SIRA
Sicherheit im öffentlichen Raum

ISBN
978-3-943207-01-9

Heft 1
November 2011

Herausgegeben von:

Mathias Bug
Prof. Dr. Ursula Münch
Prof. Dr. Viola Schmid LL.M.

PROF. DR. VIOLA SCHMID LL.M. (Harvard)
2. SIRA Conference Series: Innere Sicherheit - auf Vorrat gespeichert?
2

JÜRGEN MAURER, Vizepräsident beim Bundeskriminalamt
Mindestspeicherfristen – Praktische Erfahrungen aus Sicht der Polizei
12

Dr. des. SEBASTIAN BUKOW
Vorratsdatenspeicherung in Deutschland - Symbol des sicherheitspolitischen Wandels und des zivilgesellschaftlichen Protests?
22

RA SEBASTIAN SCHWEDA
Umsetzungsunterschiede der Vorratsdatenspeicherungsrichtlinie in Europa – ein Bericht aus dem Forschungsprojekt InVoDaS im Mai 2011
56

Dr. SUSANNE BECK LL.M. (LSE)
Vorratsdatenspeicherung und aktuelle Entwicklungen in der Inneren Sicherheit im Vereinigten Königreich – eine Analyse im Mai 2011
87


Innere Sicherheit – auf Vorrat gespeichert?

Tagungsband 2. SIRA Conference Series

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Viola Schmid

2. SIRA Conference Series: Innere Sicherheit – auf Vorrat gespeichert ?

1. Zu SIRA

Der Forschungsverbund „Sicherheit im öffentlichen Raum (SIRA)" besteht aus acht Teilprojekten[1]. Kennzeichnend ist die Zusammarbeit zwischen Vertretern/innen der Politikwissenschaft, der Kulturanthropologie, der Soziologie, der Rechtswissenschaft, der Ökonomie und der Informationstechnologie. Hervorzuheben ist auch, dass SIRA-Endanwender entsprechend der Begleitforschungskonzeption des Bundesministeriums für Bildung und Forschung in das Projekt eingebunden sind.

2. Zur Conference Series

Ein erstes Ergebnis von SIRA ist die SIRA Conference Series, die sich in ihrer zweiten Abteilung am 26. und 27. Mai 2011 an der Universität der Bundeswehr, München, dem Thema „Innere Sicherheit – auf Vorrat gespeichert?" gewidmet hat. Auf der Konferenz wurde die polizeiliche Praxis durch den Vizepräsidenten beim Bundeskriminalamt, Herrn Jürgen Maurer, repräsentiert. Vier Vertreter/innen der Wissenschaft – ein Politikwissenschaftler und drei Rechtswissenschaftler – präsentierten verfassungsrechtliche wie europarechtliche Konturen der Herausforderungen, die die Thematik Vorratsdatenspeicherung mit sich bringt. Der Politikwissenschaftler Dr. des. Sebastian U. Bukow von der Universität Düsseldorf stellte die Frage, in wie weit die Vorratsdatenspeicherung Symbol des sicherheitspolitischen Wandels und zivilgesellschaflichen Protests in Deutschland ist. Ergänzt wurden diese Fragestellungen durch Informationen über die Umsetzung der Vorratsdatenspeicherungsrichtlinie in den einzelnen europäischen Mitgliedsstaaten. Diese Informationen wurden von Herrn Rechtsanwalt Sebastian Schweda vom Institut für europäisches Medienrecht e.V. aufbereitet. Eine Kombination von sicherheitspolitischen Erwägungen und Vorratsdatenspeicherungstendenzen in einem Mitgliedsstaat – im Vereinigten Königreich – bot die Rechtswissenschaftlerin

[1] Nähere Informationen: www.sira-security.de

Dr. Susanne Beck, LL.M. (LSE) von der Universität Würzburg an. Abschließend lieferte Prof. Dr. Viola Schmid, LL.M. (Harvard) von der Technischen Universität Darmstadt eine Analyse der Vorratsdatenspeicherungsentscheidung des Bundesverfassungsgerichts, die Eckpfeiler für eine Charta des internationalen (IT-) Sicherheitsrechts sein könnte. Organisiert wurde die Konferenz von Prof. Dr. Ursula Münch von der Universität der Bundeswehr München und Prof. Dr. Viola Schmid, LL.M. (Harvard) von der Technischen Universität Darmstadt.

3. Zum Thema Vorratsdatenspeicherung

a) Zur Terminologie

Zunächst hervorzuheben ist, dass in einer informationstechnologischen und datenschutzrechtlichen Betrachtung der Titel „Vorratsdatenspeicherung" missverständlich ist. Selbstverständlich geht es nicht nur um die Erhebung bzw. Speicherung von Daten auf Vorrat, sondern auch um die Übermittlung und Nutzung dieser Daten. Diese unterschiedlichen Informationstechnologien finden sich in § 3 Abs. 3-5 Bundesdatenschutzgesetz wieder.

(3) Erheben ist das Beschaffen von Daten über den Betroffenen.
(4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:
1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung,
2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
a) die Daten an den Dritten weitergegeben werden oder
b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft
4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(5) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

b) Zur Relevanz

Durch die Wahl des Themas wird die besondere Bedeutung der Vorratsdatenspeicherung für das „Datenorganisationsrecht“[2] wie das Sicherheitsrecht der Gegenwart und der Zukunft hervorgehoben. Die Bedeutung der Vorratsdatenspeicherung für den in der Politikwissenschaft diskutierten „erweiterten Sicherheitsbegriff“ und eine „neue Sicherheitsarchitektur“ ist wohl unbestritten. Optisch und thematisch sehr simplifiziert bringt dies etwa auch das Video des Designstudenten Alexander Lehmann mit dem Titel „Du-bist-Terrorist.de“ zum Ausdruck, welches unterschiedliche Datenorganisationsoptionen (vom Körperscanner bis zur Telekommunikationsverkehrsdatenspeicherung und –nutzung bis zur Online-Durchsuchung) kombiniert. Auf dieses Video wird nicht mit einer Wertung Bezug genommen, es wird zitiert, um die Bedrohungsszenarien, die der Diskussion von Aktivisten zugeführt werden, zu verdeutlichen. Es gibt eben Pro-Cyberprotagonists, die die in der Digitalisierung geborenen Überwachungsstrategien für die Erhöhung von Sicherheit einsetzen wollen. Und es gibt eben Anti-Cyberprotagonists, die diese „Nutzung“ grundsätzlich ablehnen. Die Konferenz mit ihren Experten mit polizeilicher, rechtswissenschaftlicher und politikwissenschaftlicher Expertise, konnte diesen Konflikt durch die Präsentation von Erfahrungen, von juristischen Texten (Rechtsprechung und Rechtsetzung) und Akzeptanzanalysen Argumentationsmaterial zuführen. Eine Argumentationsgrundlage, die sicher hervorzuheben ist, ist die Entscheidung des Bundesverfassungsgerichts vom 02.03.2010 (1 BvR 256/08, 1 BvR 263/09, 1 BvR 586/08) geboten. Das Rechtssystem in der Bundesrepublik Deutschland ist seit dieser Entscheidung um grundlegende Erkenntnisse bereichert.

