nicht nur die potenziellen Straftäter, sondern alle, mit denen diese in dem betreffenden Zeitraum Telekommunikationsverbindungen nutzen. Dazu können Personen gehören, die in keiner Beziehung zu einer möglicherweise zu verhütenden oder später zu verfolgenden Straftat stehen, wie etwa Kontakt- und Begleitpersonen [...] oder gänzlich unbeteiligte Dritte [...].“*

Bei der Vorratsdatenspeicherung ist es demgegenüber sogar der absolute Regelfall, dass gänzlich unbescholtene Personen betroffen sind. Nach der Rechtsprechung des Bundesverfassungsgerichts ist es jedoch unzulässig, grundrechtseingreifende Maßnahmen ins „Blaue hinein“ vorzunehmen[95].

Es lässt sich auch nicht argumentieren, dass wesentliche Nachteile für den Betroffenen nicht schon mit der Speicherung der Verkehrsdaten, sondern erst infolge des anschließenden staatlichen Zugriffs drohen, und dass diesen Nachteilen durch eine Beschränkung der staatlichen Zugriffsrechte hinreichend begegnet werden könne[96]. Denn über derartige Zugriffsnormen kann nur der legale Datenzugriff reguliert werden; nicht ausgeschlossen werden kann hingegen die Gefahr des Datenmissbrauchs durch staatliche oder private Stellen[97]. Oder anders ausgedrückt: Je mehr Informationen über den Bürger gespeichert sind, desto eher be-

---

93 Breyer, S. 246 f.; Leutheusser-Schnarrenberger, ZRP 2007, 11.
94 Urteil vom 27.07.2005 - 1 BvR 668/04, NJW 2005, 2603, 2609.
95 Beschluss vom 04.04.2006 - 1 BvR 518/02, NJW 2006, 1939, 1946.
96 Ebenso Breyer, S. 245 f.
97 Breyer, S. 246; ähnlich Sievers, S. 192.

steht die Gefahr, dass diese zu seinen Lasten missbraucht werden.

Ferner ist die mit der Vorratsdatenspeicherung einhergehende Pauschalverdächtigung[98] geeignet, das Vertrauen des Einzelnen in die Nutzung moderner Kommunikationsmittel nachhaltig zu beeinträchtigen[99]. Wer ständig damit rechnen muss, sein Kommunikationsverhalten könne in der Zukunft einmal gegen ihn verwendet werden, wird im Zweifel versuchen, sich möglichst unauffällig zu verhalten bzw. Kommunikationsvorgänge gänzlich zu unterlassen[100]. Insoweit hat das Bundesverfassungsgericht[101] im Jahr 2003 wie folgt ausgeführt:

> *„Es gefährdet die Unbefangenheit der Nutzung der Telekommunikation und in der Folge die Qualität der Kommunikation einer Gesellschaft, wenn die Streubreite von Ermittlungsmaßnahmen dazu beiträgt, dass Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstehen."*

Noch verstärkt wird der in der Erfassung des Kommunikationsverhaltens liegende Grundrechtseingriff durch das rasante Wachstum der elektronischen Kommunikation[102]. Während vor 20 Jahren die elektronische Kommunikation lediglich einen Teilbereich der persönlichen Aktivitäten des Bürgers betraf, ist sie heute

---

98 Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder in Deutschland, DuD 2004, 605.

99 Sievers, S. 192; Breyer, S. 246, 249; Büllingen, DuD 2005, 350; BDI, DuD 2004, 608.

100 Breyer, S. 234.

101 Urteil vom 12.03.2003 - 1 BvR 330/96 und 348/99, NJW 2003, 1787, 1793.

102 Nach einer neueren ARD/ZDF Online Studie (Stand: Mai 2007) haben aktuell 40,8 Millionen Deutsche ab 14 Jahre Zugang zum Internet. Danach ist der Anteil der Internet-Nutzer in Deutschland auf 62,7 Prozent angestiegen (http://www.daserste.de/service/onlinestudie-2007-vorab.pdf). Die Risiken, die sich für den Grundrechtsschutz aus dem informationstechnischen Wandel ergeben, hat das Bundesverfassungsgericht kürzlich noch einmal in seiner GPS-Entscheidung (Urteil vom 12.04.2005 - 2 BvR 581/01, MMR 2005, 371) klargestellt, auf welche im Rahmen der nachstehenden Ausführungen zum gesetzgeberischen Handlungsbedarf (S. 49 ff.) noch näher eingegangen wird.

praktisch Teil aller Lebensbereiche[103]. Über die Erfassung und Auswertung des Kommunikationsverhaltens können weitreichende Aussagen über den Betroffenen getroffen werden[104].

Die Gewährleistung eines Mindestmaßes an unbeobachteter Kommunikation dient dabei nicht nur den individuellen Interessen der einzelnen Grundrechtsträger, sondern ist auch im Hinblick auf die Funktionsfähigkeit eines demokratischen Staatssystems (Artikel 20 Abs. 1 GG) unentbehrlich.

Jede Demokratie ist auf die aktive und unbefangene Mitwirkung ihrer Bürger angewiesen[105]. Sie lebt von der Meinungsfreude und dem Engagement der Bürger und setzt deshalb Furchtlosigkeit voraus[106].

Dort, wo

> *„ein Klima der Überwachung und Bespitzelung herrscht, [kann] ein freier und offener demokratischer Prozess nicht stattfinden“*[107]

Der unbefangene Umgang mit modernen Kommunikationsmitteln ist schließlich grundlegende Voraussetzung für die Fortentwicklung neuer Medien (Internet, Breitband, DSL, UMTS) und damit zugleich für die Weiterentwicklung der Informationsgesellschaft insgesamt[108].

---

[103] Vgl. Roßnagel, Datenschutz in einem informatisierten Alltag, S. 85 ff.; Ulmer/Schrief, DuD 2004, 596.

[104] Ähnlich Breyer, S. 247 („Die Aussagekraft der Daten ist extrem hoch.“); noch weiterreichender: Ulmer/Schrief, DuD 2004, 596 („Deshalb sind Persönlichkeitsbilder, die über die Erfassung des Kommunikationsverhaltens hergestellt werden, praktisch umfassend.“).

[105] Urteil des Bundesverfassungsgerichts vom 15.12.1983 - 1 BvR 209, 269, 362, 420, 440, 484/83, NJW 1984, 419, 422. Ähnlich: Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (8.-9. März 2007) zur Vorratsdatenspeicherung (vgl. Fn. 5).

[106] Limbach: Ist die kollektive Sicherheit Feind der individuellen Freiheit? 10.05.2002, http://www.zeit.de/reden/deutsche_innenpolitik/200221_limbach_sicherheit.

[107] Kutscha zitiert bei Limbach: Ist die kollektive Sicherheit Feind der individuellen Freiheit? 10.05.2002, http://www.zeit.de/reden/deutsche_innenpolitik/200221_limbach_sicherheit.

[108] BDI, DuD 2004, 608.

Die Behauptung, alleine auf Grund einer bloßen Datenvorhaltung könnten keine Nachteile entstehen, ist nach alledem nicht überzeugend. Tatsächlich resultieren aus einer Vorratsdatenspeicherung wesentliche Nachteile nicht nur für den einzelnen Grundrechtsträger (Überwachungsdruck, Möglichkeit des Datenmissbrauchs), sondern auch für die Gesellschaft als Ganzes (Gefährdung des furchtlosen Meinungsaustauschs als Basis eines demokratischen Staatswesens, Gefahr einer nachhaltigen Hemmung des Fortschreitens der Informationsgesellschaft).

Im Rahmen der Angemessenheit ist zudem zu berücksichtigen, dass der Staat nur einen verschwindend geringen Teil der auf seine Veranlassung gespeicherten Daten auch tatsächlich benötigt. Bei T-Online beträgt die Menge an Internetdaten, für die es Anträge zur Herausgabe durch Strafverfolgungsbehörden gibt, im Vergleich zum Gesamtverkehr 0,0004 %[109]. Die mit dieser Methode ermittelten Straftaten dürften noch deutlich unter diesem Wert liegen, denn nicht mit jedem Datenzugriff wird auch tatsächlich eine Tat aufgedeckt[110]. Ergänzend sei noch einmal darauf hingewiesen, dass die Anfragen der Behörden offensichtlich ganz überwiegend in den ersten drei Monaten erfolgen[111].

Darüber hinaus ist zu beachten, dass im Rahmen der Prüfung der Geeignetheit[112] festgestellt wurde, dass mit der Vorratsdatenspeicherung vor allem der Terrorismus und die organisierte Kriminalität bekämpft werden sollen, eine Umgehung ihrer Mechanismen aber gerade bei zunehmender Organisation der potenziellen Täter droht. Insofern kommt man nicht umhin, festzustellen, dass der staatliche Nutzen der Vorratsdatenspeicherung gegenüber den Beeinträchtigungen, die verursacht werden, gering ist[113]. Bereits an diesem Punkt erscheint die Angemessenheit der Vorratsdatenspeicherung mehr als zweifelhaft. Bezieht man dann noch mit ein, dass mit der Möglichkeit der Einführung eines „Quick Freeze“-

[109] Vgl. bei Uhe/Herrmann, S. 153.
[110] Uhe/Herrmann, S. 153.
[111] Vgl. oben S. 35.
[112] Siehe oben S. 32.
[113] Vgl. auch Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (vgl. Fn. 5), S. 19.

Verfahrens[114] eine zwar nicht vollkommen gleichwertige, aber wesentlich grundrechtsschonendere Alternative besteht, ist die Angemessenheit endgültig zu verneinen[115].

Bereits die Vorratsdatenspeicherung zur Verfolgung von Straftaten (§ 113b Nr. 1 TKG-E) ist folglich unverhältnismäßig und damit verfassungswidrig. Durch die im Regierungsentwurf zudem vorgesehenen Zugriffsmöglichkeiten zu Zwecken der Gefahrenabwehr (§ 113b Nr. 2 TKG-E) bzw. der Nachrichtendienste (§ 113b Nr. 3 TKG-E) wird die Unverhältnismäßigkeit der geplanten Regelungen noch gesteigert[116].

Hinsichtlich der Datenverwendung zum Zwecke der Abwehr von erheblichen Gefahren für die öffentliche Sicherheit (§ 113b Nr. 2 TKG-E) ist insofern zusätzlich zu berücksichtigen, dass es im Hinblick auf künftig lediglich erwartete Straftaten vielfach schwierig sein wird, das gefährdete Rechtsgut und den Grad seiner Gefährdung so klar zu bestimmen, dass eine nachvollziehbare Abwägung mit der Schwere des Eingriffs möglich ist[117]. Insoweit besteht die Gefahr einer ausufernden Datennutzung zu präventiven Zwecken. Nach der Rechtsprechung des Bundesverfassungsgerichts kann aber selbst bei höchstem Gewicht der drohenden Rechtsgutbeeinträchtigung nicht auf das Erfordernis einer hinreichenden Wahrscheinlichkeit verzichtet werden[118]. Zudem wird über § 113b Nr. 2 TKG-E der Anwendungsbereich der Vorratsda-

---

114 Siehe oben S. 35.

115 Ähnlich wie hier Leutheusser-Schnarrenberger, ZRP 2007, 13: „Der mit der Vorratsdatenspeicherung verbundene Eingriff in die Grundrechte fast aller Bürger ist zu tief und zu intensiv, als dass er von dem eher beschränkten Nutzen für den mit ihm bezweckten Rechtsgüterschutz aufgewogen werden könnte." Einen unverhältnismäßigen Eingriff in die Kommunikationsfreiheit der Bürgerinnen und Bürger nehmen auch die Datenschutzbeauftragten des Bundes und der Länder an, vgl. Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (8.-9. März 2007) zur Vorratsdatenspeicherung (vgl. Fn. 5).

