



Vorratsdatenspeicherung aus rechtlicher Perspektive

Zusammenfassung

Am 9. November 2007 haben die Bundestagsfraktionen von CDU/CSU und SPD das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ gegen die Stimmen der Oppositionsparteien und ungeachtet massiver öffentlicher Proteste beschlossen. Nachdem wenig später der Bundesrat und der Bundespräsident das Gesetz ebenfalls billigten, wurde es am 31. Dezember 2007 im Bundesgesetzblatt¹ veröffentlicht und in seinen wesentlichen Teilen zum 1. Januar 2008 in Kraft gesetzt. Das Artikelgesetz besteht im wesentlichen aus zwei Teilen. Erstens wird mit ihm die EU-Richtlinie 2006/24/EG zur Vorratsdatenspeicherung in deutsches Recht umgesetzt. Zweitens novelliert das Gesetz besonders die auf verdeckte polizeiliche Ermittlungsmaßnahmen bezogenen Regelungen der Strafprozessordnung (StPO) und passt diese an die in jüngeren Bundesverfassungsgerichtsentscheidungen enthaltenen Vorgaben an.

In Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung bestimmen nun die §§ 113a und 113b des Telekommunikationsgesetzes (TKG), dass jeder, der öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, die bei ihm betriebsbedingt erzeugten oder verarbeiteten Telekommunikations-Verkehrsdaten sechs Monate lang speichern und den Sicherheitsbehörden auf Verlangen übermitteln muss.

Die sechsmonatige Speicherpflicht umfasst alle nur denkbaren Daten der Festnetz- und Mobilfunktelefonie sowie des Telefon- und E-Mail-Verkehrs über das Internet. Dazu gehören u. a. die Rufnummern, sonstige Kennungen, Internet-Protokolladressen und die Kennungen des E-Mail Postfachs aller Kommunikationsteilnehmer, das Datum, die Uhrzeit und die Dauer der Kommunikation sowie, im Falle der Mobilfunk-

telefonie, die Standortdaten des anrufenden und angerufenen Mobiltelefons. Selbst die Daten verborgener Anrufversuche sind zu speichern. Mit diesem Datenkatalog geht das Umsetzungsgesetz erheblich über die Vorgaben der EU-Richtlinie zur Vorratsdatenspeicherung hinaus.

Berechnungen der Fachverbände ergeben, dass allein zur Erfassung der über das Internet abgewickelten Kommunikation ein Datenvolumen von 2.700 Terabyte² ständig vorgehalten werden muss. Finanzielle Ausgleichszahlungen an die zur Datenspeicherung verpflichteten Kommunikationsunternehmen sind nicht vorgesehen, so dass diese ihre auf dreistellige Millionenbeträge geschätzten Investitions- und Betriebskosten auf die Endnutzer abzuwälzen gezwungen sein werden.

Gang der europäischen Gesetzgebung

Auf europäischer Ebene gehen die Pläne zur Vorratsdatenspeicherung auf die Schlussfolgerungen des Rates für Justiz und Inneres vom 20. September 2001 zurück. Nach den Terroranschlägen des 11. Septembers 2001 hat dieser zur Erarbeitung eines Vorschlages aufgefordert, der die Sicherheitsbehörden befähigen soll, unter Nutzung der elektronischen Telekommunikation begangene Straftaten besser aufzuklären und zu verfolgen. Er werde jedoch darauf achten, so der Rat, dass die Balance zwischen dem Schutz persönlicher Daten und den Bedürfnissen der Strafverfolgungsbehörden, auf solche Daten zugreifen zu können, gewahrt bleibe.³

Von einer Speicherung von Telekommunikationsdaten „auf Vorrat“ ist auf Ratsebene erstmals in der vom Rat am 25. März 2004 angenommenen Erklärung zum Kampf gegen den Terrorismus die Rede. In dieser Erklärung, die eine Reaktion auf die Terroranschläge von Madrid war, beauftragt der Rat den Rat der EU, Vorschläge für Rechtsvorschriften zu beraten, die die Aufbewahrung