[2] In der Terminologie des Fachgebiets Öffentliches Recht an der Technischen Universität Darmstadt handelt es sich um einen Oberbegriff für die in § 3 Abs. 3-5 Bundesdatenschutzgesetz genannten Optionen des Umgangs mit Daten.

c) Die Vorratsdatenspeicherungsentscheidung des Bundesverfassungsgerichts – Eckpfeiler für eine Charta des (internationalen) (IT-)Sicherheitsrechts?

Die folgenden Ausführungen rollen die Überschrift „Eckpfeiler für eine Charta des (internationalen) (IT-)Sicherheitsrechts?" von hinten auf. Zunächst bleibt auch nach dem Ende der SIRA Conference Series wie auch am Ende dieser Veröffentlichung das **„?"** bestehen. Trotz des eindrucksvollen Postulats des Vizepräsidenten des Bundeskriminalamts muss es angesichts der existierenden Skepsis von Aktivisten – wie etwa dem Arbeitskreis Vorratsdatenspeicherung – aus wissenschaftlicher Sicht bei einem „?" bleiben. Auch handelt es sich um eine globale Frage, die eben nicht nur für die Bundesrepublik Deutschland oder die europäischen Mitgliedsstaaten Bedeutung hat. Die Zukunft wird beantworten, in wie weit die Entscheidung des höchsten deutschen Gerichts auch über die Bundesrepublik Deutschland hinaus für andere Rechtsordungen, etwa im Wege der rechtsvergleichenden Wissenschaft, Bedeutung erlangen wird. Jedenfalls enthält die Entscheidung hinsichtlich des weiteren Überschriftenbestandteils **„Recht"** den Hinweis auf eine neuere Tendenz. Im „informationstechnologischen Sicherheitsrecht" in Deutschland mag es eine „Karlsruher Republik" geben. Belege dafür, dass das Bundesverfassungsgericht im informationstechnologischen Sicherheitsrecht als Reservegesetzgeber tätig wird, lassen sich in den Entscheidungen zur

- Akustischen Wohnraumüberwachung (1BvR 2378/98)
- Polizeirechtlichen Telekommunikationsüberwachung (1BvR 668/04)
- Rasterfahndung (1 BvR 518/02)
- Kennzeichenscanning (1 BvR 2074/05)
- Online-Druchsuchung (1 BvR 370/07)
- Videosurveillance am Denkmal (1 BvR 2368/06)
- Verkehrsüberwachung (2 BvR 941/08)
- Kontostammdaten (1BvR 1550/03)

finden. In all diesen Fällen hat das Bundesverfassungsgericht (den Gesetzgeber) gezwungen, einen neuen und anderen Kurs einzuschlagen. Die Konsequenz dieser Rechtsprechungserfahrung ist, dass aus rechtswissenschaftlicher Sicht **„Sicherheit"** nicht eine statische Definition zugrunde liegt, sondern es sich um einen Prozess handelt, der zu optimieren ist. Die Digitalisierung, die zu einer ubiquitären und

allzeitigen Durchdringung unserer Umwelt mit Informationstechnologie führt, führt auch zu einer neuen Relation zwischen **Sicherheit** und **IT-Sicherheit**: Sicherheit und IT-Sicherheit bedingen sich gegenseitig. Im Zeitalter des „Ubiquitous Computing", des „Ambient Assisted Living" oder der „Connected World" und des „Internet of Things" kann weder Sicherheit ohne IT-Sicherheit noch IT-Sicherheit ohne Sicherheit erzielt werden. Deswegen ist die Klammer **„(IT-)"**, die eine Verknüpfung von IT-Sicherheit und Sicherheit symbolisiert, gerechtfertigt. Bereits bei den Ausführungen zum „?" wurde angedeutet, welche Bedeutung das Bundesverfassungsgericht für das nationale und internationale **(IT-)Sicherheitsrecht** haben könnte. In seiner Entscheidung (1 BvR 256/08) hat das Bundesverfassungsreicht nicht behauptet, dass in der Verfassung alles über Sicherheit und IT-Sicherheit in Bezug auf Telekommunikationsverbindungsdaten steht. Es hat aber im Wege einer dynamisch-technikorientierten Auslegung rechtliche Mindeststandards entwickelt, die sich auch in den Beiträgen zum Tagungsband wiederfinden. Im Rahmen dieser Einfühung seien nur einige dieser Mindeststandards hervorgehoben: zum einen die **„Antiprofilierungsratio"**. Diese Antiprofilierungsratio lässt sich als ständige Rechtsprechung seit der bahnbrechenden Volkszählungsentscheidung (BVerfGE 65, 1 (43)) nachweisen:

> „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, **wer was wann und bei welcher Gelegenheit über sie weiß**".

Diese Antiprofilierungsratio wird auch in der Vorratsdatenspeicherungsentscheidung (Rn.241) aufrecht erhalten:

> **<241>:** „Eine vorsorglich anlasslose Speicherung aller Telekommunikationsverkehrsdaten über sechs Monate ist unter anderem deshalb ein so schwerwiegender Eingriff, weil sie ein Gefühl des ständigen Überwachtwerdens hervorrufen kann; sie erlaubt in unvorhersehbarer Weise tiefe Einblicke in das Privatleben, ohne dass der Rückgriff auf die Daten für den Bürger unmittelbar spürbar oder ersichtlich ist. Der

Einzelne weiß nicht, was welche stattliche Behörde über ihn **weiß, weiß aber, dass die Behörden vieles, auch Höchstpersönliches über ihn wissen können**".