116 So auch Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (vgl. Fn. 5), S. 23.

117 Urteil des Bundesverfassungsgerichts vom 27.07.2005 - 1 BvR 668/04, NJW 2005, 2603, 2610.

118 Beschluss vom 04.04.2006 - 1 BvR 518/02, NJW 2006, 1939, 1946.

tenspeicherung auf eine Vielzahl auch minderschwerer Fälle ausgedehnt, denn der Begriff der erheblichen Gefahr erfasst jegliche Gefahr für ein bedeutsames Rechtsgut[119].

Da das bestehende Nachrichtendienstrecht eine Beobachtung auch ohne konkreten Straftatenverdacht bzw. ohne konkrete Gefahrenlage ermöglicht, lässt der geplante Zugriff der Dienste auf die Vorratsdaten (§ 113b Nr. 3 TKG-E) eine extensive Überwachung weiter Bevölkerungskreise befürchten[120]. Dadurch potenzieren sich die bereits aufgezeigten Risiken für ein freies politisches und persönliches Engagement der Bürger.

3.2. Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 GG (informationelle Selbstbestimmung)

Das Recht auf informationelle Selbstbestimmung wird in Form der besonderen Gewährleistung in Artikel 10 Abs. 1 Var. 3 GG (Fernmeldegeheimnis) speziell geschützt[121].

3.3. Artikel 5 Abs. 1 S. 2 Alt. 1 GG (Pressefreiheit)

3.3.1. Anwendbarkeit

Nach der Rechtsprechung des Bundesverfassungsgerichts[122] kann die Pressefreiheit parallel neben Artikel 10 herangezogen werden:

> *„Der auf die prinzipielle Geheimnisqualität der Kommunikation bezogene Schutz des Artikel 10 GG kann [...] durch weitere Grundrechtsgarantien ergänzt werden, die wegen des Inhalts und des Kon-*

[119] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (vgl. Fn 5), S. 24.
[120] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (vgl. Fn. 5), S. 24 f.
[121] Vgl. oben S. 23.
[122] Urteil des Bundesverfassungsgerichts vom 14.07.1999 - 1 BvR 2226/94, 2420/95 und 2437/95, NJW 2000, 55, 58.

> *texts einer Kommunikation oder im Hinblick auf die beeinträchtigenden Folgen der Verwendung erlangter Kenntnisse in neuen Verwendungszusammenhängen einschlägig sind".*

3.3.2. Schutzbereich

Das Schutzgut der Pressefreiheit wird durch den Pressebegriff bestimmt[123]. Grundrechtsberechtigt sind alle *„im Pressewesen tätigen Personen und Unternehmen"*[124]. Dies sind vor allem Verleger, Herausgeber, Redakteure und Journalisten. Erfasst wird aber etwa auch der Sachbearbeiter in der Anzeigenabteilung oder der Buchhalter eines Presseunternehmens[125].

Der Schutzbereich der Pressefreiheit

> *„reicht von der Beschaffung der Information bis zur Verbreitung der Nachrichten und Meinungen"*[126].

Nach dem Bundesverfassungsgericht[127] erfasst die Gewährleistung der Pressefreiheit auch den sog. Informantenschutz:

> *„Die Gewährleistungsbereiche der Presse- und Rundfunkfreiheit schließen diejenigen Voraussetzungen und Hilfstätigkeiten mit ein, ohne welche die Medien ihre Funktion nicht in angemessener Weise erfüllen können. Geschützt sind namentlich die Geheimhaltung der Informationsquellen und das Vertrauensverhältnis zwischen Presse beziehungsweise*

---

123 Vgl. hierzu Ipsen, Rdnr. 411 ff.

124 Urteil des Bundesverfassungsgerichts vom 05.08.1966 - 1 BvR 586/62, 610/63 und 512/64, NJW 1966, 1603, 1604.

125 Vgl. Pieroth/Schlink, Rdnr. 570 (mit entsprechenden Rechtsprechungsnachweisen).

126 Urteil des Bundesverfassungsgerichts vom 05.08.1966 - 1 BvR 586/62, 610/63 und 512/64, NJW 1966, 1603, 1604.

127 Urteil vom 12.03.2003 - 1 BvR 330/96 und 348/99, NJW 2003, 1787, 1793. Dies hat das Bundesverfassungsgericht jüngst noch einmal in der Cicero-Entscheidung bestätigt (Urteil vom 27.02.2007 - 1 BvR 538/06 und 1 BvR 2045/06).

> *Rundfunk und den Informanten. Staatlichen Stellen ist es darüber hinaus grundsätzlich verwehrt, sich Einblick in die Vorgänge zu verschaffen, die zur Entstehung von Nachrichten oder Beiträgen führen, die in der Presse gedruckt oder im Rundfunk gesendet werden."*

Das Vertrauensverhältnis zwischen Pressevertretern und Informanten ist also Bestandteil der Gewährleistung der Pressefreiheit. Damit ist auch die Vertraulichkeit der elektronischen Kommunikation mit Presseangehörigen vom Schutzbereich des Art. 5 Abs. 1 S. 2 GG erfasst.

3.3.3. Eingriff

In die Pressefreiheit wird durch jede staatliche Maßnahme eingegriffen, die zu einer Unterbindung oder Behinderung der geschützten Pressetätigkeiten führt[128].

Ein solcher Eingriff liegt jedenfalls vor, sobald ein Telekommunikationsunternehmen auf Grund staatlicher Anordnung Auskunft über den Telekommunikationsverkehr von Pressevertretern erteilt[129].

Ebenso wie im Bereich des Fernmeldegeheimnisses[130] ist jedoch fraglich, ob ein Eingriff allein schon in der staatlich veranlassten Datenspeicherung gesehen werden kann.

Diesbezüglich hat das Bundesverfassungsgericht in der bereits zuvor zitierten Entscheidung Folgendes festgestellt[131]:

> *„Der freie Informationsfluss zwischen den Medien und Informanten wird bereits dann gefährdet, wenn der Informant durch die Mitteilung an den Journalisten Schwierigkeiten zu befürchten hat. Solche*

[128] Jarass/Pieroth, Artikel 5 Rdnr. 29.
[129] Urteil vom 12.03.2003 - 1 BvR 330/96 und 348/99, NJW 2003, 1787, 1793.
[130] Vgl. dazu oben S. 27.
[131] NJW 2003, 1787, 1793.

> *Nachteile können aber nicht nur durch die Preisgabe der Identität des Informanten, sondern auch dadurch entstehen, dass Strafverfolgungsorgane durch Zugriff auf die Medien wichtige Informationen wie seinen Aufenthaltsort oder ähnliche Tatsachen ermitteln können, an deren Geheimhaltung ihm gelegen ist. Durch deren befürchtete Offenlegung könnte der Informant sich von der Mitteilung an die Presse abschrecken lassen."*

Damit hat das Bundesverfassungsgericht anerkannt, dass der Informationsfluss zwischen Presse und Informanten nicht erst durch den staatlichen Zugriff als solchen beeinträchtigt wird. Vielmehr kann allein das Wissen um mögliche Zugriffe des Staates den Einzelnen daran hindern, sich vertrauensvoll an die Presse zu wenden. Das Vertrauensverhältnis zwischen Presse und Informanten wird also bereits durch eine staatlich veranlasste Datenspeicherung beeinträchtigt.

Mithin bedeutet die Vorratsspeicherung von Daten der elektronischen Kommunikation von bzw. zu Pressevertretern einen Eingriff in Artikel 5 Abs. 1 S. 2 GG.

3.3.4. Verfassungsrechtliche Rechtfertigung

Im Hinblick auf die Verfolgung eines legitimen Zwecks durch die Vorratsdatenspeicherung sowie die Geeignetheit und Erforderlichkeit der Maßnahme gelten die Ausführungen entsprechend, die bezüglich des Fernmeldegeheimnisses gemacht wurden[132].

Bezüglich der Verhältnismäßigkeit im engeren Sinne (Angemessenheit) ist zunächst die besondere Bedeutung zu betonen, die der Presse in einem freiheitlichen Staatswesen zukommt[133]:

> *„Die Freiheit der Medien ist konstituierend für die freiheitliche demokratische Grundordnung. Eine*

[132] Vgl. oben S. 32 ff.

[133] Urteil des Bundesverfassungsgerichts vom 12.03.2003 - 1 BvR 330/96 und 348/99, NJW 2003, 1787, 1793.

> *freie Presse und ein freier Rundfunk sind daher von besonderer Bedeutung für den freiheitlichen Staat. Dementsprechend gewährleistet Artikel 5 Abs. 1 S. 2 GG den im Bereich von Presse und Rundfunk tätigen Personen und Organisationen subjektive Freiheitsrechte [...] - von der Beschaffung der Information bis zur Verbreitung der Nachrichten und Meinungen."*

Innerhalb der Pressefreiheit besitzen das Recht zur Geheimhaltung der Informationsquellen und der Schutz des Vertrauensverhältnisses zwischen Presse und Informanten besondere Relevanz. Denn ohne die Zuarbeit von Informanten kann die Presse letztlich keinen Beitrag zur öffentlichen Diskussion, Offenlegung und Kontrolle gesellschaftlicher, wirtschaftlicher und politischer Vorgänge leisten[134]. Dem Vertrauensverhältnis zwischen Presse und Informanten kommt damit eine Bedeutung zu, die über den einzelnen konkreten Fall hinausgeht und die Arbeitsfähigkeit der Presse insgesamt betrifft[135].

Zwar hat das Bundesverfassungsgericht[136] - zuletzt im Cicero-Urteil[137] - festgestellt, dass der Medienfreiheit kein prinzipieller Vorrang vor dem Interesse an Strafverfolgung zukomme, die Medienfreiheit es mithin auch nicht gebiete, Journalisten generell von strafprozessualen Maßnahmen mit informatorischer Eingriffswirkung auszunehmen. Vielmehr bedürfe es der Abwägung durch den Gesetzgeber, ob und wie weit die Erfüllung der publizistischen Aufgaben einen Vorrang der Pressefreiheit gegenüber dem Interesse an einer rechtsstaatlich geordneten Rechtspflege rechtfertige und wie weit die Pressefreiheit ihrerseits an diesem Interesse ihre Grenzen finde.

Die vorhandenen gesetzlichen Zugriffsregelungen erhalten durch die Einführung der Vorratsdatenspeicherung eine vollkommen

---

134 Birkner/Rösler, ZRP 2006, 111.
135 Birkner/Rösler, ZRP 2006, 111.
136 Urteil vom 12.03.2003 - 1 BvR 330/96 und 348/99, NJW 2003, 1787, 1793 f.
137 Urteil vom 27.02.2007 - 1 BvR 538/06 und 1 BvR 2045/06.

neue Dimension. Während der Staat seine Strafverfolgungsmaßnahmen bislang nur auf solche Telekommunikationsverkehrsdaten stützen konnte, die bei den Telekommunikationsanbietern ohnehin vorhanden waren, würde der Nutzer moderner Informations- und Kommunikationsdienste und potenzielle Informant im Falle einer Vorratsdatenspeicherung damit leben müssen, dass sein Kommunikationsverhalten in nicht unerheblichem Maß allein zu staatlichen Zwecken dokumentiert wird. Dass insoweit eine grundsätzliche Änderung des Kommunikationsverhaltens droht, wurde bereits dargestellt[138]. Damit würde die Presse, die ihre Arbeitsfähigkeit ganz wesentlich auch aus der Möglichkeit der vertraulichen Mitteilung sensibelster Informationen bezieht, durch die Vorratsdatenspeicherung mit besonderer Intensität getroffen.

Mit der Vorratsdatenspeicherung wäre nach alledem ein einschneidender Eingriff in die Pressefreiheit verbunden. Ein solcher ist jedoch nicht gerechtfertigt.