Die beschlossene Vorratsdatenspeicherung geht erheblich über die Vorgaben der EU-Richtlinie hinaus.



von Verkehrsdaten durch die Anbieter von Telekommunikationsdiensten regeln.⁴

Daraufhin sahen sich Frankreich, Großbritannien, Irland und Schweden veranlasst, dem Rat am 28. April 2004 den Entwurf eines auf die Artikel 31 Abs. 1 Buchstabe b und Artikel 34 Abs. 2 Buchstabe b des Vertrages über die Europäische Union (EUV) gestützten Rahmenbeschlusses über die Vorratsdatenspeicherung von Telekommunikationsdaten vorzulegen⁵ und den Mitgliedstaaten sowie dem Europäischen Parlament zur Stellungnahme zuzuleiten. Der Rahmenbeschlussentwurf sah vor, für Telekommunikationsdaten Speicherfristen von mindestens einem Jahr und höchstens drei Jahren vorzuschreiben. Ratsinterne Meinungsverschiedenheiten, öffentliche Kritik und die ablehnende Haltung des Europäischen Parlaments haben die damalige niederländische Ratspräsidentschaft Ende 2004 veranlasst, den Rahmenbeschlussentwurf im Rat nicht weiter zu beraten.⁶ In den Schlussfolgerungen der Ratspräsidentschaft vom 15. Juli 2005 wird aber betont, dass dem Rechtsetzungsverfahren zur Verstärkung der polizeilichen und justiziellen Zusammenarbeit der Mitgliedstaaten, besonders hinsichtlich der Speicherung von Telekommunikationsdaten, höchste Priorität eingeräumt bleibe.⁷ Die Beratungen im Rat zu dem aus seiner Mitte eingebrachten Rahmenbeschlussvorschlag wurden nicht wieder aufgenommen.

Anstelle des Rahmenbeschlussentwurfs legte die Europäische Kommission am 21. September 2005 den Vorschlag für eine auf Artikel 95 EGV gestützte Richtlinie über die Vorratsspeicherung vor.⁸ In ihm waren für die bei der Internetnutzung anfallenden Daten sechsmonatige und für alle anderen Daten einjährige Speicherfristen vorgesehen.⁹ Nach der mehrheitlichen Zustimmung des Europäischen Parlaments am 14. November 2005 wurde die Richtlinie im Rat gegen die Stimmen der Slowakei und Dänemarks angenommen und am 15. März 2006 in Kraft gesetzt.¹⁰ Abweichend vom Kommissionsvorschlag sind in der vom Rat letztlich verabschiedeten Richtlinienfas-

sung für alle Kommunikationsdaten Speicherfristen von mindestens sechs Monaten und höchstens zwei Jahren vorgeschrieben.¹¹

Gang der deutschen Gesetzgebung

Die Versuche, den Anbietern von Telekommunikationsdiensten eine über das betrieblich notwendige Maß hinausgehende Speicherpflicht für Telekommunikationsdaten vorzuschreiben, gehen auf Initiativen des Bundesrats aus dem Jahre 2002 zurück. Im Zuge der Beratungen zur Änderung des Telekommunikationsgesetzes (TKG) und des Teledienstedatenschutzgesetzes (TDDSG) sowie zur Änderung der Strafprozessordnung, um Ermittlungsmaßnahmen wegen des Verdachts

Sollte das beim EuGH anhängige Verfahren zu Gunsten Irlands entschieden werden, dann wäre die europarechtliche Vorgabe entfallen, die von der Bundesregierung zur Einführung der Vorratsdatenspeicherung verwendet wurde.