Der zweite Minimalstandard, der hervorgehoben werden soll, ist die **„Differenzierungsratio"**. Es geht eben – unter Zugrundelegung von § 3 Abs. 3 – 5 BDSG – um die **E**rhebung, **S**peicherung, **Ü**bermittlung und **N**utzung von Daten („ESÜN"). Belegen lässt sich diese „informationstechnologisch differenzierte Betrachtungsweise" des Bundesverfassungsgerichts in der Vorratsdaten-speicherungsentscheidung (Rn. 250), wo sogar eine Differenzierung zwischen Push- und Pull-Betrieb vorgenommen wird:

<250>: „Zur Wirksamkeit der Kontrolle gehört es auch, dass die Daten aufgrund der Anordnung von den Telekommunikationsunternehmen als speicherungs-verpflichteten Dritten herausgefiltert und übermittelt werden, das heißt den Behörden also **nicht ein Direktzugriff** auf die Daten eröffnet wird. Auf diese Weise wird die Verwendung der Daten auf das **Zusammenwirken verschiedener Akteure** verwiesen und damit in **sich gegenseitig kontrollierende Entscheidungsstrukturen** eingebunden".

Die dritte, maßgebende Ratio ist und bleibt die **„Kernbereichsratio"** im informationstechnologischen Sicherheitsrecht. Es gibt eben einen Kreis auf besondere Vertraulichkeit angewiesener Telekommunikationsverbindungen, und für diese ist ein Übermittlungsverbot vorzusehen.

<238>: „Verfassungsrechtlich geboten ist […], zumindest für einen **engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen** ein grundsätzliches Übermittlungsverbot vorzusehen. Zu denken ist hier etwa an **Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen, die grundsätzlich anonym bleibenden Anrufern** ganz oder überwiegend telefonische Beratung in seelischen oder sozialen Notlagen anbieten und die selbst oder deren Mitarbeiter insoweit anderen Verschwiegenheitsverpflichtungen unterliegen (vgl. § 99 Abs. 2 TKG) ".

Eine weitere Ratio ist die **„Kombinationsratio“**. Wer die Erhebung, Speicherung und Übermittlung von Daten regelt (Art. 73 Abs. 1 Nr. 7 GG „Telekommunikationsrechtliche Kompetenz“), muss klare Kriterien zur Nutzung zugrunde legen („Sachkompetenz“). Grundsätzlich ist die Erhebung und Speicherung von Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken verfassungsrechtlich strikt untersagt.

<264> 5. „Die […] den Verhältnismäßigkeitsanforderungen genügenden normenklaren Begrenzung der Datenverwendung ist ein **untrennbarer** Bestandteil der Anordnung der Speicherungsverpflichtung und obliegt deshalb dem die Verpflichtung auferlegenden Bundesgesetzgeber. […]

<213> Allerdings entspricht es der ständigen Rechtsprechung des Bundesverfassungsgerichts, dass dem Staat eine Sammlung von personenbezogenen Daten auf Vorrat **zu unbestimmten oder noch nicht bestimmbaren Zwecken verfassungsrechtlich strikt untersagt ist** (vgl. BVerfGE 65, 1 <46>; 100, 313 <360>; 115, 320 <350>; 118, 168 <187>).

<266> Demgegenüber ist es unzulässig, **unabhängig von solchen Zweckbestimmungen einen Datenpool auf Vorrat zu schaffen, dessen Nutzung je nach Bedarf und politischem Ermessen der späteren Entscheidung verschiedener staatlicher Instanzen überlassen bleibt“.**

Nicht nur ein regulatorisches Prinzip wie die Kombinationsratio, die verpflichtet über Erhebung und Speicherung auf der einen uno actu mit der Übermittlung und Nutzung zu entscheiden, ist in der Entscheidung enthalten: vielmehr ist IT-Sicherheit als Verfassungsprinzip konturiert. Zunächst wird die Qualität der IT-Sicherheit beschrieben und ein besonders hoher Standard verlangt.

<221> „Eine Speicherung der Telekommunikationsverkehrsdaten im Umfang des § 113a TKG bedarf der gesetzlichen Gewährleistung eines **besonders hohen Standards der Datensicherheit**“.

Das Bundesverfassungsgericht begnügt sich aber nicht damit, hohe Qualität der IT-Sicherheit zu fordern, sondern macht auch detaillierte Vorgaben für die Realisierung

der Qualitätsanforderungen. Im Wesentlichen können hier sieben Realisierungsdoktrinen unterschieden werden:

(1) Getrennte Speicherung der Daten
(2) Anspruchsvolle Verschlüsselung
(3) Gesichertes Zugriffsregime unter Nutzung etwa des 4-Augen-Prinzips
(4) Revisionssichere Protokollierung
(5) Einhaltung des Zweckbindungsgrundsatzes (bestimmte Zwecke; mit Erreichen der Zwecke Löschungsverpflichtung)
(6) Effektivität der Durchsetzung der IT-Standards bei der Übermittlung: Pedigree (Kennzeichnung)
(7) Differenzierung: „Push"- und „Pull-Betrieb"

Zusammenfassend werden alleine diese IT-Sicherheitsprinzipien in Literatur und Praxis in Zukunft hohe Herausforderungen bieten. Exemplarisch, wie differenziert das BVerfG sich hier auf die Informationstechnologie einlässt, zeigen die Randnummern 223 und 250 der Entscheidung:

<223> „[Sachverständigenvortrag in der mündlichen Verhandlung und in schriftlichen Stellungnahmen (Ergänzung der Verfasserin):] […] „ein weites Spektrum von Instrumenten zur Erhöhung der Datensicherheit aufgezeigt. **Genannt wurden etwa** eine **getrennte Speicherung** der nach § 113a TKG zu speichernden Daten auf auch **physisch getrennten und vom Internet entkoppelten Rechnern, eine asymmetrische kryptografische Verschlüsselung unter getrennter Verwahrung der Schlüssel, die Vorgabe des Vier-Augen-Prinzips** für den Zugriff auf die Daten verbunden **mit fortschrittlichen Verfahren zur Authentifizierung für den Zugang zu den Schlüsseln, die revisionssichere Protokollierung des Zugriffs auf die Daten und deren Löschung** sowie der Einsatz von automatisierten Fehlerkorrektur- und Plausibilitätsverfahren. Ergänzend […] **Schaffung von Informationspflichten bei Datenschutzverletzungen, die Einführung einer verschuldensunabhängigen Haftung oder eine Stärkung der Ausgleichsansprüche für immaterielle Schäden** […].

<250> Zur Wirksamkeit der Kontrolle gehört es auch, dass die Daten aufgrund der Anordnung von den Telekommunikationsunternehmen als speicherungsverpflichte-

ten Dritten herausgefiltert und übermittelt werden, das heißt den Behörden **also nicht ein Direktzugriff auf die Daten** eröffnet wird. Auf diese Weise wird die Verwendung der Daten auf das Zusammenwirken verschiedener Akteure verwiesen und damit in sich gegenseitig kontrollierende Entscheidungsstrukturen eingebunden".