Zur Rechtfertigung eines derart tiefgreifenden Eingriffs in die Pressefreiheit müssten mit der Vorratsdatenspeicherung zumindest nicht unerhebliche Vorteile einhergehen. Denn verhältnismäßig im engeren Sinne ist eine Maßnahme nur dann, wenn die Nachteile, die mit ihr verbunden sind, nicht außer Verhältnis zu den Vorteilen stehen, die sie bewirkt. Die Zweifelhaftigkeit der Effektivität der Vorratsdatenspeicherung wurde im Rahmen der Prüfung des Fernmeldegeheimnisses (Artikel 10 Abs. 1 Var. 3 GG) ebenso angesprochen wie die Möglichkeit des „Quick Freeze“ als deutlich grundrechtsschonenderes Mittel[139]. Die dargestellten Bedenken gelten auch im Hinblick auf den Eingriff in die Pressefreiheit. Angesichts der staatspolitischen Bedeutung des Schutzes der Vertraulichkeit der Redaktionsarbeit und der vertraulichen Kommunikation zwischen den Medien und ihren Informanten liegt daher erst recht ein unverhältnismäßiger und damit ungerechtfertigter Eingriff in die Pressefreiheit vor. Dies gilt jedenfalls dann, wenn eine Flankierung der Vorratsdatenspeiche-

[138] Vgl. oben S. 37 ff.
[139] Vgl. S. 32 f. und 35 f.

rung durch spezielle verfahrensrechtliche Sicherungen der Presse unterbleibt[140].

3.4. Ergebnis der verfassungsrechtlichen Würdigung

Die vorgesehene Umsetzung der Richtlinie 2006/24/EG in nationales Recht würde die Nutzer der betroffenen Kommunikationsformen (Telefonfestnetz und Mobilfunk, Internetzugang, Internet-E-Mail und Internet-Telefonie) in ihrem Grundrecht auf Gewährleistung des Fernmeldegeheimnisses (Artikel 10 Abs. 1 Var. 3 GG) verletzen[141]. Daneben würde auch das Grundrecht der Pressefreiheit (Artikel 5 Abs. 1 S. 2 Alt. 1 GG) unter dem Aspekt der vertraulichen Kommunikation zwischen Pressevertreter und Informant verletzt.

4. Handlungsbedarf des deutschen Gesetzgebers

4.1. Gebot der verfassungsschonenden Umsetzung

Trotz der beim Europäischen Gerichtshof eingereichten Nichtigkeitsklagen beabsichtigt der Gesetzgeber, die Umsetzung der Richtlinie 2006/24/EG in nationales Recht zeitnah zu vollziehen[142]. Die Erfahrung zeigt, dass grundrechtliche Positionen selten wieder aufgewertet werden, wenn nur einmal ein Konsens über ihre Einschränkung bestand[143]. Schon von daher sollte besonderer

---

140 Vgl. hierzu im Einzelnen auf S. 65 ff.

141 Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder in Deutschland, DuD 2004, 605; Breyer, S. 389 ff.; Ulmer/Schrief, DuD 2004, 593 ff.; Kühling, K&R 2004, 108 ff.; Vassilaki, MMR 2/2006, XIII.

142 Nach dem Regierungsentwurf soll das Gesetz zum 1. Januar 2008 in Kraft treten.

143 Sievers, S. 225.

Wert auf eine möglichst verfassungsschonende Regulierung gelegt werden.

Wie im Rahmen der verfassungsrechtlichen Würdigung aufgezeigt, ist bereits der durch die Richtlinie vorgegebene Speicherbefehl materiell grundrechtswidrig. Vor diesem Hintergrund obliegt dem Gesetzgeber im Übrigen eine besondere Verpflichtung zum Freiheitsschutz. Auch wenn er hinsichtlich der ersten Stufe der Vorratsdatenspeicherung, d.h. der Datenerhebung und -speicherung an die Vorgaben des europäischen Gesetzgebers gebunden sein mag, so gebietet die Grundrechtswidrigkeit dieser Maßnahme, jedenfalls den im Rahmen einer zweiten Stufe stattfindenden Datenzugriff möglichst grundrechtsschonend auszugestalten.

Für den Gesetzgeber wird es nicht nur darauf ankommen, überobligatorische[144] Umsetzungsmaßnahmen zu vermeiden, sondern auch darauf, dass die von der Richtlinie gewährten Spielräume entsprechend genutzt werden.

Insofern hat auch das Bundesverfassungsgericht[145] in seiner Entscheidung zum Europäischen Haftbefehl folgende Feststellungen getroffen:

> *„Der Gesetzgeber war jedenfalls verpflichtet, die Umsetzungsspielräume, die der Rahmenbeschluss den Mitgliedstaaten belässt, in einer grundrechtsschonenden Weise auszufüllen." (...)*
>
> *„Diese Bestimmungen lassen eine Begrenzung der Auslieferung durch innerstaatliches Recht zu. Der Gesetzgeber war beim Erlass des Umsetzungsgesetzes zum Rahmenbeschluss verpflichtet, das Ziel des Rahmenbeschlusses so umzusetzen, dass die dabei unumgängliche Einschränkung des Grundrechts auf Auslieferungsfreiheit verhältnismäßig ist. Insbeson-*

[144] Dies könnte zu einer Überprüfung durch das Bundesverfassungsgericht führen; vgl. auch die Ausführungen auf S. 17.

[145] Urteil des Bundesverfassungsgerichts vom 18.07.2005 - 2 BvR 2236/04, NJW 2005, 2289, 2291.

> *dere hat der Gesetzgeber über die Beachtung der Wesensgehaltsgarantie hinaus dafür Sorge zu tragen, dass der Eingriff in den Schutzbereich des Art. 16 Abs. 2 GG schonend erfolgt."*

Zwar hatte die Bundesregierung in Aussicht gestellt, es bei einer Minimalumsetzung der Richtlinie 2006/24/EG bewenden lassen zu wollen, und diese Absicht ist vom Deutschen Bundestag, der die Bundesregierung aufgefordert hat, alsbald einen mit Augenmaß formulierten Entwurf eines Gesetzes zur gebotenen Umsetzung der Richtlinie in innerstaatliches Recht vorzulegen, ausdrücklich befürwortet worden[146]. Gleichwohl beinhaltet der inzwischen vorgelegte Entwurf der Bundesregierung für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen und zur Umsetzung der Richtlinie 2006/24/EG"[147] Regelungen, die über das von der Richtlinie geforderte Maß hinausgehen und die Grenze zur Verfassungswidrigkeit überschreiten[148].

Derartige gesetzliche Vorschriften wären vom Bundesverfassungsgericht überprüfbar[149].

4.2. Maßgaben des Bundesverfassungsgerichts

Dem Gesetzgeber wird empfohlen, verstärkt die jüngere Rechtsprechung des Bundesverfassungsgerichts zu berücksichtigen.

Bedingt durch die Technikentwicklung in der Informationsgesell-

---

[146] Beschluss vom 16.02.2006 (vgl. BT-Dr 16/545). Anlässlich der dem Beschluss vorausgegangenen Debatte wurde nicht nur von Seiten der Opposition heftige Kritik an der Richtlinie geübt. Der SPD-Abgeordnete Tauss hat in diesem Zusammenhang einen „Anschlag auf Bürgerrechte und auf Datenschutz in Europa, der inakzeptabel ist" konstatiert (vgl. Plenarprotokoll 16/19 vom 16.02.2006).

[147] BR-Dr 275/07.

[148] Ebenso: Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (8.-9. März 2007) zur Vorratsdatenspeicherung (vgl. Fn. 5).

[149] Siehe vorstehend S. 17.

schaft und bestimmte gesetzgeberische Maßnahmen aus Gründen der inneren Sicherheit sind die Freiheitsrechte der Nutzer moderner Informations- und Kommunikationsdienste in erhöhtem Maße gefährdet. Mit Blick auf den erstgenannten Aspekt hat das Bundesverfassungsgericht[150] Folgendes festgestellt:

> *„Wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels muss der Gesetzgeber die technischen Entwicklungen aufmerksam beobachten und notfalls durch ergänzende Rechtssetzung korrigierend eingreifen."*

Neben dem vorzitierten GPS-Urteil sollten auch die jüngeren Entscheidungen des Bundesverfassungsgerichts zur Rasterfahndung[151] und zur präventiven Telekommunikationsüberwachung[152] berücksichtigt werden. Diese Entscheidungen verdeutlichen die Intensität von technikbasierten, verdachtlosen Grundrechtseingriffen mit großer Streubreite, die das Gericht in beiden Fällen als nicht gerechtfertigt angesehen hat. Dementsprechend hat inzwischen auch der Bundestag[153] hinsichtlich der Vorratsdatenspeicherung festgestellt, dass Grundrechtseingriffe, von denen zahlreiche Personen betroffen werden, die in keiner Beziehung zu einem konkreten Tatvorwurf stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben, besonders schwerwiegend sind und deshalb einer besonderen Rechtfertigung bedürfen.

Vor diesem Hintergrund werden nachfolgend gesetzgeberische Handlungsmöglichkeiten aufgezeigt, mit denen dem Recht auf informationelle Selbstbestimmung in seiner speziellen Ausprägung als Fernmeldegeheimnis und dem Grundrecht der Pressefreiheit zumindest bedingt Rechnung getragen werden kann. Im Vordergrund der Betrachtung steht dabei eine verfassungsschonende Richtlinienumsetzung im TKG und in der StPO[154].

---

150 Urteil vom 12.04.2005 - 2 BvR 581/01, MMR 2005, 371.
151 Beschluss vom 04.04.2006 - 1 BvR 518/02, NJW 2006, 1939.
152 Urteil vom 27.07.2005 - 1 BvR 668/04, NJW 2005, 2603.
153 BT-Dr 16/545, S. 3.
154 Soweit diese Regelungswerke den Umgang mit personenbezogenen Daten regeln, handelt es sich um bereichsspezifische Bestimmungen. Ziel derarti-

4.3. Regelungsbedarf in Bezug auf das TKG

4.3.1. Sechsmonatige Speicherpflicht zum Zwecke der Ermittlung, Feststellung und Verfolgung schwerer Straftaten

Zunächst ist festzustellen, dass schon aus Gründen der Grundrechtsschonung nicht über die in der Richtlinie vorgesehene Mindestspeicherfrist von sechs Monaten hinausgegangen werden sollte[155]. Dem trägt der Regierungsentwurf in § 113a Abs. 1 TKG-E Rechnung. Anders als in § 113a Abs. 11 TKG-E vorgesehen sollte jedoch eine Pflicht zur unverzüglichen Löschung der Daten nach Ablauf der sechsmonatigen Speicherfrist geregelt werden. Eine solche Pflicht besteht bereits nach geltender Rechtslage (vgl. §§ 96 Abs. 2 S. 2, 97 Abs. 3 S. 2 TKG). Gesetzliche Unklarheiten bezüglich der Löschungspflicht sollten vermieden werden.

§ 113b TKG-E, der die Verwendung der nach § 113a TKG-E gespeicherten Daten regelt, trägt dem Gebot der Grundrechtsschonung nicht angemessen Rechung, da er die von der Richtlinie eröffneten Spielräume nicht ausschöpft und überdies Zweifel an der notwendigen Bestimmtheit[156] der Norm bestehen. Nach der Richtlinienvorgabe soll mittels der Vorratsdatenspeicherung sichergestellt werden, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung „schwerer Straftaten“ verfügbar sind. Die Definition dessen, was unter den Begriff der schweren Straftaten subsumierbar ist, überlässt die Richtlinie den nationalen Gesetzgebern. Nach dem Wortlaut des § 113b TKG-E soll die

---

ger Regelungen ist, die generellen Anforderungen des Bundesdatenschutzgesetzes für einen jeweils näher definierten Verwendungszusammenhang zu präzisieren und weiterzuentwickeln. Siehe hierzu im Einzelnen Simitis/Simitis, § 28 Rdnr. 5 und Einleitung, Rdnr. 42, 122 ff.; ferner Gola/Schomerus, § 1 Rdnr. 23 ff. und § 4 Rdnr. 7. Zur Geltung des Grundsatzes der Datenvermeidung und Datensparsamkeit für Anbieter von Telekommunikationsdiensten vgl. Büttgen, RDV 2003, 215.