sexuellen Missbrauchs von Kindern zu verbessern, verlangte der Bundesrat damals, die Anbieter öffentlicher Telekommunikationsdienste zu verpflichten, die bei ihnen anfallenden Telekommunikationsdaten über den betrieblich bedingten Zeitraum hinaus „auf Vorrat“ zu speichern und zur Übermittlung an die Sicherheitsbehörden bereit zu halten.¹² Die zur Einführung dieser Regelung vom Bundes-

rat vorgeschlagenen Änderungen des TKG und des TDDSG wurden von der Bundesregierung jedoch mit dem Hinweis auf entgegenstehende grundgesetzliche Erwägungen abgelehnt.¹³

Im Zuge der 2003 wieder aufgenommenen Beratungen zur Änderung des TKG beschloss der Bundesrat im Dezember 2003, seinen Vorschlag vom Juli 2002 zu erneuern. Aber auch er wurde von der Bundesregierung abgelehnt.¹⁴ Stattdessen wurde die Novellierung des TKG ohne die vom Bundesrat angestrebte Vorratsdatenspeicherung durch ein im Mai 2004 im Vermittlungsausschuss erzieltetes Ergebnis abgeschlossen und die TKG-Novelle im Juni 2004 in Kraft gesetzt.

Trotz dieser Einigung im Vermittlungsausschuss sah sich der Bundesrat in seiner Sitzung am 13. September 2004 veranlasst, den inzwischen von der Kommission der Europäischen Union vorgelegten Entwurf eines Rahmenbeschlusses über die Vorratsdatenspeicherung ausdrücklich zu begrüßen.¹⁵ Anders der Bundestag: Anlässlich



der Vorlage des Jahresberichts des Bundesdatenschutzbeauftragten bekräftigt er im Dezember 2004 seine grundsätzlich ablehnende Haltung.¹⁶ Einen Monat später, am 26. Januar 2005, fasste er im Rahmen der Debatte über den Entwurf des EU-Rahmenbeschlusses auf Empfehlung des Wirtschafts- und Rechtsausschusses einen Beschluss, in dem an die ablehnende Haltung des Deutschen Bundestages erinnert und die Bundesregierung aufgefordert wurde, die ablehnende Position auf europäischer Ebene zu vertreten.¹⁷

Wie schon zuvor der Rahmenbeschlussentwurf wurde auch der am 21. November 2005 von der Europäischen Kommission vorgelegte Vorschlag für eine Richtlinie zur Vorratsdatenspeicherung vom Bundesrat ausdrücklich begrüßt.¹⁸ Jedoch meldet dieser Zweifel an, ob die nunmehr gewählte gemeinschaftsrechtliche Verankerung des Vorhabens unter EU-vertragsrechtlichen Gesichtspunkten gerechtfertigt werden kann.

Nachdem die Bundesregierung den Bundestag darüber informiert hatte, dass es in den Verhandlungen des Rats gelungen sei, die im Kommissionsentwurf vorgesehene Mindestspeicherfrist von einem auf ein halbes Jahr zu verkürzen, beschloss der Deutsche Bundestag dann jedoch am 7. Februar 2006 gegen die Stimmen der Oppositionsparteien, die Bundesregierung aufzufordern, der Richtlinie in der geänderten Form zuzustimmen.¹⁹ Die Richtlinie 2006/24/EG wurde am 15. März 2006 vom Europäischen Parlament und bei Zustimmung der Bundesregierung vom Rat der EU erlassen.

Die Vorratsdatenspeicherung im Lichte des europäischen Vertragsrechts

Ein Anlass zur kritischen Würdigung des europarechtlichen Vorhabens ergibt sich daraus, dass die Frage, ob die Vorratsdatenspeicherung vertragskonform im Gemeinschaftsrecht (1. Säule, Art. 95 EGV) oder im Unionsrecht (3. Säule, Art 34 EUV) geregelt werden muss, strittig und wegen einer diesbezüglich anhängigen Klage der Republik Irland²⁰ beim Europäischen Gerichtshof (EuGH) offen ist.