Mit diesen Rationes Decidendi konturiert das Bundesverfassungsgericht ein nationales (IT-) Sicherheitsrecht, dessen Mindeststandards aber auch teilweise „europarechtsresilient" sein könnten. Als europarechtsresilient könnten sie deswegen interpretiert werden, weil sie Bestandteil des „unantastbaren Kerngehalts der Verfassungsidentität des Grundgesetzes" (BVerfG-Urteil vom 30.06.2009 – 2 BvE 2/08, Rn. 240) sein könnten und insoweit weder europa- noch völkerrechtlich zur Disposition stehen würden. In seiner Vorratsdatenspeicherungsentscheidung (Rn. 218) hat das Bundesverfassungsgericht auf die Rechtsprechung zum „unantastbaren Kerngehalt der Verfassungsidentität des Grundgesetzes" auch im Kontext des informationstechnologischen Sicherheitsrechts Bezug genommen:

<218> „[…] **Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert** werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland (vgl. zum grundgesetzlichen Identitätsvorbehalt BVerfG, Urteil des Zweiten Senats vom 30. Juni 2009 – 2 BvE 2/08 u.a. -, juris, Rn. 240), **für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss. Durch eine vorsorgliche Speicherung der Telekommunikationsverkehrsdaten wird der Spielraum für weitere anlasslose Datensammlungen auch über den Weg der Europäischen Union erheblich geringer**".

Mit diesem Zitat ist deutlich, dass jedenfalls die „Antiprofilierungsratio" zur verfassungsrechtlichen Identität gehört. Die Zukunft wird erweisen, inwieweit auch die Kombinationsratio – nämlich die Verpflichtung über Erhebung und Speicherung auf der einen und Übermittlung und Nutzung auf der anderen uno actu zu entscheiden – Anteil an dieser Europarechtsresilienz hat. Die Antwort auf diese Frage wird die

Pfeilerqualität der BVerfG-Entscheidung für eine Charta des nationalen und internationalen IT-Sicherheitsrechts konturieren.

Mit der Positionierung dieses Vorworts zur Frage „Die Vorratsdatenspeicherungsentscheidung des Bundesverfassungsgerichts – Eckpfeiler für eine Charta des (internationalen) (IT-)Sicherheitsrechts?“ soll auf die Einzelfragen, die in den folgenden Verschriftlichungen der Vorträge behandelt werden, vorbereitet werden. Sie stellen jeweils den Diskussionsstand zum Mai 2011 dar. Die formale Unterschiedlichkeit in der Zitierweise ist dem Usus der Einzeldisziplinen geschuldet.

Ein besonderer Dank gilt der Sekretärin des Fachgebiets Öffentliches Recht, Frau Heidi Roßmann, sowie den beiden studentischen Hilfskräften des Lehrstuhls für Innenpolitik und Vergleichende Regierungslehre, Konstantin Seliverstov und Caroline Wegener. Bei der Durchführung der Conference Series sowie bei dieser Veröffentlichung konnte auf deren tatkräftige Unterstützung gebaut werden. Möge dieser Tagungsband viele Interessenten gewinnen und Diskussion initiieren bzw. begleiten.

Darmstadt, im November 2011 Prof. Dr. Viola Schmid, LL.M. (Harvard)

Prof. Dr. Viola Schmid, LL.M. (Harvard) ist Lehrstuhlinhaberin im Fachgebiet für Öffentliches Recht an der Technischen Universität Darmstadt. E-Mail: schmid@jus.tu-darmstadt.de

Jürgen Maurer, Vizepräsident beim Bundeskriminalamt

Mindestspeicherfristen – Praktische Erfahrungen aus Sicht der Polizei

Abstract

Das BVerfG hat am 02.03.2010 die Speicherung von Verkehrsdaten nach der damals geltenden Rechtslage für nichtig erklärt. Das Gericht hat in seinem Urteil aber ausdrücklich bestätigt, dass eine Rekonstruktion gerade der Telekommunikationsverbindungen für eine effektive Strafverfolgung und Gefahrenabwehr von besonderer Bedeutung ist. Für die Polizei stellen Daten über die Nutzung elektronischer Kommunikationsmittel sowohl bei der Verfolgung von Straftaten als auch bei der Gefahrenabwehr ein unverzichtbares Ermittlungswerkzeug dar. Die Verkehrsdaten sind oft der erste Ermittlungsansatz für weitere Maßnahmen oder für die Beweisführung gegen oder zu Gunsten des Beschuldigten. Problematisch ist, dass das BVerfG in seinem Urteil keine Übergangsregelung bis zur Schaffung verfassungskonformer Normen eingeräumt hat. Deshalb sind in der polizeilichen Arbeit seit dem 02.03.2010 nachweislich erhebliche Schutzlücken und Ermittlungsdefizite entstanden. Das BKA hat seit der Entscheidung des BVerfG alle seitens des BKA gestellten Auskunftsersuchen erfasst, ausgewertet und bedeutsame Rechtstatsachen in den Ländern erhoben. Die Speicherdauer von sechs Monaten wäre aus Sicht der Strafverfolgungsbehörden wünschenswert.

Einleitung

Das Thema Mindestspeicherfristen ist nicht neu, nach wie vor jedoch aktuell und Gegenstand von Debatten. In der heutigen Zeit stellen Daten über die Nutzung elektronischer Kommunikationsmittel ein für die Polizei unverzichtbares Ermittlungswerkzeug dar, und zwar nicht nur bei der Verfolgung von Straftaten, sondern auch für die Gefahrenabwehr. Dies gilt insbesondere für den internationalen Terrorismus und schwere Fälle der Organisierten Kriminalität. Die sogenannten Verkehrsdaten spielen dabei als häufig „ersten“ Ermittlungsansatz für weitere Maßnahmen oder für die Beweisführung gegen oder zu Gunsten eines Beschuldigten eine wichtige Rolle. Am 2. März 2010 hat das BVerfG die Speicherung von Verkehrsdaten, in der damaligen Ausgestaltung, als mit dem Grundgesetz unvereinbar und daher für nichtig erklärt. Das Gericht erkannte gleichzeitig ausdrücklich an, dass eine Rekonstruktion gerade der Telekommunikationsverbindungen für eine effektive Strafverfolgung und Gefahrenabwehr von besonderer Bedeutung ist:

„Sie [die Speicherung der Telekommunikationsverkehrsdaten für sechs Monate] knüpft vielmehr in noch begrenzt bleibender Weise an die besondere Bedeutung der Telekommunikation in der modernen Welt an und reagiert auf das spezifische Gefahrenpotential, das sich mit dieser verbindet. […] Eine Rekonstruktion gerade der Telekommunikationsverbindungen ist daher für eine effektive Strafverfolgung und Gefahrenabwehr von besonderer Bedeutung".