155 Vgl. BT-Dr 16/545, S. 4.

156 Vgl. S. 30.

Speicherung der Verkehrsdaten allgemein zur Verfolgung von Straftaten (Nr. 1 der Vorschrift), zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit (Nr. 2 der Vorschrift) bzw. zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes (Nr. 3 der Vorschrift) erfolgen[157]. Somit bliebe sowohl auf der Ebene der Datenspeicherung als auch auf der Ebene der Datenverwendung ein Umsetzungsspielraum insoweit ungenutzt, als es an einer Zweckbegrenzung auf die Ermittlung, Feststellung und Verfolgung schwerer Straftaten fehlt. Dieser Mangel würde nach dem Gesetzentwurf auch nicht etwa durch eine verfahrensrechtliche Zugriffsbeschränkung relativiert, da es auch auf der Zugriffsebene an einer entsprechenden Eingrenzung fehlt[158]. Insofern erscheint es angesichts der Verfassungswidrigkeit des Speicherbefehls und dem Gebot einer verfassungsschonenden Regulierung sachgerecht, die Speicherpflicht und die Datenverwendung auf den Zweck der Ermittlung, Feststellung und Verfolgung von Straftaten nach § 139 StGB zu begrenzen. Damit wäre eine richtlinienkonforme Umsetzung unter Wahrung des Bestimmtheitsgrundsatzes in nationales Recht erreicht.

Anders als in dem ursprünglichen Referentenentwurf[159] wird in der Begründung des Regierungsentwurfs eine ausdrückliche Regelung des Speicherungszwecks in § 113a TKG-E für entbehrlich gehalten. Es sollte aber weiterhin zwischen der Phase der Datenspeicherung und der nachfolgenden Datenverwendung unterschieden werden. Dass schon die Datenspeicherung den ersten Grundrechtseingriff darstellt, wurde bereits festgestellt[160]. Speziell mit Blick auf die Wahrung der Pressefreiheit sollte der Gesetzgeber im Übrigen prüfen, ob nicht bereits auf der Ebene der Datenerhebung bzw. im Rahmen der Aufbereitung der Daten zu staatlichen Zugriffszwecken in Kooperation mit bestimmten Akkreditierungsstellen seitens der Provider angemessene technisch-

[157] Zur Unverhältnismäßigkeit dieser Regelungen vgl. S. 37 ff.
[158] Vgl. S. 63 ff.
[159] Stand: 27. November 2006.
[160] Zu den verschiedenen Eingriffsstufen vgl. auch die Ausführungen auf S. 27.

organisatorische Vorkehrungen getroffen werden können (z.B. Filterung bestimmter Rufnummern bzw. Kennungen), die einen späteren Zugriff durch die Ermittlungs- bzw. Strafverfolgungsbehörden sachgerecht begrenzen. Insoweit sei darauf hingewiesen, dass der Gesetzgeber schon im Zusammenhang mit dem Einzelverbindungsnachweis in § 99 Abs. 2 TKG eine Regelung zur Wahrung der vertraulichen Kommunikation mit Berufsgeheimnisträgern getroffen hat[161].

Mit einer derartigen Beschränkung bereits auf der Ebene der Datenerhebung würde zugleich dem in § 3a BDSG normierten Grundsatz der Datenvermeidung und Datensparsamkeit[162] Rechnung getragen. Die Vorschrift konkretisiert ausweislich der Gesetzesbegründung den Grundsatz der Verhältnismäßigkeit für die technische Gestaltung der Datenverarbeitungssysteme. Bereits durch die Gestaltung der Systemstrukturen soll die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten soweit wie möglich vermieden werden. So sollen die Gefahren für das informationelle Selbstbestimmungsrecht des Betroffenen von vornherein minimiert werden.

4.3.2. Beschränkung der zu speichernden Datenkategorien/Klarstellung zur dynamischen IP-Adresse

Angesichts der europa- und verfassungsrechtlichen Bedenken und speziell mit Blick auf den Grundsatz der Verhältnismäßigkeit ist bei der nationalen Umsetzung insbesondere darauf zu achten, die Datenkategorien, auf die sich die Vorratsdatenspeicherung bezieht, strikt auf die Richtlinienvorgaben zu begrenzen[163].

---

[161] Zu der gesetzgeberischen Intention der Wahrung der Vertraulichkeit von Anrufen vgl. Königshofen/Ulmer, S. 84 ff.

[162] Zum so genannten Systemdatenschutz vgl. Roßnagel/Dix, S. 363 ff.; Roßnagel/Pfitzmann/Garstka, S. 39 ff.; Simitis/Bizer, § 3a Rdnr. 25.

[163] Auf die Notwendigkeit einer restriktiven Richtlinienumsetzung hat auch der Deutsche Bundestag (BT-Dr 16/545, S. 4) hingewiesen. Ferner hat sich die Gruppe nach Artikel 29 der EG-Datenschutzrichtlinie dafür ausgesprochen,

Sicherzustellen ist insbesondere, dass keine Inhalte elektronischer Datenübermittlung gespeichert werden. Diesbezüglich hat der Europäische Datenschutzbeauftragte[164] darauf hingewiesen, dass Artikel 1 Abs. 2 der Richtlinie auch im Internet eingesehene Informationen als Inhaltsdaten definiert. Vor diesem Hintergrund ist es als positiv zu bewerten, dass nach dem Regierungsentwurf[165] keine Speicherung der im Internet aufgerufenen Adresse (URL) vorgesehen ist.

Gemäß Artikel 5 Abs. 1 lit. a Ziffer 2 lit. iii der Richtlinie 2006/24/EG und § 113a Abs. 3 und 4 TKG-E zählt die IP-Adresse explizit zu den von den Providern vorzuhaltenden Datenkategorien. Die Einführung der in § 113a TKG-E vorgesehenen Speicherpflicht würde freilich eine Änderung der derzeit in Deutschland gegebenen Rechtslage bedeuten, nach der eine bei Einwahl in das Internet zugeteilte dynamische IP-Adresse[166] des Nutzers gelöscht werden muss, sobald sie für Abrechnungszwecke nicht mehr erforderlich ist[167]. § 113a Abs. 4 TKG-E verpflichtet Anbieter von Internetzugangsdiensten zur Speicherung der zugewiesenen IP-Adresse. Die Verfügbarkeit dieser Daten ist nach der Begründung des Regierungsentwurfs[168] für Ermittlungszwecke unverzichtbar, um nachvollziehen zu können, welchem Anschluss zu einem bestimmten Zeitpunkt eine bestimmte IP-Adresse zugewiesen war, die für einen bestimmten Kommunikationsvorgang im Internet genutzt wurde.

In Zeiten moderner elektronischer Kommunikation und der zunehmenden Nutzung der anfallenden Daten durch Strafverfolgungs- und Sicherheitsbehörden ist ein effektiver Grundrechts-

---

dass so wenig Daten wie möglich auf Vorrat gespeichert werden (WP 119 vom 25.03.2006).

164 Vgl. Amtsblatt der Europäischen Union, C 298/8.

165 BR-Dr 275/07, S. 166.

166 Zur Qualifizierung der IP-Adresse als personenbeziehbares Verkehrsdatum vgl. Tinnefeld/Ehmann/Gerling, S. 284 ff.

167 Beschluss des BGH vom 26.10.2006 - III ZR 40/06, K &R 2006, 578; Urteil des LG Darmstadt vom 25.01.2006 - 25 S 118/05, RDV 2006, 125. Vgl. hierzu auch Wüstenberg, RDV 2006, 102 sowie Köcher/Kaufmann, DuD 2006, 360.

168 BR-Dr 275/07, S. 165.

schutz nur erreichbar, wenn auch die Verknüpfung der dynamischen IP-Adresse mit Bestandsdaten der Nutzer im Wege eines staatlichen Auskunftsersuchens dem Fernmeldegeheimnis unterliegt[169]. Hinsichtlich der Nachvollziehbarkeit des „Surfens“ im Internet ist daher eine gesetzliche Klarstellung[170] dahingehend angezeigt, dass die Zuordnung der dynamischen IP-Adresse zu einem bestimmten Nutzer als näherer Umstand eines Telekommunikationsvorgangs nach § 88 TKG dem Fernmeldegeheimnis unterliegt[171]. Denn erst aus der Kombination dieser Daten wird ersichtlich, wer zu welchem Zeitpunkt welche Internetseiten aufgerufen hat. Zu Recht hat daher das LG Bonn[172] festgestellt, dass erst durch eine Auswertung des konkreten Verbindungsvorgangs durch den Provider eine entsprechende Zuordnung möglich wird. Ohne den staatlich veranlassten Zugriff auf durch das Fernmeldegeheimnis geschützte Verkehrsdaten kann die begehrte Auskunft also gar nicht erteilt werden. Insofern ist es sachgerecht, dass nach dem Gesetzentwurf[173] ein auf entsprechende Überwachungs- und Auskunftsanordnungen spezialisierter Richter entscheidet.

Mit der hier vorgeschlagenen Lösung wäre - der Eingriffsintensität angemessen - sichergestellt, dass die von der Richtlinie bezweckte Zugriffsmöglichkeit auf die von den Providern zu Ermittlungs- bzw. Strafverfolgungszwecken vorzuhaltenden personenbezogenen Daten, die Aufschluss über die Art und Weise der Internetnutzung geben, nicht nach § 113 TKG[174], sondern nur unter den Voraussetzungen von § 100g i.V.m. §§ 100a, 100b StPO-E, also grundsätzlich nur bei Vorliegen einer ordnungsge-

---

169 Dies ist bislang streitig. Zum Meinungsstand vgl. die Begründung des Regierungsentwurfs, S. 53.

170 Eine solche fordern auch Gercke, StraFo 2005, 244 sowie Gnirck/Lichtenberg, DuD 2004, 598.

171 Ebenso Spindler/Dorschel, CR 2005, 46 sowie Köbele, DuD 2004, 609; anderer Ansicht z.B. Bundesrat, BR-Dr 275/07 (Beschluss), S. 14.

172 DuD 2004, 628; ebenso zuletzt AG Offenburg, Beschl. v. 20.7.2007 - Az. 4 Gs 442/07

173 BR-Dr 275/07, S. 53 und 71.

174 Die Vorschrift regelt das so genannte manuelle Auskunftsverfahren im Hinblick auf Bestandsdaten.

mäßen richterlichen Anordnung besteht[175]. Insofern bietet sich eine Ergänzung der in § 3 Nr. 30 TKG enthaltenen Legaldefinition an. Hier sollte gesetzlich klargestellt werden, dass der Begriff der „Verkehrsdaten" auch Bestandsdaten der „Teilnehmer eines konkreten Telekommunikationsvorgangs" erfasst.

Angesichts der modernen Kommunikationsformen hat auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit wiederholt die Schaffung eines umfassenden Kommunikations-[176] bzw. Mediennutzungsgeheimnisses[177] gefordert.

Überdies hat das Bundesverfassungsgericht[178] bereits in anderem Zusammenhang klargestellt, dass es mit dem aus Artikel 10 Abs. 2 GG resultierenden Erfordernis einer bereichsspezifischen, präzisen und normenklaren Begrenzung des Grundrechtseingriffs nicht vereinbar wäre, „wenn die Ermittlungsbehörden auf eine andere Zwangsmaßnahme zurückgreifen könnten, an die geringere Anforderungen in Bezug auf das Anordnungsverfahren gestellt sind, um zum gleichen Ziel zu gelangen, nämlich dem unfreiwilligen Offenbaren der durch Artikel 10 Abs. 1 GG geschützten Daten".

4.3.3. Zugriffsberechtigte und Zweckbindung

Nach § 88 Abs. 3 S. 3 TKG dürfen Kenntnisse über den Inhalt oder die näheren Umstände der Telekommunikation zu anderen Zwecken als der sicheren Erbringung des Telekommunikationsdienstes nur verwendet oder an andere weitergegeben werden,

---

[175] Vgl. auch Urteil des Bundesverfassungsgerichts vom 12.03.2003 - 1 BvR 330/96 und 1 BvR 348/99, NJW 2003, 1787, 1792. Für eine richterliche Prüfung plädiert auch die Artikel 29-Datenschutzgruppe, vgl. WP 119 vom 25.03.2006.