Die damals vorgebrachten schwerwiegenden verfassungsrechtlichen Argumente gegen die Vorratsdatenspeicherung haben ihre Gültigkeit nicht verloren.

Dazu vertreten die Kommission und das Europäische Parlament die Ansicht, dass die Kommunikationsdaten von den Diensteanbietern im Rahmen einer in den Gemeinschaftsbereich fallenden Tätigkeit erhoben und gespeichert werden. Daraus folge, dass gesetzgeberische Maßnahmen, die der Angleichung der diesbezüglich in den Mitgliedstaaten geltenden Rechts- und Verwaltungsvorschriften dienen, zur Gewährleistung des freien Datenverkehrs geboten sind und diese dann ebenso im Gemeinschaftsrecht gemäß Artikel 95 EGV ihre Ermächtigungsgrundlage finden.²¹

In dieser Rechtsauffassung sehen sich die Kommission und das Europäische Parlament vom Urteil des EuGH vom 13. September 2005 bestätigt, das dem Kommissionsantrag entsprochen hatte, den Rahmenbeschluss des Rates 2003/80/JI vom 27. Januar 2003 über die Angleichung strafrechtlicher Normen der Mitgliedstaaten zum Schutze der Umwelt wegen der rechtswidrig dem Unionsvertrag entnommenen Ermächtigungsgrundlage nach Artikel 34 EUV für nichtig zu erklären. In diesem Urteil hatte der EuGH ausgeführt, dass das Straf- und Strafprozessrecht grundsätzlich zwar nicht in die Zuständigkeit der Gemeinschaft falle, dies „den Gemeinschaftsgesetzgeber jedoch nicht daran hindere, Maßnahmen in Bezug auf das Strafrecht zu ergreifen, um die volle Wirksamkeit der von ihm zum Schutze der Umwelt erlassenen Rechtsnormen zu gewährleisten.“²²

Der Rechtsmeinung der Kommission und des Europäischen Parlaments steht jedoch das am 30. Mai 2006 ergangene Urteil des EuGH zur Rechtmäßigkeit des mit den USA vom Gemeinschaftsgesetzgeber geschlossenen Abkommens über die Erhebung und Weitergabe von Fluggastdaten entgegen.²³ Dort betont der Gerichtshof, dass die Übermittlung von Fluggastpassagierdaten an USA-Behörden eine Datenverarbeitung darstelle, die die öffentliche Sicherheit und die Tätigkeiten des Staates im strafrechtlichen Bereich betreffe. Zwar treffe es zu, dass die Daten von den Fluggesellschaften ursprünglich im Rahmen einer unter das Gemeinschaftsrecht fallenden Tätigkeit,



dem Verkauf von Flugtickets, erhoben werden. Die Weitergabe dieser Daten an USA-Behörden sei jedoch zur Erbringung dieser Dienstleistung nicht erforderlich. Sie diene allein dem Schutz der öffentlichen Sicherheit und der Strafverfolgung. Daraus folge, dass das Gemeinschaftsrecht, also der Artikel 95 EGV, die Vereinbarung mit den USA nicht begründen könne und folglich das auf Artikel 95 EGV gegründete Abkommen mit den USA vertragsrechtswidrig und nichtig sei.

Dieses wie auch das Umweltschutzurteil legt entgegen der Rechtsauffassung der Kommission und des Europäischen Parlaments die Interpretation nahe, dass der EuGH seine Entscheidungen über die Zugehörigkeit eines Rechtsaktes zum Gemeinschafts- oder Unionsrecht strikt vom Hauptzweck der mit dem Rechtsakt legalisierten Maßnahme abhängig macht. Legt man diesen Maßstab an, wird also berücksichtigt, dass die auf einen Mindestzeitraum von sechs Monaten festgelegte Speicherung der Telekommunikationsdaten keinen betrieblichen Zwecken dient, sondern den behördlichen Zugriff zu Zwecken des Strafrechts sicherstellen soll, dann wird analog zur EuGH-Entscheidung zum Passagierdatenabkommen einsichtig, dass die EU-Regelung der Vorratsdatenspeicherung nicht, wie geschehen, im Gemeinschaftsrecht nach Art. 95 EGV als mit Mehrheit zu verabschiedende Richtlinie, sondern im Unionsrecht nach Artikel 34 EUV als einstimmig zu beschließender Rahmenbeschluss hätte verankert werden müssen.