Folglich erklärte das BVerfG nicht das Instrument der Speicherung und Beauskunftung von Verkehrsdaten der Telekommunikation in Gänze für verfassungswidrig und nichtig, sondern bezog sich allein auf die konkret angefochtenen Regelungen der Speicherung und Beauskunftung von „Vorratsdaten". Für eine verfassungsgemäße (Neu-)Regelung sind – so das Gericht - Regelungen zur Datensicherheit, zur Begrenzung der Datenverwendung, zur Transparenz und zum Rechtsschutz erforderlich. Für die Polizei ist hinsichtlich der Minderspeicherungsfristen einerseits die anlasslose Speicherung von Verkehrsdaten bei den Providern, andererseits die Auskunftserteilung zu diesen Daten von Bedeutung. Diese Datenerhebung stellt zwar einen Eingriff in das Fernmeldegeheimnis nach Art. 10 GG dar. Die Beauskunftung von Verkehrsdaten ist jedoch nur bei

- schwerwiegenden Straftaten (siehe § 100g StPO) oder
- erhöhtem Gefahrengrad für ein hochwertiges Rechtsgut (siehe z. B. § 20m BKAG) und
- unter Richtervorbehalt möglich.

Dem gegenüber ist die Auskunft zu polizeilich bereits bekannten IP-Adressen lediglich eine Art Anschlussinhaberfeststellung, die zur Identifizierung des Inhabers der IP-Adresse führen soll. Dies stellt keinen gesonderten Eingriff in Art. 10 Abs. 1 GG dar, die verfassungsrechtlichen Anforderungen bei der mittelbaren Nutzung von Verkehrsdaten sind dementsprechend geringer als bei Auskunftsersuchen nach § 100g StPO.

Das Bundesverfassungsgericht hat dies ausdrücklich bestätigt:

Bei Vorliegen eines Anfangsverdachts (unabhängig von der zugrundeliegenden Straftat) oder einer konkreten Gefahr (unabhängig vom betroffenen Rechtsgut) sind

Auskunftsansprüche gegenüber den Diensteanbietern hinsichtlich der Anschlussinhaber bereits bekannter IP-Adressen auf Grundlage der § 113 TKG i. V. m. den Generalklauseln (StPO, Polizeirecht) ohne Richtervorbehalt zulässig. Diese Vorgehensweise ist mit der Auskunft zu einer Telefonnummer oder einem Kfz-Kennzeichen vergleichbar. Diese klare Differenzierung der Abfragemodalitäten ist zu begrüßen. Der Senat hat damit die Auskunft zu bereits polizeilich bekannten IP-Adressen strikt von der Erhebung von Verkehrsdaten getrennt, so dass das Urteil zunächst auch keine direkten Auswirkungen auf Auskunftsersuchen zu Anschlussinhaberdaten zu einer IP-Adresse hat. Um das Auskunftsersuchen zu einer bekannten IP-Adresse zu beantworten, muss der Diensteanbieter jedoch auf Verkehrsdaten zurückgreifen. Das bedeutet, dass für Fälle, in denen diese Verkehrsdaten nicht zu Abrechnungszwecken erforderlich sind und deshalb auch nicht gespeichert werden dürfen, selbst diese Auskunftsersuchen ohne Mindestspeicherfristen ins Leere gehen. Die Problematik der IP-Adresse als erster und erfolgversprechendster Ermittlungsansatz ist im Phänomenbereich Cybercrime besonders offenkundig. Die Notwendigkeit von Mindestspeicherfristen wird ebenso im Bereich Kinderpornografie und in Gefahrenabwehrfällen wie z. B. bei Amok- oder Suizidankündigungen im Internet deutlich. Höchste Bedeutung hat diese Form der Nutzung von Verkehrsdaten vor allem angesichts der zunehmenden Verbreitung von sogenannten Flatrate-Geschäftsmodellen, bei denen Abrechnungsdaten gar nicht mehr vorhanden sind bzw. ohne Vorratdatenspeicherungsverpflichtung gar nicht gespeichert werden dürfen. Das Bundesverfassungsgericht hat in seinem Urteil wider Erwarten keine Übergangsregelung bis zur Schaffung verfassungskonformer Normen eingeräumt. Deshalb sind in der polizeilichen Arbeit seit dem 2. März 2010 nachweisbar erhebliche Schutzlücken und Ermittlungsdefizite entstanden. Insgesamt lassen sich hierzu drei Fallkategorien bilden:

- die Identifizierung einer polizeilich bekannten IP-Adresse,
- die Erhebung von retrograden Verkehrsdaten und
- die sogenannte Standortabfrage.

Die genannten Kategorien möchte ich anhand folgender Beispiele erläutern:

1. Kategorie: Identifizierung des Inhabers einer polizeilich bekannten IP-Adresse

Beispielsfall 1 (Strafverfolgung)

Die polnischen Behörden fahndeten im Rahmen der Strafvollstreckung europaweit nach einem Mörder. Der Gesuchte meldete sich regelmäßig bei seinem Account eines polnischen sozialen Netzwerks an. Die polnischen Behörden übermittelten eine Liste der Login-Daten einschließlich der beim Anmelden genutzten IP-Adressen mit der Bitte um Feststellung der hinter diesen stehenden Kundendaten. Da jedoch der Zeitpunkt der letzten Anmeldungen länger als sieben Tage zurück lag, konnte durch die deutschen Provider keine Zuordnung zu den Kundendaten mehr erfolgen. Die hierzu erforderlichen Verkehrsdaten werden bei einzelnen Providern nur sieben Tage bzw. überhaupt nicht vorgehalten. Die Provider konnten in diesem Fall keine Auskunft geben. Durch die polnischen Behörden wurde mitgeteilt, dass es sich bei den übermittelten IP-Adressen der letzten Login-Daten um den bislang einzigen Fahndungsansatz in Deutschland handelt und folglich weitere Ermittlungen zur Festnahme des gesuchten Mörders dadurch verhindert wurden.