[176] Vgl. den Bericht von Klug über das 6. Symposium des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit „Datenschutz in der Telekommunikation und bei Telediensten", RDV 2006, 37.

[177] „Zehn Thesen für eine datenschutzfreundliche Informationstechnik" vom 18.12.2006, Ziffer 7.

[178] Beschluss vom 04.02.2005 - 2 BvR 308/04, RDV 2005, 114 = MMR 2005, 520, 523.

soweit das TKG oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht.

Bereits die Datenerhebung und -speicherung stellen Grundrechtsbeeinträchtigungen dar[179]. Der staatliche Zugriff auf die Daten ist ein noch intensiverer Eingriff. Er sollte daher strikt begrenzt werden. Diesbezüglich stellt Artikel 4 der Richtlinie 2006/24/EG folgende Anforderungen:

> *„Die Mitgliedstaaten erlassen Maßnahmen, um sicherzustellen, dass die gemäß dieser Richtlinie auf Vorrat gespeicherten Daten nur in bestimmten Fällen und in Übereinstimmung mit dem innerstaatlichen Recht an die zuständigen nationalen Behörden weitergegeben werden."*

Notwendig sind mithin aus bundesdeutscher Sicht dem Bestimmtheitsgrundsatz Rechnung tragende Regelungen, die nicht nur den Anlass, sondern auch die zur Datenabfrage Berechtigten konkret festlegen. Von zentraler Bedeutung ist in diesem Zusammenhang die Wahrung des Zweckbindungsgrundsatzes. Artikel 1 Abs. 1 der Richtlinie 2006/24/EG trifft hierzu die Aussage, dass die Daten zum Zwecke der Ermittlung, Feststellung und Verfolgung schwerer[180] Straftaten zur Verfügung stehen. Diese Zweckbindung darf nicht unterlaufen werden. Vor diesem Hintergrund war der Regierungsentwurf[181] eines TKG-Änderungsgesetzes insofern zu Recht kritisiert worden, als er in § 96 Abs. 2 S. 1 vorsah, dass Verkehrsdaten über das Ende der Verbindung auch verwendet werden, wenn sie

> *„für die durch andere gesetzliche Vorschriften begründeten Zwecke erforderlich sind".*

Inzwischen ist das Gesetz ungeachtet der vorherigen Kritik mit gleichem Wortlaut in Kraft getreten[182]. Durch die Neufassung von

---

179 Siehe vorstehend S. 27.
180 Vgl. hierzu auch nachstehende Ausführungen auf S. 63 f.
181 BR-Dr 92/05.
182 BGBl. I vom 23.02.2007, S. 106.

§ 96 Abs. 2 S. 1 TKG ist der bisher relativ klar bezeichnete Zweckbindungskatalog der Vorschrift erheblich erweitert worden. Nach der Entwurfsbegründung[183] soll mit der Regelung klargestellt werden, dass die Daten für die in §§ 100g, 100h StPO, § 8 Abs. 8 und 10 BVerfSchG, § 10 Abs. 3 MAD-Gesetz und § 8 Abs. 3a BND-Gesetz geregelte Erteilung von Auskünften an Strafverfolgungs- und Sicherheitsbehörden verwendet werden dürfen. Auf Grund des nunmehr unbestimmten Wortlauts ist allerdings eine immer weiter ausgreifende Auslegung anhand aktueller Bedürfnisse sogar über den Sicherheitsbereich hinaus und damit eine schleichenden Zweckentfremdung zu befürchten[184]. Diese bereits erfolgte TKG-Änderung ist im Zusammenhang mit der geplanten Neuregelung in § 113a TKG-E (Speicherpflichten für Daten), § 113b TKG-E (Verwendung der nach § 113a gespeicherten Daten) und den eigentlichen gesetzlichen Eingriffsermächtigungen zu sehen. § 100g StPO-E, der die Verwendung von Verkehrsdaten zu Strafverfolgungszwecken regelt, nimmt ausdrücklich auf die §§ 96 Abs.1, 113a TKG Bezug.

Aus Gründen der Transparenz für die Normadressaten und die betroffenen Grundrechtsträger hat die Artikel 29-Datenschutzgruppe die Veröffentlichung einer Liste der zugangsberechtigten Behörden gefordert[185].

Des Weiteren ist festzustellen, dass der - bereits im Hinblick auf

---

183 BR-Dr 92/05, S. 36.

184 So auch Köcher/Kaufmann, DuD 2006, 364. Parallel regelt inzwischen § 14 Abs. 2 TMG Folgendes: „Auf Anordnung der zuständigen Stellen darf der Diensteanbieter im Einzelfall Auskunft über Bestandsdaten erteilen, soweit dies für Zwecke der Strafverfolgung, zur Gefahrenabwehr durch die Polizeibehörden der Länder, zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes oder zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist.“ § 15 Abs. 5 S. 4 TMG ordnet die entsprechende Anwendung von § 14 Abs. 2 TMG für den Bereich der Nutzungsdaten an.

185 WP 119 vom 25.03.2006. Vgl. ferner den Bericht von Klug über das 5. Symposium des Bundesbeauftragten für den Datenschutz „Datenschutz in der Telekommunikation und bei Telediensten“, RDV 2004, 289, 292, wonach Provider einen Leitfaden betreffend ihrer Mitwirkungspflichten bei staatlichen Ermittlungstätigkeiten als sinnvoll erachten.

die in § 113b Nr. 1 TKG-E genannte Verfolgung von Straftaten zu weit gehende[186] - Gesetzentwurf der Bundesregierung auch hinsichtlich der Verwendung von Daten zur Gefahrenabwehr (Nr. 2 der Vorschrift) und zur Aufgabenerfüllung der Nachrichtendienste (Nr. 3 der Vorschrift) über die Vorgaben der Richtlinie 2006/24/EG hinausgeht[187]. Insofern blieben wesentliche Richtlinienspielräume ungenutzt und das Gebot einer verfassungsschonenden Richtlinienumsetzung bliebe schon auf der Ebene der Datenspeicherung bzw. -verwendung unbeachtet.

Vor diesem Hintergrund sollten die in dem ursprünglichen Referentenentwurf des Bundesministeriums der Justiz noch nicht enthaltenen Verwendungsmöglichkeiten nach § 113b Nr. 2 und 3 TKG-E wieder gestrichen werden.

4.4. Regelungsbedarf im Rahmen der StPO

4.4.1. Notwendigkeit verfahrensrechtlicher Grundrechtssicherung

Die Richtlinie zur Vorratsdatenspeicherung hat dem nationalen Gesetzgeber hinsichtlich ihrer Umsetzung folgenden Rahmen vorgegeben (Artikel 4 S. 2):

> *„Jeder Mitgliedstaat legt in seinem innerstaatlichen Recht unter Berücksichtigung der einschlägigen Bestimmungen des Rechts der Europäischen Union oder des Völkerrechts, insbesondere der EMRK in der Auslegung durch den Europäischen Gerichtshof für Menschenrechte, das Verfahren und die Bedingungen fest, die für den Zugang zu auf Vorrat gespeicherten Daten gemäß den Anforderungen der Notwendigkeit und der Verhältnismäßigkeit einzuhalten sind."*

[186] Siehe hierzu die nachstehenden Ausführungen auf S. 63 ff.

[187] Ebenso Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (vgl. Fn. 5), S. 23 ff. sowie BITKOM-Stellungnahme zum Regierungsentwurf (vgl. Fn. 5), Ziffer 2.3.1.

Das Bundesverfassungsgericht[188] hat unlängst im Rahmen der GPS-Entscheidung angesichts der technikbedingten Risiken für den Grundrechtsschutz darauf hingewiesen, dass der Gesetzgeber notfalls durch ergänzende Rechtssetzung korrigierend eingreifen müsse. In diesem Zusammenhang hat das Gericht hinsichtlich einer verfahrensrechtlichen Grundrechtssicherung Folgendes festgestellt:

> *„Dies betrifft auch die Frage, ob die bestehenden verfahrensrechtlichen Vorkehrungen angesichts zukünftiger Entwicklungen geeignet sind, den Grundrechtsschutz effektiv zu sichern und unkoordinierte Ermittlungsmaßnahmen verschiedener Behörden verlässlich zu verhindern."*

Mit der gesetzlichen Einführung einer anlasslosen, massenhaften Vorratsdatenspeicherung „im Auftrag" des Staates durch Institutionen der Privatwirtschaft erfolgt ein Paradigmenwechsel[189], der die strafprozessualen Ermittlungsbefugnisse (§§ 100g, 53b StPO-E) in einem neuen Licht erscheinen lässt. Die Überwachungsmöglichkeiten des Staates steigen mit der Vorratsdatenspeicherung immens. Gerade beim Einsatz moderner, insbesondere dem Betroffenen verborgenen Ermittlungsmethoden müssen den Strafverfolgungsbehörden mit Rücksicht auf das dem „additiven" Grundrechtseingriff innewohnende Gefährdungspotenzial im Verfahrensrecht Grenzen gesetzt werden. Mit Blick auf den in der GPS-Entscheidung formulierten Auftrag an den Gesetzgeber und die besondere Intensität von technikbasierten, verdachtlosen Grundrechtseingriffen mit großer Streubreite bedarf es einer besonderen verfahrensrechtlichen Grundrechtssicherung, zumal schon der richtlinienbedingte Speicherbefehl materiell grundrechtswidrig ist[190].

---

188 Urteil vom 12.04.2005 - 2 BvR 581/01, MMR 2005, 371.

189 Zum Verbot der Sammlung von Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken vgl. das Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983 - 1 BvR 209, 269, 362, 420, 440, 484/83, NJW 1984, 419.

190 Siehe vorstehende verfassungsrechtliche Würdigung (S. 23 ff.).

Der Regierungsentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen und zur Umsetzung der Richtlinie 2006/24/EG“ trägt der Notwendigkeit eines effektiven Grundrechtsschutzes insofern nur bedingt Rechnung.

4.4.2. Verfahrensrechtliche Sicherung des Fernmeldegeheimnisses

Zum Schutz des Fernmeldegeheimnisses bedarf es im Hinblick auf die verdachtlos auf Vorrat gespeicherten Daten einer restriktiven Zugriffsermächtigung.

Die technikbasierte Vorratsdatenspeicherung ist materiell grundrechtswidrig. Schon dieser Umstand zwingt den deutschen Gesetzgeber, alle sich aus der Richtlinie 2006/24/EG ergebenden Spielräume zum Schutz der Grundrechte auszuschöpfen. Der Vorrang des Gemeinschaftsrechts kann als „Rechtfertigung“ für Grundrechtsverletzungen in Deutschland nur insoweit „tragen“, als dieses dem nationalen Gesetzgeber zwingende Vorgaben macht. Auch wenn der Gesetzgeber hinsichtlich der ersten Stufe der Vorratsdatenspeicherung, d.h. der Datenerhebung und -speicherung an die Vorgaben des europäischen Gesetzgebers gebunden sein mag, so gebietet die Grundrechtswidrigkeit dieser Maßnahme doch, zumindest den im Rahmen einer zweiten Stufe stattfindenden Datenzugriff möglichst grundrechtsschonend auszugestalten.

Gemäß § 100g Abs. 1 StPO-E sollen zwei Kategorien von Straftaten die Erhebung von Verkehrsdaten rechtfertigen, nämlich Straftaten von auch im Einzelfall erheblicher Bedeutung (Nr. 1 der Vorschrift) und „mittels Telekommunikation“ begangene Straftaten (Nr. 2 der Vorschrift).

Es wurde bereits festgestellt[191], dass die Mitgliedstaaten nach der Richtlinie die gesetzlichen Voraussetzungen dafür schaffen müssen, dass die auf Vorrat zu speichernden Verkehrsdaten zum

[191] Siehe vorstehende Ausführungen auf S. 11 ff.