Diese Rechtsmeinung wird nicht nur von der Republik Irland und den meisten Sachverständigen vertreten. Ausweislich der Beschlüsse vom 26. Januar 2005 und 7. Februar 2006 wurde sie auch vom Deutschen Bundestag und Bundesrat eingenommen. Dies hat die Bundesregierung jedoch nicht davon abgehalten, der auf Gemeinschaftsrecht gegründeten Richtlinie im Rat der EU zuzustimmen und die Oppositionsforderung abzulehnen, die Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung in deutsches Recht bis zur Irland-Entscheidung des EuGH auszusetzen. Sollte also das beim EuGH anhängige Verfahren der Republik Irland zu Gunsten der Klägerin

entscheiden, die EU-Richtlinie zur Vorratsdatenspeicherung also als Verstoß gegen europäisches Vertragsrecht gewertet werden, was wahrscheinlich ist, dann wäre die europarechtliche Vorgabe entfallen, die von der Bundesregierung unter Hinweis auf ihre Pflicht zur Umsetzung in nationales Recht als Druckmittel zur Einführung der Vorratsdatenspeicherung verwendet wurde.

Die Vorratsdatenspeicherung im Lichte des Grundgesetzes

Als die Bundesregierung 2002 den Versuch des Bundesrates, eine Speicherpflicht für Telekommunikationsdaten einzuführen, ablehnte, hat sie betont, dass „bei Überlegungen hinsichtlich der

Es konnte deshalb nicht verwundern, dass die Einführung der Vorratsdatenspeicherung auf breite öffentliche Ablehnung gestoßen ist.

Einführung von Mindestspeicherpflichten die tatsächlichen und rechtlichen Gegebenheiten, insbesondere das Fernmeldegeheimnis, das Grundrecht auf informationelle Selbstbestimmung, das Gebot der konkreten Bestimmung des Zwecks der

Datenverarbeitung, die Grundsätze der Verhältnismäßigkeit sowie der Datenvermeidung und -sparsamkeit und die Grundrechte und schutzwürdigen Interessen der Dienstanbieter einerseits und die Interessen der Sicherheitsbehörden andererseits abzuwägen seien“. Es ist nicht ersichtlich, in welcher Weise diese zu Recht benannten Abwägungserfordernisse in dem am 1. Januar 2008 in Kraft getretenen Gesetz zur Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung berücksichtigt worden wären. Die damals vorgebrachten schwerwiegenden verfassungsrechtlichen Argumente gegen die Vorratsdatenspeicherung einer Fülle personenbezogener Daten eines jeden Teilnehmers an der Telekommunikation haben ihre Gültigkeit nicht verloren.

Es konnte deshalb nicht verwundern, dass die Einführung der Vorratsdatenspeicherung auf breite öffentliche Ablehnung gestoßen ist, die in Deutschland in öffentlichen Protesten und in mehreren mittlerweile dem Bundesverfassungsgericht vorgelegten Verfassungsbeschwerden zum Ausdruck kommt. Darunter eine Beschwerde, an der auch die Verfasserin des vorliegenden Aufsatzes beteiligt ist und eine Verfassungsbeschwerde nebst Antrag auf Erlass einer einstweiligen Verfügung gegen die §§ 113a und 113b TKG, der sich



bislang mehr als 34.400 Bürgerinnen und Bürger angeschlossen haben.