Beispielsfall 2 (Gefahrenabwehr / Strafverfolgung)

Aufgrund eines anonymen Hinweises auf einen möglichen Amoklauf in Hessen wurde in einem Internet-Forum tatsächlich eine Ankündigung eines Amoklaufs an einer bestimmten Schule festgestellt. Über die IP zum Eintrag konnte der Provider festgestellt werden. Erste Ermittlungen zur Person des Absenders verliefen jedoch negativ, da der Provider keine retrograden Verbindungsdaten mehr speichert. Die Person des Absenders/Täters konnte später nur zufällig durch Recherchen über seinen Nickname festgestellt werden, da der Täter in einem anderen Forum mit demselben Nickname angemeldet war und dabei Bruchstücke seines Namens und der Adresse angegeben hatte. Der Täter wurde festgenommen, war geständig und wurde in eine psychiatrische Klinik eingewiesen.

Beim Täter wurde ein hohes Maß an tatsächlicher Amok-Bereitschaft festgestellt. Ort und Datum des Amok-Laufs waren bereits festgelegt. Der Täter hatte bereits erfolglos versucht, sich eine "scharfe" Schusswaffe zu verschaffen. Wegen der fehlenden Verkehrsdaten konnte die Gefahr erst zu einem späteren Zeitpunkt beseitigt und die Tat nur wesentlich erschwert aufgeklärt werden.

Beispielsfall 3 (Gefahrenabwehr):

Seit dem 19.12.2009 verschickte ein unbekannter Täter über ein Briefzentrum mehr als 100 Briefe, adressiert an Schulen, Universitäten und Privatpersonen im gesamten Bundesgebiet. Die Briefe enthielten die Androhung eines Sprengstoffanschlags im Fall der Nichtzahlung einer geforderten Geldsumme. Mit E-Mail vom 22.04.2010 trat der unbekannte Verfasser erstmals mit einer Geschädigten über deren Profil bei dem Netzwerk „studiVZ" in Kontakt. Der Betreiber von studiVZ wurde daraufhin um Benennung der IP-Adresse des Absenders ersucht. Diese wurde herausgegeben. Mittels der IP-Adresse wurde der festgestellte Anbieter um Benennung des hinter der IP mit Zeitstempel stehenden Anschlusses ersucht. Dieser teilte jedoch mit, dass aufgrund des BVerfG-Urteils diese Daten nicht mehr gespeichert werden, da die Speicherung der dynamischen IP-Adresse für Abrechnungszwecke nicht erforderlich ist. Der Täter konnte aus diesem Grund nicht ermittelt werden.

Beispielsfall 4 (Gefahrenabwehr)

Aufgrund eines Hinweises aus Luxemburg nach der im Rahmen eines dortigen Ermittlungsverfahrens erfolgten Auswertung eines beschlagnahmten Command- und Control-Servers eines Botnetzes wurde bekannt, dass dieser zu DDos-Attacken, als Proxy-Rechner zur Verschleierung der Täterkommunikation und zur Erlangung der digitalen Identität der User diente. Es wurden 218.703 deutsche IP-Adressen, die auf den Server zugriffen, an das BKA übermittelt. Primäres Ziel war es, im Rahmen der Gefahrenabwehr durch die Länderpolizeien die betroffenen Opfer, also die Inhaber der Rechner zu informieren bzw. zu warnen. Die daraufhin gestellten Auskunftsersuchen durch die Länderpolizeien gingen nach der Entscheidung des Bundesverfassungsgerichts vom 02.03.2010 weitgehend ins Leere. Von den infizierten Rechnern geht nach wie vor eine Gefahr für die Öffentliche Sicherheit und Ordnung aus.

2. Kategorie: Erhebung von retrograden Verkehrsdaten (Vorratsdatenspeicherung im engeren Sinne)

Beispielsfall 5 (Strafverfolgung)

Nach dem Bandendiebstahl von PKW und hochwertigen Baumaschinen wurden diese in Einzelteile zerlegt durch die Täter über die Internetplattform ebay veräußert. Im Rahmen eines Ermittlungsverfahrens wegen gewerbsmäßiger Bandenhehlerei wurden Beschlüsse zur Herausgabe retrograder Verbindungsdaten für die Handy- und Festnetznummern, die polizeilich anderweitig bekannt geworden waren, erlassen. Die retrograden Verkehrsdaten konnten jedoch nicht beauskunftet werden. Somit kann ein Großteil der Täterstruktur, nämlich die Diebe und deren Übergabeorte, nicht mehr ermittelt werden. Der Tatnachweis anhand der Koordinaten (Tatorte) ist nicht mehr möglich, Treffpunkte für Absprachen sind nicht mehr lokalisierbar. Die Identifizierung der Täter ist unmöglich, begangene Straftaten sind nicht aufklärbar.

Beispielsfall 6 (Gefahrenabwehr)

Hintergrund waren Hinweise US-amerikanischer und libanesischer Behörden auf Anschlagsplanungen durch Mitglieder einer Gruppe der Fatah al-Islam in Deutschland in 2010. Die durchgeführten Gefahrenabwehrmaßnahmen dienten zunächst der Identifizierung und Lokalisierung möglicher Zellenmitglieder in Deutschland sowie der Gewinnung von Erkenntnissen zur gruppeninternen Kommunikation. Letztlich konnte lediglich eine der genannten Personen in Deutschland identifiziert werden. Gegen diese Person, welche sich unter Benutzung von Falschpersonalien in Deutschland aufhielt, lag ein Haftbefehl der libanesischen Behörden wegen allgemeinkrimineller Delikte vor; die Person wurde festgenommen und befindet sich in Auslieferungshaft. Der Gefahrenverdacht gegen diese Person wegen eines terroristischen Anschlags konnte ausgeräumt werden. Alle weiteren Maßnahmen gegen die Gruppe liefen ins Leere, weil die Vorratsdaten nicht oder nur unvollständig von den Providern zur Verfügung gestellt wurden.

3. Kategorie: Funkzellen- und Standortabfrage

Beispielsfall 7 (Strafverfolgung)

Nach dem Mord an einem Polizeibeamten flüchtete/n die/der Täter mit dem PKW des Opfers. Die Tatortuntersuchung erbrachte keine weiterführenden Hinweise zu einem Tatverdächtigen, Augenzeugen sind nicht bekannt. Für einen bestimmten Funkzellenbereich bestand die Annahme, dass die Täter das Fluchtfahrzeug nach dem Abstellen verlassen und eine Beförderungsmöglichkeit (z. B. Taxi) per Handy anforderten. Aufgrund des Funkzellenabfrage-Beschlusses für einen potentiell in Frage kommenden Netzbetreiber (höchste Netzabdeckung) teilte dieser mit, dass keine Verkehrsdaten mehr vorliegen. Diese hätten den aussichtsreichsten Ermittlungsansatz geboten.