Zwecke der Ermittlung, Feststellung und Verfolgung von „schweren Straftaten“ zur Verfügung stehen. Dabei belässt die Richtlinie den Mitgliedstaaten einen Spielraum hinsichtlich der Definition des Begriffs der „schweren Straftat“. Diesen Umsetzungsspielraum sollte der Gesetzgeber in verfassungsschonender Weise nutzen.

Erwägungsgrund 9 der Richtlinie nennt insofern ausdrücklich Fälle der organisierten Kriminalität und Terrorismus. Vor diesem Hintergrund und mit Blick darauf, dass bereits die Speicherverpflichtung materiell grundrechtswidrig ist, erscheint es sachgerecht, lediglich schwere Straftaten i.S.v. § 139 StGB als Anlasstaten anzuerkennen. Hierdurch könnte auch dem Bestimmtheitsgrundsatz[192] Rechnung getragen werden.

Insbesondere eine Einbeziehung von mittels Telekommunikation begangenen Straftaten, die nicht schwer wiegen, würde hingegen eindeutig über das von der Richtlinie geforderte Maß an Umsetzung hinausgehen[193]. Der Umstand, dass das Bundesverfassungsgericht in einer jüngeren Entscheidung[194] mittels einer Endeinrichtung begangene Straftaten als Anordnungsvoraussetzung nicht beanstandet hat, vermag nichts daran zu ändern, dass die festgestellte materielle Grundrechtswidrigkeit der Vorratsdatenspeicherung den deutschen Gesetzgeber zwingt, alle sich aus der Richtlinie 2006/24/EG ergebenden Spielräume zum Schutz der Grundrechte auszuschöpfen. Ferner stand der Beschluss des Gerichts auch noch nicht im Zeichen der durch die Vorratsdatenspeicherung erheblich verstärkten Eingriffsintensität. Auch die Begründung des Regierungsentwurfs[195] räumt insofern ein, dass die Verkehrsdatenerhebung schon alleine durch die Ausweitung des mit der Vorratsdatenspeicherung einhergehenden Datenvolumens insgesamt an Eingriffsintensität gewinnt.

---

192 Siehe vorstehend S. 30.

193 Zur Überprüfbarkeit derartiger Regelungen durch das Bundesverfassungsgericht siehe vorstehend S. 17.

194 Beschluss des Bundesverfassungsgerichts vom 22.08.2006 - 1 BvR 1168/04, RDV 2006, 259.

195 BR-Dr 275/07, S. 117.

Dieser additive und materiell verfassungswidrige Grundrechtseingriff auf der Speicherebene macht im Hinblick auf die „Vorratsdaten“ eine angemessene Zugriffsbeschränkung erforderlich. Daher sollte in § 100g StPO ein eigener Tatbestand für den Zugriff auf „Vorratsdaten“ eingefügt werden, der den Zugriff auf die nach § 113a TKG-E zu speichernden Daten nur zum Zwecke der Verfolgung von Straftaten nach § 139 StGB gestattet. Damit würde der Maßstab der Richtlinie (schwere Straftaten) in verfassungsschonender Weise umgesetzt.

Die hier vorgeschlagene Lösung bedingt freilich eine Abgrenzung der „Vorratsdaten“ gegenüber den sonstigen Daten. In diesem Zusammenhang bietet es sich an, den Begriff der „Vorratsdaten“ in § 3 TKG legal so zu definieren, dass es sich hierbei um Verkehrsdaten handelt, die für eigene Geschäftszwecke der TK-Unternehmen (Diensteerbringung, Abrechnung, Datensicherheit) nicht mehr erforderlich, aber gemäß § 113a Abs. 1 TKG-E zu speichern sind. Dies würde auch der bisherigen Rechtsprechung Rechnung tragen[196], die ebenfalls von einer Bevorratung mit Daten ausgeht, wenn die vorgenannten Zwecke entfallen sind.

4.4.3. Verfahrensrechtliche Sicherung der Pressefreiheit

Was für die Nutzer moderner Informations- und Kommunikationsmittel nach den in Artikel 10 GG zum Ausdruck gebrachten Grundsätzen des Rechts auf informationelle Selbstbestimmung gilt, muss im Wege eines Erst-Recht-Schlusses auf die vom Grundgesetz zusätzlich geschützten Pressevertreter und deren Informanten[197] übertragen werden[198].

---

[196] Vgl. zuletzt BGH, Beschluss vom 26.10.2006 - III ZR 40/06, MMR 2007, 37; Vorinstanzen: LG Darmstadt, Urteil vom 25.01.2006 - 25 S 118/05, MMR 2006, 330 und AG Darmstadt, Urteil vom 30.06.2005 - 300 C 397/04, MMR 2005, 634.

[197] Zum Informantenschutz allgemein vgl. Gola/Schomerus, § 19 Rdnr. 25.

Der mit der Vorratsdatenspeicherung einhergehende Paradigmenwechsel wirkt sich im Bereich der Presse in besonderem Maße aus, denn mit der Vorratsdatenspeicherung wird auch jede Kontaktaufnahme per Telefon, E-Mail, SMS und Internet von oder zu einem Pressevertreter für einen längeren Zeitraum rückverfolgbar. Dieser Umstand lässt befürchten, dass ein Einschüchterungseffekt[199] eintritt und die Informationsquellen der Presse weniger werden.

Angesichts der geänderten Gefährdungslage bedarf es einer Anpassung der Verfahrensvorschriften, die der aktuellen Arbeitsweise der Presse und dem Informantenschutz unter den Bedingungen der Informationsgesellschaft angemessen Rechnung trägt[200]. Auch das Bundesverfassungsgericht[201] hat jüngst noch einmal die Unentbehrlichkeit der Vertrauenssphäre zwischen den Medien und ihren Informanten und die Bedeutung des Redaktionsgeheimnisses betont.

Beispielsweise die Fälle Cicero[202], WAZ[203] und BND[204] haben zuletzt verdeutlicht, dass die Hemmschwelle staatlicher Ermittlungsbehörden gegenüber Journalisten offensichtlich gesunken ist und dass im Hinblick auf die Wahrung der Pressefreiheit gesetzgeberischer Handlungsbedarf besteht[205]. Auch nach der Koalitionsvereinbarung sollen im Rahmen einer Reform der Medien-

---

198 Soweit die Arbeit der Presse unter Nutzung von Telekommunikationseinrichtungen erfolgt, greifen Artikel 5 Abs. 1 S. 2 GG und Artikel 10 Abs. 1 GG. Vgl. hierzu Kugelmann, NJW 2003, 1777.

199 Vgl. auch Sievers, S. 177, der der freien Internetkommunikation in einer demokratischen Informationsgesellschaft insgesamt hohes Gewicht beimisst.

200 So auch Kugelmann, ZRP 2005, 261.

201 Urteil vom 27.02.2007 - 1 BvR 538/06, 1 BvR 2045/06.

202 RDV 2007, 67, vgl. auch Birkner/Rösler, ZRP 2006, 109 sowie Kugelmann, ZRP 2005, 260.

203 Vgl. Birkner/Rösler, a. a. O.

204 Auf Antrag des betroffenen Journalisten durfte der so genannte Schäfer-Bericht über die BND-Bespitzelung von Medienvertretern aus Gründen der informationellen Selbstbestimmung nicht mit den personenbezogenen Daten des Antragstellers veröffentlicht werden (vgl. VG Berlin, Beschluss vom 23.05.2006, VG 2 A 72.06).

205 Im Ergebnis ebenso Birkner/Rösler, ZRP 2006, 109; Kugelmann, ZRP 2005, 262; ferner Gola/Klug, NJW 2006, 2460.

und Kommunikationsordnung insbesondere die Pressevielfalt, die Bürgerrechte und der besondere Schutz der Journalisten gesichert werden.

Das Europäische Parlament hat anlässlich seiner legislativen Entscheidung[206] zur Vorratsdatenspeicherung vom 14. Dezember 2005 folgende Aussage getroffen:

> *„Das Europäische Parlament ... ist der Auffassung, dass die Mitgliedstaaten das Recht haben, ihre eigenen Verfassungsgrundsätze anzuwenden, und ist insbesondere der Ansicht, dass das Berufsgeheimnis bei der Anwendung dieser Richtlinie gewahrt bleibt."*

Dieser Aussage hat sich nachfolgend auch der Deutsche Bundestag durch Beschluss vom 16. Februar 2006 angeschlossen[207].

Näheren Aufschluss über die gesetzgeberische Intention des Europäischen Parlaments gibt die englischsprachige Fassung der Entschließung:

> *„The European Parliament … considers that the Member States have the right to apply their national constitutional principles and considers especially that professional secrecy will also be respected in the application of the present directive."*

Die Formulierung verdeutlicht, dass nach dem Willen des EU-Parlaments bei der Anwendung der Richtlinie ein besonderes Augenmerk auf die Wahrung von Berufsgeheimnissen gerichtet werden soll.

Es wurde bereits festgestellt, dass der Gesetzgeber die Befugnis hat, im verfassungsrechtlich vorgegebenen Rahmen über Beschränkungen der Pressefreiheit - auch im Rahmen der StPO - zu entscheiden, wobei für ihn keine verfassungsrechtliche Verpflich-

---

206 P6_TA(2005)0512, Ziffer 4.

207 BT-Dr 16/545, S. 4. Ebenso hat sich der Berliner Beauftragte für Datenschutz und Informationsfreiheit geäußert, http://www.datenschutz-berlin.de/ueber/referate/ebert_stiftung.pdf, S. 8.

tung besteht, der Pressefreiheit den absoluten Vorrang vor der Strafrechtspflege einzuräumen. An dieser Stelle sei aber nochmals die staatspolitische Bedeutung einer nicht staatlich gelenkten und beeinflussten Presse betont, auf die auch der Bundestag im Zusammenhang mit der Vorratsdatenspeicherung hingewiesen hat[208]. Die Rückverfolgbarkeit jeder elektronischen Kommunikation der Presse gefährdet die Informationsquellen der Pressemitarbeiter und damit die Funktionsfähigkeit der Presse insgesamt. Vor diesem Hintergrund ist nicht ersichtlich, warum zwar Abgeordnete um des Funktionierens der Demokratie willen über § 53b Abs. 1 StPO-E vor Ermittlungsmaßnahmen geschützt werden sollen, solange sie nicht strafbarer Beteiligung hinreichend verdächtig sind, Pressemitarbeiter hingegen nicht.

Wenn auch das Bundesverfassungsgericht keinen generellen Vorrang der Pressefreiheit annimmt[209], so hat es aber immerhin - schon vor der durch die Vorratsdatenspeicherung verstärkten Eingriffsintensität - deutlich gemacht, dass der grundgesetzliche Schutz von Journalisten bei der Strafverfolgung durch besondere nach Artikel 5 Abs. 1 S. 2 GG erforderliche Verhältnismäßigkeitserwägungen zu garantieren ist, in die namentlich sowohl die Schwere der Straftat als auch der elementare Schutz der Presse und der Informantenschutz einzubeziehen sind. Primär ist es dabei Aufgabe des Gesetzgebers, im verfassungsrechtlichen Rahmen die einfachgesetzliche Güterabwägung zwischen Pressefreiheit und staatlichen Sicherheitsinteressen vorzunehmen[210]. Zwar lässt der Regierungsentwurf das Bemühen um dem Verhältnismäßigkeitsgrundsatz entsprechende Regelungen erkennen. Allerdings greift er hinsichtlich der verfahrensrechtlichen Sicherung der vertraulichen Pressekommunikation zu kurz, da er weder die Grundrechtswidrigkeit des richtlinienbedingten Speicherbefehls noch die verstärkte Gefährdung der Pressefreiheit hinreichend berücksichtigt. Diese gefährdungserhöhenden Umstände lassen

---

208 BT-Dr 16/545, S. 3.

209 Entscheidung vom 12.03.2003 - 1 BvR 330/96 und 1 BvR 348/99, NJW 2003, 1787 sowie zuletzt Cicero-Urteil vom 27.02.2007 - 1 BvR 538/06, 1 BvR 2045/06.