Allen Verfassungsbeschwerden gemeinsam ist die Rüge der Beschwerdeführer, dass die §§ 113a und 113b TKG gegen das Fernmeldegeheimnis des Artikels 10 GG und gegen das aus dem allgemeinen Persönlichkeitsrecht (Artikel 2 Abs. 1 GG) in Verbindung mit dem Menschenwürdeachtungsgebot (Artikel 1 Absatz 1 GG) abgeleitete Grundrecht auf informationelle Selbstbestimmung verstoßen.

In vielen Entscheidungen betont das Bundesverfassungsgericht, dass nicht erst die Verarbeitung und Verwendung, sondern schon die Erhebung und Speicherung personenbezogener Daten und Informationen einen Eingriff in das Recht auf informationelle Selbstbestimmung²⁴ und, soweit einschlägig, in das Fernmeldegeheimnis Artikel 10 GG²⁵ ist.²⁶ Auch besteht kein Zweifel daran, dass eine den Anbietern von Kommunikationsdiensten gesetzlich auferlegte Pflicht zur Speicherung personenbezogener Kommunikationsdaten über den betrieblich erforderlichen Zeitraum hinaus einen von der betriebsbedingten Datenspeicherung separierten, eigenständigen Eingriff in die Grundrechtspositionen der Kommunikationsteilnehmer darstellt, zumal sie anderen als den ursprünglich vorgesehenen Zwecken dient.²⁷ Dieser Eingriff bedarf einer eigenständigen Rechtfertigung. Das heißt vor allem, dass der mit der Vorratsspeicherung zu erzielende Nutzen für den Rechtsgüterschutz in einem angemessenen Verhältnis zum Umfang und der Tiefe des mit der Vorratsspeicherung verbundenen Eingriffs in die Grundrechtspositionen der betroffenen Personen stehen muss.

Bei dieser für die verfassungsrechtliche Zulässigkeit der Vorratsdatenspeicherung entscheidenden Verhältnismäßigkeitsprüfung muss in Rechnung gestellt werden, dass es sich bei ihr um eine heimliche Maßnahme von hoher Eingriffsintensität handelt. Weil heute nahezu jeder an der elektronischen Kommunikation teilnimmt und dabei eine Vielzahl von Datenspuren erzeugt, ist von der Vorratsdatenspeicherung nahezu jeder

Mensch unmittelbar betroffen.²⁸ Mit den auf Vorrat gespeicherten Daten, die dem Herrschaftsbereich des Kommunikationsteilnehmers entzogen sind, sind die Sicherheitsbehörden in der Lage, Persönlichkeits-, Verhaltens- und Bewegungsprofile jedes einzelnen Kommunikationsteilnehmers zu erstellen.²⁹

Hinzu kommt, dass es sich bei der Vorratsdatenspeicherung um eine verdachtslose Maßnahme, also um eine Maßnahme handelt, in deren Wirkungsbereich nicht nur zahlreiche, sondern fast ausschließlich solche Personen einbezogen sind, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und die den Eingriff in ihre Grundrechte durch ihr Verhalten in keiner Weise veranlasst haben.³⁰

Der hohen Eingriffsintensität der Vorratsspeicherung von Telekommunikationsdaten steht in der Verhältnismäßigkeitsprüfung ihr eher geringer Nutzen gegenüber.

Die mit Hilfe der Vorratsdatenspeicherung abzuwehrenden Bedrohungen oder Gefahren für die Sicherheit spezieller oder allgemeiner Rechtsgüter sind weder konkretisierbar, noch können Wahrscheinlichkeiten für deren tatsächliches Eintreffen

angegeben werden.³¹ Das heißt, dass der Verwendungszweck der gespeicherten Daten weder bereichsspezifisch noch präzise bestimmbar ist.³²

Mit all diesen Merkmalen überschreitet die Vorratsdatenspeicherung jene Grenze, die das Bundesverfassungsgericht in seiner einschlägigen Rechtsprechung als absolute Grenze für die Zulässigkeit eines strafrechtlich motivierten Instruments der inneren Sicherheit benannt hat. Als Grenze, die selbst dann nicht überschritten werden darf, wenn mit der Maßnahme der Schutz vor schwerwiegenden Beeinträchtigungen des Allgemeinwohls oder wichtigster Rechtsgüter bezweckt wird.³³