Beispielsfall 8 (Strafverfolgung)

Unmittelbar an einer Straßenböschung wurde ein zunächst nicht identifiziertes Mordopfer aufgefunden. Nach wenigen Tagen konnte die Identität des Mannes als 43-jähriger italienischer Staatsangehöriger ermittelt werden. Der Mann hielt sich unangemeldet in Köln auf. Italienische Behörden hatten zwischenzeitlich mitgeteilt, der Geschädigte stünde der Mafia nahe. Im Rahmen der Ermittlungen gelang es ca. drei Monate nach der Tat den möglichen Tatort und vier mögliche Tatbeteiligte zu ermitteln. Für das Ermittlungsverfahren ist es unerlässlich, die retrograden Daten zu der Telefonie aller Tatbeteiligten auswerten zu können. Das Auskunftsersuchen wurde jedoch nicht gestellt, da die Staatsanwaltschaft Köln die Stellung eines Antrags zur Anordnung eines Auskunftsersuchens nach dem Urteil des BVerfG abgelehnt hat. Nun kann nicht mehr überprüft werden, ob die drei Tatverdächtigen, die den Mord begangen haben sollen, sich in dem Zeitraum, in dem die Leiche abgelegt wurde, am Ablageort oder im tatrelevanten Zeitraum am möglichen Tatort befunden und in einer relevanten Funkzelle telefoniert haben. Die Aufklärung der Tat ist zumindest wesentlich erschwert. Die Ermittlungen dauern an.

Vor dem Hintergrund der Entscheidung des Bundesverfassungsgerichts vom 2. März 2010 hat das BKA seitdem alle seitens des BKA gestellten Auskunftsersuchen erfasst und ausgewertet. Ich möchte einen kurzen Überblick zu den Ergebnissen der statistischen Datenerhebung für den Zeitraum vom 02.03.2010 bis zum aktuellen Stichtag am 26.04.2011 geben:

- Die Auskunftsersuchen bezogen sich auf 5.082 Anschlüsse, wovon durch die Telekommunikationsanbieter 4.292, also ca. 84 % aller Ersuchen nicht beauskunftet wurden.
- Die Hauptanwendungsfälle stellten mit rund 90 % Erhebungen der hinter einer IP-Adresse stehenden Kundendaten/Bestandsdaten dar.
- In rund 9 % waren retrograde Verkehrsdatenerhebungen Gegenstand der Auskunftsersuchen. Hieraus darf aber keine abgestufte Wertigkeit abgeleitet werden, da gerade die Ermittlungen schwerster Straftaten die unmittelbare Auskunft über retrograde Verkehrsdaten erfordern. Dies deckt sich auch mit den Erfahrungen der Länderpolizeien.
- Nach knapp zwölf Monaten Erhebung im BKA fallen von den bisher erfassten 4.256 Negativ-Fällen im Bereich der Strafverfolgung 1.639 Fälle (ca. 39 %) in den Deliktsbereich der Verbreitung, des Erwerbs oder Besitzes kinder- und jugendpornografischer Schriften oder von Straftaten gegen die sexuelle Selbstbestimmung.
- 1.898 Fälle (ca. 45 %) fallen in den Deliktsbereich des Betrugs sowie Computer- und Subventionsbetrugs.
- In den beiden letztgenannten Fallgruppen handelt es sich fast ausschließlich – bis auf einen Fall um Erhebungen der hinter einer IP-Adresse stehenden Kundendaten bzw. Bestandsdaten.
- Im Bereich der Strafverfolgung waren die Auskunftsersuchen für 93 Anschlüsse bei Straftaten gegen die öffentliche Ordnung, z.B. Unterstützung einer terroristischen Vereinigung im Ausland und für 42 Anschlüsse bei Mord und Totschlag erfolglos.
- Im Bereich der Strafverfolgung insgesamt konnte in den Fällen einer Negativauskunft die zu Grunde liegende Straftat in rund 83 % der Fälle (3.521 Anschlüsse) gar nicht aufgeklärt werden, die übrigen Straftaten konnten nur teilweise aufgeklärt werden oder die Aufklärung konnte erst zu einem späteren Zeitpunkt erfolgen oder war wesentlich erschwert.

Die geschilderten und den statistischen Auswertungen zugrunde liegenden Sachverhalte belegen die polizeifachliche Erforderlichkeit der Verkehrsdatenspeicherung für eine Dauer von sechs Monaten. Die Ergebnisse belegen auch, dass die polizeiliche Reaktionszeit nur geringen Einfluss auf diesen polizeilich für erforderlich erachteten Mindestspeicherzeitraum hat. Zwischen dem Zeitpunkt der Kenntniserlangung des BKA über das Vorliegen ermittlungsrelevanter Verkehrsdaten und dem Moment der Stellung des Auskunftsersuchens lagen in 86% der Fälle maximal sieben Tage. Dies bedeutet im Umkehrschluss, dass nicht die polizeiliche Reaktionszeit, sondern das „Alter“ der Verkehrsdaten den erforderlichen Speicherzeitraum bestimmt. Das tatsächliche „Alter“ der relevanten Verkehrsdaten bei Auskunftsersuchenstellung muss daher zumeist annähernd sechs Monate

betragen haben. Polizei bzw. Staatsanwaltschaft haben aber meist keinen Einfluss darauf, wie schnell sie durch Anzeige o. ä. von dem Fall und somit dem Vorliegen möglicherweise ermittlungsrelevanter Verkehrsdaten erfahren.