210 Vgl. Birkner/Rösler, ZRP 2006, 110; ferner Kugelmann, ZRP 2005, 261.

den in dem Regierungsentwurf vorgesehenen Schutz der Presse als unzureichend erscheinen.

Das Zeugnisverweigerungsrecht der Medienmitarbeiter ist zwar in § 53 Abs. 1 S. 1 Nr. 5 StPO nicht absolut, aber immerhin - insbesondere hinsichtlich des Schutzes der Informanten der Medien - weitreichend gewährleistet[211]. Selbst dieser Schutz wird aber durch § 53b Abs. 2 S. 1 StPO-E relativiert. Hiernach ist das primär öffentliche Interesse an einer wirksamen Strafrechtspflege mit dem öffentlichen Interesse an den durch die zeugnisverweigerungsberechtigten Personen wahrgenommenen Aufgaben und dem individuellen Interesse an der Geheimhaltung der einem Berufsgeheimnisträger anvertrauten oder bekannt gewordenen Tatsachen abzuwägen. Somit würde Richtern und Staatsanwälten die Aufgabe zugewiesen, über die Gewichtung dieser Werte zu entscheiden. Dies birgt die Gefahr, dass im Rahmen der Einzelfallabwägung ein Werturteil über seriöse und unseriöse Medien oder über politische und unterhaltende Beiträge getroffen oder sonst zwischen Medien und ihren Nachrichten und Beiträgen differenziert wird. Ein solches staatliches Urteil liefe aber der Freiheit der Medien zuwider. Entsprechend hat das Bundesverfassungsgericht in der Cicero-Entscheidung darauf hingewiesen, dass die Staatsanwaltschaften es nicht uneingeschränkt in der Hand haben sollen, den besonderen grundrechtlichen Schutz der Medienangehörigen zum Wegfall zu bringen. Nach der Entscheidung ist es ferner unzulässig, wenn auf die Kommunikationsdaten von Pressevertretern ausschließlich oder vorwiegend zu dem Zweck zugegriffen wird, die Person des Informanten zu ermitteln.

Nach alledem sollten Pressemitarbeiter in den Schutz des § 53b

[211] Nach in der Literatur vertretener Ansicht führt eine verfassungskonforme Auslegung des § 53 Abs. 1 S. 2 StPO zu einem besonderen Schutz der kommunikativen Freiheit von Journalisten gegen Informationseingriffe (so Kugelmann, NJW 2003, 1777, 1779).

Abs. 1 StPO-E einbezogen werden[212]. Schließlich können nur durch einen eindeutigen gesetzlichen Schutz im Ergebnis immer nur relative[213] Einzelentscheidungen vermieden werden. Auch das ist durch die Cicero-Entscheidung[214] des Bundesverfassungsgerichts nochmals deutlich geworden.

Insgesamt besteht die Gefahr, dass der im Bereich von Durchsuchung, Beschlagnahme und Zeugnisverweigerung für Journalisten geltende und durch die Cicero-Entscheidung gestärkte gesetzliche Quellenschutz bei der Überwachung der elektronischen Kommunikation wieder ausgehebelt würde. § 53b StPO-E sollte daher jedenfalls klarstellen, dass der Informantenschutz auch im Falle elektronischer Journalistenkommunikation nicht schon mit - praktisch immer leicht darzustellenden - Verhältnismäßigkeitserwägungen beseitigt werden kann. Auch hier darf ein staatlicher Zugriff nur im Fall eines hinreichenden Verdachts strafbarer Beteiligung des Journalisten möglich sein.

---

212 Ebenso: Entschließung der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder (8.-9. März 2007) zur Vorratsdatenspeicherung (vgl. Fn. 5). Einen ähnlichen Ansatz verfolgten auch zwei Gesetzentwürfe zum Schutz von Pressevertretern, die bereits vor der Versendung des Referentenentwurfs des Bundesjustizministeriums vorgelegt worden waren. In weiten Teilen zielten die Gesetzentwürfe von Bündnis 90/Die Grünen (BT-Dr 16/576) und der FDP (BT-Dr 16/956) in die gleiche Richtung. Insbesondere haben sich beide Fraktionen für eine Einbeziehung von Journalisten in den Schutzbereich des § 100h Abs. 2 S. 1 StPO ausgesprochen. Auch danach wäre das Verlangen einer Auskunft über Telekommunikationsverbindungen, die von oder zu einem Journalisten hergestellt wurden, zukünftig unzulässig bzw. die entsprechenden Informationen wären unverwertbar gewesen. Zum Erfordernis einer entsprechenden Gesetzesänderung vgl. auch Birkner/Rösler, ZRP 2006, 109, 111. Die Einbeziehung aller nach § 53 Abs. 1 StPO zeugnisverweigerungsberechtigten Personen in den Schutz des § 100 h Abs. 2 StPO hat zuletzt die Fraktion Bündnis 90/Die Grünen im Rahmen eines Gesetzentwurfs zur Reform der Telekommunikationsüberwachung gefordert (BT-Dr 16/3827, S. 9 und 21).

213 Beschluss des Bundesverfassungsgerichts vom 04.07.2006 - 2 BvR 950/05, RDV 2006, 206.

214 Oben Fn. 209.

5. Vorschläge an den Gesetzgeber

5.1. Richtlinienumsetzung im TKG

5.1.1. § 3 Nr. 30 TKG: Konkretisierung des Begriffs „Verkehrsdaten“

Die Vorschrift sollte wie folgt gefasst werden:

„Verkehrsdaten“ Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden, ***einschließlich der Bestandsdaten der Teilnehmer eines konkreten Telekommunikationsvorgangs****.*

Hilfsweise sollte zumindest in der Gesetzesbegründung (ggf. zu § 113 TKG) eine Klarstellung erfolgen, dass auch die Zusammenführung einer den einschlägigen Behörden bekannten dynamischen IP-Adresse mit bei den Providern befindlichen Bestandsdaten grundsätzlich nicht ohne eine ordnungsgemäße richterliche Anordnung nach § 100g i.V.m. §§ 100a, 100b StPO-E erfolgen darf.

5.1.2. § 3 Nr. 30a TKG: Einfügung einer Legaldefinition „Vorratsdaten“

Es sollte eine Begriffsdefinition „Vorratsdaten“ mit folgendem Wortlaut eingefügt werden:

„Vorratsdaten“ Verkehrsdaten, die für den Aufbau weiterer Verbindungen oder für die in den §§ 97, 99, 100 und 101 genannten Zwecke nicht erforderlich sind, und nach § 113a TKG vom Diensteanbieter gespeichert werden müssen.

5.1.3. § 113a Abs. 1 S. 1 TKG-E: Konkretisierung der Speicherzwecke

§ 113a Abs. 1 S. 1 TKG-E sollte wie folgt gefasst werden:

Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ist verpflichtet, von ihm bei der Nutzung seines Dienstes erzeugte oder verarbeitete Verkehrsdaten ***zum Zwecke der Verfolgung von Straftaten nach § 139 Abs. 3 StGB*** *nach Maßgabe der Absätze 2 –5 sechs Monate im Inland oder in einem anderen Mitgliedstaat der Europäischen Union zu speichern.*

5.1.4. § 113a Abs. 11 TKG-E: Pflicht zur unverzüglichen Löschung nach Fristablauf

Die Vorschrift sollte wie folgt gefasst werden:

Der nach § 113a Verpflichtete hat die allein auf Grund dieser Vorschrift gespeicherten Daten ***unverzüglich*** *nach Ablauf der in § 113a Abs. 1 genannten Frist zu löschen oder die Löschung sicherzustellen.*

5.1.5. § 113b Nr. 1, 2 und 3 TKG-E: Begrenzung der Verwendungszwecke auf schwere Straftaten

Nr. 1 sollte wie folgt lauten:

zur Verfolgung von ***Straftaten nach § 139 Abs. 3 StGB.***

Die Regelungen in Ziffer 2 und 3 sollten **ersatzlos gestrichen** werden.

5.2. Richtlinienumsetzung in der StPO

5.2.1. § 53b Abs. 1 S. 1 StPO-E: Einbeziehung von Medienmitarbeitern

Die Vorschrift sollte wie folgt gefasst werden:

Eine Ermittlungsmaßnahme, die sich gegen eine in § 53 Abs. 1 Satz 1 Nr. 1, 2, 4 ***oder Nr. 5*** *genannte Person richtet und voraussichtlich Erkenntnisse erbringen würde, über die diese Person das Zeugnis verweigern dürfte, ist unzulässig.*

5.2.2. § 100g Abs. 2 StPO-E: Einfügung eines eigenständigen Tatbestandes für die Erhebung von Vorratsdaten

In § 100g StPO-E sollte ein neuer Absatz 2 mit folgendem Wortlaut eingefügt werden:

Die Erhebung von Vorratsdaten (§ 3 Nr. 30a TKG) ist nur zulässig, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand eine schwere Straftat nach § 139 Abs. 3 StGB begangen hat.

Die Nummerierung der nachfolgenden Absätze ändert sich entsprechend.

5.3. Befristung

Mit Blick auf die eventuelle Europarechtswidrigkeit der Richtlinie 2006/24/EG und vor dem Hintergrund einer - wünschenswerten - weitergehenden Evaluation der Speicherungs-, Verwendungs- und Zugriffsvorschriften durch eine unabhängige Stelle sollten die entsprechenden gesetzlichen Regelungen angemessen befristet werden.

Literaturverzeichnis

Alvaro, Alexander	Positionspapier zur Einführung einer Vorratsspeicherung von Daten, in: RDV 2005, S. 47 ff., zit.: Alvaro, RDV 2005
Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder in Deutschland	Ablehnung der Vorratsdatenspeicherung, Stellungnahme zur Anhörung der Europäischen Kommission, Public consultation on traffic data retention, in: DuD 2004, S. 603 ff., zit.: Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder in Deutschland, DuD 2004
Arbeitskreis Vorratsdatenspeicherung	Gemeinsame Stellungnahme des Arbeitskreises Vorratsdatenspeicherung, des Netzwerkes Neue Medien und der Neuen Richtervereinigung zum Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (http://www.vorratsdatenspeicherung.de/images/stellungnahme_vorratsdatenspeicherung.pdf)
ARD u.a.	Gemeinsame Stellungnahme zum Referenten-Entwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ von ARD, BDZV, DJV, Deutscher Presserat, VDZ, Ver.di, VPRT und ZDF vom 19.01.2007, Aktenzeichen: RB 3-4104/11-R5 884//2006

(http://www.presserat.de/fileadmin/download/Stellungnahme_Telekommunikationsueberwachung.pdf)

Artikel-29-Datenschutzgruppe — Stellungnahme zur Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, angenommen am 25.03.2006, 654/06/DE, WP 119

BDI — Position des Bundesverbandes der Deutschen Industrie (BDI) zum Entwurf eines Rahmenbeschlusses der Europäischen Union über die Vorratsspeicherung (Ratsdokument 8958/04) vom 07.07.2004, in: DuD 2004, S. 606 ff., zit.: BDI, DuD 2004

Birkner, Stefan/Rösler, Philipp — Pressefreiheit stärken - Strafprozessordnung ändern, in: ZRP 2006, S. 109 ff., zit.: Birkner/Rösler, ZRP 2006

BITKOM — Stellungnahme des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) vom 22.05.2007 zum Regierungsentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (Kabinettsbeschluss vom 18. April 2007, BR-Drs. 275/07)
(http://www.bitkom.org/files/documents

	/Stellungnahme_BITKOM_RegE_Neuregelung_TKUe_22_05_07.pdf)
Breyer, Patrick	Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin 2005, zit.: Breyer
Büllingen, Franz	Vorratsspeicherung von Telekommunikationsdaten im internationalen Vergleich, in: DuD 2005, S. 349 ff., zit.: Büllingen, DuD 2005
Büttgen, Peter	Neuer Datenschutz für neue Medien?, in: RDV 2006, S. 213 ff., zit.: Büttgen, RDV 2003
Bundesbeauftragter für den Datenschutz	Zehn Thesen für eine datenschutzfreundliche Informationstechnik vom 18.12.2006
Bundesrat	Entwurf eines Gesetzes zur Änderung telekommunikationsrechtlicher Vorschriften vom 04.02.2005, BR-Dr 92/05
Bundesrat	Stellungnahme zum Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 08.06.2007, BR-Dr 275/07 (Beschluss)
Bundesregierung	Entwurf eines Gesetzes zur Verlängerung der Geltungsdauer der §§ 100g, 100h StPO vom 16.06.2004, BT-Dr 15/3349
Bundesregierung	Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung

der Richtlinie 2006/24/EG, BR-Dr 275/07

Deutscher Bundestag — „Speicherung mit Augenmaß - Effektive Strafverfolgung und Grundrechtswahrung“: Beschlussempfehlung vom 07.02.2006, BT-Dr 16/545 (auch abgedruckt in RDV 2006, 86 ff.). Zur Annahme der Empfehlung vgl. Plenarprotokoll 16/19 vom 16.02.2006, S. 1430 (B).