Der hohen Eingriffsintensität der Vorratsspeicherung von Telekommunikationsdaten steht in der Verhältnismäßigkeitsprüfung ihr eher geringer Nutzen gegenüber. Die Vorratsdatenspeicherung ist ihrer technischen Eigenart nach vergangenheitsbezogen und daher, wenn überhaupt, primär der Aufklärung begangener Straftaten dienlich. Von einer generalpräventiven Wirkung kann nicht ausgegangen werden. Es ist nicht damit zu rechnen, dass das Instrument potenzielle Straftäter



von der Ausführung geplanter Straftaten abhalten wird. Allenfalls ist damit zu rechnen, dass die Vorratsdatenspeicherung in nur sehr wenigen und nur wenig bedeutsamen Einzelfällen der Aufklärung von Straftaten und dem präventiven Rechtsgüterschutz nützlich sein kann.

Fazit

Es spricht vieles dafür, dass die Umsetzung der Richtlinie über die Vorratsdatenspeicherung in deutsches Recht wenigstens in Teilen vom Bundesverfassungsgericht als verfassungswidrig bewertet wird. 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.

Die mit der Vorratsdatenspeicherung in qualitativer und quantitativer Hinsicht verbundenen tiefen Eingriffe in die Grundrechte auf informationelle Selbstbestimmung nahezu aller Bürgerinnen und Bürger droht das Misstrauen gegenüber staatlichen Institutionen massiv zu befördern und wird zu umfassenden kommunikativen Verhaltensänderungen führen.³⁴ In besonderem Maße werden dadurch diejenigen Berufsgruppen betroffen sein, die auf die Vertraulichkeit übermittelter Informationen konstitutiv angewiesen sind. Dazu zählen allgemein die Vertrauensberufe, nicht zuletzt auch die Journalisten, deren Rolle als „vierte Gewalt“ erheblich geschwächt werden dürfte. Die Regelungen der Vorratsdatenspeicherung insbesondere die der §§ 113a und 113b gelten uneingeschränkt und machen für Vertrauensberufe und Berufsgeheimnisträger – und damit auch Journalisten – keine Ausnahme.

Endnoten:

- 1 BGBl. 2007 I.
- 2 Vgl. Verfassungsbeschwerde Vorratsdatenspeicherung vom 31. 12.2007, S. 109 ff AZ. 1 BvR 256/08, (<http://vorratsdatenspeicherung.de/content/view/51/70>).
- 3 Ratsdok. SN 3926/6/01 REV 6, Conclusions adopted by the Council (Justice and Home Affairs), Schlussfolgerung Nr. 4, Brüssel, 20. September 2001.
- 4 Vgl. Erklärung zum Kampf gegen den Terrorismus, Brüssel, 25. März 2004.
- 5 Ratsdok. 8958/04, Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten ..., 28. April 2004.
- 6 Diese Entscheidung der niederländischen Ratspräsidentschaft wurde von der Bundesregierung unter Hinweis auf die mit dem Entwurf verbundenen grundrechtlichen und datenschutzrechtlichen Problemen begrüßt. Vgl. Pressemitteilung des Bundesministeriums der Justiz vom 18. November 2004.
- 7 Ratsdok. 10255/1/05 REV 1, Presidency Conclusion on the Brussels European Council, Concl. 2, 15. Juli 2005.