Deutscher Bundestag — Richtlinie zur Vorratsdatenspeicherung durch den Europäischen Gerichtshof prüfen lassen, Antrag vom 26.05.2006, BT-Dr 16/1622

Europäischer Datenschutzbeauftragter — Stellungnahme zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (KOM(2005) 438 endg.), Amtsblatt der Europäischen Union, C 298/1

Europäisches Parlament — Bericht über die Initiative der Französischen Republik, Irlands, des Königreichs Schweden und des Vereinigten Königreichs für einen Rahmenbeschluss des Rates über die Vorratsspeicherung von Daten etc. vom 31.05.2005, Ausschuss des Europäischen Parlaments für Bürgerliche Freiheiten, Justiz und Inneres, A6-0174/2005

Europäisches Parlament — Legislative Entschließung zu dem Vorschlag für eine Richtlinie des Europäi-

	schen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (KOM(2005) 0438 - C6-0293/2005 - 2005/0182 (COD)), P6_TA(2005)0512
Fraktion Bündnis 90/ Die Grünen	Freiheit des Telefonverkehrs vor Zwangsspeicherungen, Antrag vom 14.12.2005, BT-Dr 16/237
Fraktion Bündnis 90/ Die Grünen	Entwurf eines Gesetzes zum Schutz von Journalisten und der Pressefreiheit in Straf- und Strafprozessrecht vom 07.02.2006, BT-Dr 16/576
Fraktion Bündnis 90/ Die Grünen	Entwurf eines Gesetzes zur Reform der Telekommunikationsüberwachung vom 13.12.2006, BT-Dr 16/3827
Fraktion der FDP	Gegen eine europaweit verpflichtende Vorratsdatenspeicherung, Antrag vom 01.12.2005, BT-Dr 16/128
Fraktion der FDP	Entwurf eines Gesetzes zur Sicherung der Pressefreiheit vom 15.03.2006, BT-Dr 16/956
Germann, Michael	Gefahrenabwehr und Strafverfolgung im Internet, 1. Auflage, Berlin 2000, zit.: Germann
Gnirck, Karen/ Lichtenberg, Jan	Internetprovider im Spannungsfeld staatlicher Auskunftsersuchen, in: DuD 2004, S. 598 ff., zit.: Gnirck/ Lichtenberg, DuD 2004
Gola, Peter/ Klug, Christoph	Grundzüge des Datenschutzrechts, München 2003, zit.: Gola/Klug

Gola, Peter/ Klug, Christoph	Die Entwicklungen des Datenschutzrechts in den Jahren 2005/2006, in: NJW 2006, S. 2454 ff., zit.: Gola/Klug, NJW 2006
Gola, Peter/ Schomerus, Rudolf	Bundesdatenschutzgesetz, 8. Auflage, München 2005, zit.: Gola/Schomerus
Ipsen, Jörn	Staatsrecht II, Grundrechte, 9. Auflage, Neuwied 2006, zit.: Ipsen
Jarass, Hans/ Pieroth, Bodo	Grundgesetz für die Bundesrepublik Deutschland, 8. Auflage, München 2006, zit.: Jarass/Pieroth
Köbele, Bernd	Anspruch auf Mitteilung des Anschlussinhabers bei bekannter IP-Adresse, in: DuD 2004, S. 609 ff., zit.: Köbele, DuD 2004
Köcher, Jan K./ Kaufmann, Noogie C.	Speicherung von Verkehrsdaten bei Internet-Access-Providern, Anmerkung zum Urteil des LG Darmstadt vom 07.12.2005 - 25 S 118/2005, in: DuD 2006, S. 360 ff., zit.: Köcher/Kaufmann, DuD 2006
Koenig, Christian/ Neumann, Andreas/ Senger, Marion	Gesetzliche Ausgestaltung des regulierungsbehördlichen Ermessens im Telekommunikationsrecht, in: MMR 2006, S. 365 ff., zit.: Koenig/Neumann/Senger
Königshofen, Thomas/ Ulmer, Claus D.	Datenschutz-Handbuch in der Telekommunikation, Frechen 2006, zit.: Königshofen/Ulmer
Konferenz der Datenschutzbeauftragten des Bundes und der Länder	Entschließung der 73. Konferenz (8.-9. März 2007) zur Vorratsdatenspeicherung (http://www.datenschutz. thueringen.de/veroeffentlichungen/entschliessungen/konferenz_73/Vorratsdatenspeicherung 73.htm)

Kühling, Jürgen	Freiheitsverluste im Austausch gegen Sicherheitshoffnungen im künftigen Telekommunikationsgesetz?, in: K&R 2004, S. 105 ff.; zit.: Kühling, K&R 2004
Kugelmann, Dieter	Die Vertraulichkeit journalistischer Kommunikation und das BVerfG, zugleich Besprechung von BVerfG, Urteil vom 12.03.2003 - 1 BvR 330/96, 1 BvR 348/99 -, in: NJW 2003, S. 1777 ff., zit.: Kugelmann, NJW 2003
Kugelmann, Dieter	Pressefreiheit ohne Informantenschutz?, in: ZRP 2005, S. 260 ff., zit.: Kugelmann, ZRP 2005
Leutheusser-Schnarrenberger, Sabine	Vorratsdatenspeicherung - Ein vorprogrammierter Verfassungskonflikt, in: ZRP 2007, S. 9 ff., zit.: Leutheusser-Schnarrenberger, ZRP 2007
Limbach, Jutta	Ist die kollektive Sicherheit Feind der individuellen Freiheit?, 10.05.2002 http://www.zeit.de/reden/deutsche_innenpolitik/200221_limbach_sicherheit
Max-Planck-Institut	Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen http://www.bmj.bund.de/files/-/134/Abschlussbericht.pdf
Münch, Ingo von/ Kunig, Philip (Hrsg.)	Grundgesetz-Kommentar, Band I, 5. Auflage, München 2000, zit.: MüKu/Bearbeiter
Pieroth, Bodo/ Schlink, Bernhard	Grundrechte, Staatsrecht II, 21. Auflage, Heidelberg 2005, zit.: Pieroth/ Schlink

Roßnagel, Alexander	Datenschutz in einem informatisierten Alltag, Gutachten im Auftrag der Friedrich-Ebert-Stiftung, Berlin 2007, zit.: Roßnagel, Datenschutz in einem informatisierten Alltag
Roßnagel, Alexander (Hrsg.)	Handbuch Datenschutzrecht, München 2003, zit.: Roßnagel/Bearbeiter
Roßnagel, Alexander/ Pfitzmann, Andreas/ Garstka, Hans-Jürgen	Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern 2001, zit.: Roßnagel/Pfitzmann/Garstka
Sachs (Hrsg.)	Grundgesetz, 3. Auflage, München 2003, zit.: Sachs/Bearbeiter
Sankol, Barry	Die Qual der Wahl: § 113 TKG oder §§ 100g, 100h StPO?, in: MMR 2006, S. 361 ff., zit.: Sankol, MMR 2006
Sievers, Malte	Der Schutz der Kommunikation im Internet durch Artikel 10 des Grundgesetzes, Baden-Baden 2003, zit.: Sievers
Simitis, Spiros (Hrsg.)	Bundesdatenschutzgesetz, 6. Auflage, Baden-Baden 2006, zit.: Simitis/Bearbeiter
Simitis, Spiros	Hat der Datenschutz noch eine Zukunft?, in: RDV 2007, S. 143 ff., zit.: Simitis, RDV 2007
Spindler, Gerald/ Dorschel, Joachim	Auskunftsansprüche gegen Internet-Service-Provider, Zivilrechtliche Grundlagen und datenschutzrechtliche Grenzen, in: CR 2005, S. 38 ff., zit.: Spindler/Dorschel, CR 2005
Stern, Klaus	Das Staatsrecht der Bundesrepublik Deutschland, Band III/2: Allgemeine Lehren der Grundrechte, München 1994, zit.: Stern

Streinz, Rudolf	Europarecht, 7. Auflage, Heidelberg 2005, zit.: Streinz
Tinnefeld, M-T/ Ehmann, E./ Gerling, R. W.	Einführung in das Datenschutzrecht, 4. Auflage, München 2005, zit.: Tinnefeld/Ehmann/Gerling
Uhe, Bianca/ Herrmann, Jens	Überwachung im Internet - Speicherung von personenbezogenen Daten auf Vorrat durch Internet Service Provider, Diplomarbeit, 18.08.2003, zit.: Uhe/ Herrmann
	http://ig.cs.tu-berlin.de/oldstatic/da/ 2003-08/UheHerrmann-Diplomarbeit-082003.pdf
ULD	Stellungnahme des Unabhängigen Landeszentrums für den Datenschutz Schleswig-Holstein (ULD) vom 27.06.2007 zum Gesetzesentwurf der Bundesregierung für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, BR-Drucksache 275/07
	https://www.datenschutzzentrum.de/polizei/20070627-vorratsdatenspeicherung.pdf
ULD	27. Tätigkeitsbericht (2005) des Unabhängigen Landeszentrums für den Datenschutz Schleswig-Holstein (ULD), 4.2.3 Bekämpfung der Internetkriminalität - „quick freeze“, S. 29 f.
Ulmer, Claus D./ Schrief, Dorothee	Vorratsdatenspeicherung durch die Hintertür, in: DuD 2004, S. 591 ff., zit.: Ulmer/Schrief, DuD 2004

Vassilaki, Irini	EU-Richtlinie zur Vorratsdatenspeicherung: Aufklärung von Straftaten oder Aushöhlung von Grundrechten?, in: MMR 2/2006, S. XIII, zit.: Vassilaki, MMR 2/2006
VATM	Stellungnahme des Verbandes der Anbieter von Telekommunikations- und Mehrwertdiensten (VATM) e.V. zum Referentenentwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ vom 19.01.2007 (http://www.vatm.de/content/stellungnahmen/inhalt/19-01-2007.pdf)
Weichert, Thilo	Technik, Terror, Transparenz - Stimmen Orwells Visionen?, in: Sonderbeilage zur RDV 1/2005, S. 6 ff., zit.: Weichert, Sonderbeilage zur RDV 1/2005
Wissenschaftliche Dienste des BT	Zulässigkeit der Vorratsdatenspeicherung nach europäischem und deutschem Recht, WD 3 - 282/06 - korrigiert http://www.bundestag.de/bic/analysen/2006/zulaessigkeit_der_vorratsdatenspeicherung_nach_europaeischem_und_deutschem_recht.pdf
Wüstenberg, Dirk	Argumente gegen die Rechtmäßigkeit einer Vorratsdatenspeicherung, in: RDV 2006, S. 102 ff., zit.: Wüstenberg, RDV 2006