- 8 KOM(2005) 438 endg. Vorschlag für eine Richtlinie über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, 21. September 2005.
- 9 KOM(2005) 438 endg. Artikel 7.
- 10 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsspeicherung ...15. März 2006, ABL L 105/54.
- 11 Richtlinie 2006/24/EG a. a. O. Artikel 6.
- 12 Bundesratsentwurf eines Gesetzes zur Verbesserung der Ermittlungsmaßnahmen wegen des Verdachts sexuellen Missbrauchs von Kindern und der Vollstreckung freiheitsentziehender Maßnahmen. Abgedruckt als Anlage 1 der Bundestagsdrucksache 14/9801 vom 17. Juli 2002.
- 13 BT-DS 14/9801 vom 17. Juli 2002.
- 14 BR-DS 755/03B vom 19. Dezember 2003, Beschluss zur Änderung des Telekommunikationsgesetzes, besonders des § 94 TKG.
- 15 BR-DS 406/1/04 vom 13. September 2004.
- 16 BT-DS 15/4597 vom 22. Dezember 2004.
- 17 BT-DS 15/4748 vom 26. Januar 2005.
- 18 BR-DS 723/05 vom 25. November 2005.
- 19 BT-DS 16/545 vom 7. Februar 2006.
- 20 Rechtssache C-301/06: Irland gegen den Rat der Europäischen Union und das Europäische Parlament (OJ L 105, S. 54).
- 21 Vgl. KOM(2005) 438 endg, S. 8.
- 22 Vgl. hierzu: KOM(2005) 538 endg/2, Mitteilung der Kommission an das Europäische Parlament und den Rat über die Folgen des Urteils des Gerichtshofs vom 13. September 2005 (Rs. C-176/03), S. 2, Brüssel 24. November 2005.
- 23 Vgl. Urteil des Europäischen Gerichtshofs Nr. C-317/04 und C-318/04 vom 30. Mai 2006.
- 24 Vgl. z.B. BVerfGE 65, 1 und BVerfGE 103, 21 (33).
- 25 Vgl. z.B. BVerfGE 85, 386 (398) und BVerfGE 100, 313 (366).
- 26 So auch Breyer/Patrick (2005): Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland, Berlin, S. 89.
- 27 So auch Breyer, Patrick: a. a. O. S. 92.
- 28 Vgl. BVerfGE 1 BvR 518/02 vom 23. Mai 2006, (123).
- 29 Vgl. BVerfGE, 2 BvR 2099/04 vom 2. März 2006 (90, 91).
- 30 Vgl. BVerfGE 1 BvR 518/02 vom 23. Mai 2006 (117).
- 31 Vgl. Ebd., (136, 137 und 138).
- 32 Vgl. BVerfGE 65 1 (47).
- 33 So betont das Bundesverfassungsgericht z. B.: „Der Zwang zur Angabe personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbareren Zwecken nicht zu vereinbaren. (BVerfGE 65 1 (47)) Oder: „Verzichtet der Gesetzgeber auf begrenzende Anforderungen an die Wahrscheinlichkeit des Gefahreneintritts sowie an die Nähe der Betroffenen zur abzuwehrenden Bedrohung und sieht er gleichwohl eine Befugnis zu Eingriffen von erheblichem Gewicht vor, genügt dies dem Verfassungsrecht nicht. (BVerfGE 1 BvR 518/02 (137))“
- 34 Eindrucksvolle Hinweise auf schon jetzt bemerkbare Änderungen im kommunikativen Verhalten sind dem ergänzenden Schriftsatz zur Verfassungsbeschwerde (Dr. Christoph Gusy et al.) vom 8. Februar 2008 zu entnehmen, vgl. <http://vorratsdatenspeicherung.de/content/view/51/70>.

Die Autorin

Bundesministerin a. D. Sabine Leutheusser-Schnarrenberger

ist seit 1990 Mitglied des Deutschen Bundestages. Zudem ist sie Mitglied des Bundesfachausschusses Innen und Recht und stellvertretende Vorsitzende der FDP-Fraktion. Von 1992 bis 1996 war sie Bundesministerin der Justiz. Weiterhin gehört zu den Antragstellern der Verfassungsklage gegen die Vorratsdatenspeicherung, die voraussichtlich im März 2008 verhandelt wird.