Wie ist das seitens des Justizministeriums favorisierte sog. Quick-Freeze-Verfahren zu bewerten? Statt der Speicherung aller Verkehrsdaten werden – nach diesem Verfahren – nur auf Antrag Daten ab einem bestimmten Zeitpunkt „eingefroren" und den Sicherheitsbehörden anlassbezogen zeitnah übermittelt. Die Bedeutung von Verkehrsdaten, die in der Vergangenheit angefallen sind, wird oft jedoch erst im Rahmen der meist umfangreichen und zeitintensiven Ermittlungen offensichtlich. Die nie gespeicherten oder zu diesem Zeitpunkt bereits gelöschten Daten können jedoch nicht mehr „eingefroren" und beauskunftet werden. Um Herrn Wengenmeir, den bayrischen Landesvorsitzenden des BDK, zu zitieren: „Das ist ungefähr so, wie wenn eine Hausfrau ein Steak einfrieren möchte, das der Hund bereits vor drei Tagen gefressen hat." Selbst die Beschwerdeführer vor dem BVerfG hatten vorgetragen, dass das „Quick-Freeze-Verfahren" nicht gleich gut (wie Mindestspeicherfristen) geeignet ist, weil es ins Leere geht, wenn Verkehrsdaten nicht oder nicht mehr vorhanden sind (Urteil BVerfG vom 02.03.2010, Rdnr. 141). Das BVerfG stellte schließlich auch fest (Urteil BVerfG vom 02.03.2010, Rdnr. 208), dass sechs Monate Speicherung nicht zu beanstanden und mildere Mittel mit gleicher Eignung nicht erkennbar sind. Insbesondere ist das „Quick-Freeze-Verfahren, das Daten aus der Zeit vor der Anordnung ihrer Speicherung nur erfassen kann, soweit sie noch vorhanden sind, kein geeignetes Korrektiv". Die Polizei kann weder im Bereich der Strafverfolgung noch für die Gefahrenabwehr auf die Möglichkeit der Rekonstruktion von Verkehrsdaten verzichten. Seit dem 2. März 2010 bestehen in beiden Bereichen erhebliche Sicherheitslücken. Einhellige Fachmeinung ist, dass es keine anderen Ermittlungsinstrumente gibt, die die fehlenden retrograden Verkehrsdaten im Zeitalter des Internets und der digitalen Kommunikation ersetzen können. Das haben nicht nur die Beschwerdeführer selbst in Karlsruhe vorgetragen, auch das Bundesverfassungsgericht hat dies deutlich zum Ausdruck gebracht.

Angesichts des aus polizeilicher Sicht derzeit untragbaren Zustandes ist der Gesetzgeber gefordert, die Beauskunftung von Verkehrsdaten einer verfassungsgemäßen Regelung zuzuführen. Dabei muss gewährleistet werden, dass die Daten den Sicherheitsbehörden für einen Zeitraum von mindestens sechs Monaten zur Verfügung gestellt werden können.

Sebastian Bukow

Vorratsdatenspeicherung in Deutschland

Symbol des sicherheitspolitischen Wandels und des zivilgesellschaftlichen Protests?

Abstract

Der freiheitliche Rechtsstaat hat sich in den letzten Jahren zum sicherheitsorientierten Präventionsstaat entwickelt, eine neue deutsche Sicherheitsarchitektur entsteht. Diese Veränderungen im Politikfeld Innere Sicherheit werden seit über zehn Jahren höchst kontrovers politisch-medial diskutiert. Besonders umstritten ist dabei die Vorratsdatenspeicherung. Befürworter sehen in ihr ein zentrales Präventions- und Ermittlungsinstrument im digitalen Zeitalter, Kritiker vermuten den staatlichen Generalverdacht und eine vollumfängliche Überwachung. Der Beitrag diskutiert die Bedeutung der Vorratsdatenspeicherung im sicherheitspolitischen Diskurs und stellt die Überlegung in den Mittelpunkt, dass die Vorratsdatenspeicherung vor allem als Symbol des sicherheitspolitischen Paradigmenwandels und des zivilgesellschaftlichen Protests betrachtet werden sollte.

„Interpol und Deutsche Bank, FBI und Scotland Yard,
Flensburg und das BKA haben unsere Daten da."
(Kraftwerk 1981)

1. Einleitung

Der Vormarsch digitaler Kommunikation im alltäglichen Leben ist ein kulturell prägendes, irreversibles Phänomen. Dabei stellt die Zunahme der Internetnutzung – mittlerweile sind ca. 75 Prozent der Bevölkerung „online"[1] – nur einen besonders augenfälligen, allgegenwärtigen Digitalisierungsausschnitt dar. „Die schnelle Entwicklung der Informations- und Kommunikationstechnologien sowie der elektronischen Medien hat gravierende Auswirkungen auf Wirtschaft, Arbeitsmarkt, Gesellschaft, Kultur, Politik und Demokratie." (BT-Drs. 13/11002) Das Spektrum der digitalisierungsbedingten Veränderungen ist sehr weit, zu denken ist etwa an die Verlagerung des Privaten in den digitalen Raum (Social Networks u.ä.) sowie an das Aufkommen digitalen Protests und wiederbelebter Partizipation (Kampagnennetzwerke,

[1] Aktuelle Studien nennen knapp 52 Mio. Internetnutzer in Deutschland (ARD/ZDF 2011), wobei die Abdeckung im Westen höher ist als im Osten (Forschungsgruppe Wahlen 2011). In diesem Zusammenhang wird schon länger eine neue digitale Spaltung der Gesellschaft diskutiert, vgl. dazu bspw. jüngst D21/Infratest (2011). Rund 27 Mio. Deutsche besitzen bspw. ein Online-Profil, auch andere Kommunikationswege werden zunehmend genutzt: 83% aller Deutschen ab 14 Jahren besitzen ein Mobiltelefon und verschickten 2010 rund 80.000 SMS pro Minute, d.h. über 41 Milliarden im Jahr 2010 (BITKOM 2011a, 2011b).

neue Responsivitätsoptionen, Massenpetitionen u.ä.). Der technisch-kommunikative Wandel verändert dabei en passant auch das Verhältnis von Staat und Bevölkerung. Durch die zunehmende Nutzung des digitalen Kommunikations- und Interaktionsraumes wird dieser zu einer quasiöffentlichen und damit auch staatlich relevanten Sphäre, die sich allerdings im transnationalen Netz entwickelt. Diese Überwindung nationaler Kontrollräume führt in Verbindung mit einer veränderten Bedrohungswahrnehmung (insb. „Neuer Terrorismus") zu neuen staatlichen Handlungsmöglichkeiten, -wünschen und -notwendigkeiten, wie etwa die CDU/CSU-Bundestagsfraktion (2011) betont: „Das Internet ist mehr als ein bloßes Medium, es kann ein Raum für bestimmte Bereiche des Zusammenlebens sein. (…) Das Internet ist kein rechtsfreier Raum. Der Staat benötigt effektive Werkzeuge, um Rechtsverstöße im Internet zu unterbinden und zu ahnden". Der Staat ist ganz offensichtlich nicht gewillt, diese neue Arena unbeobachtet und unreguliert zu lassen. Er sucht nach neuen Formen sozialer und rechtlicher Kontrolle: „Die Grundsätze unserer Rechtsordnung müssen auch im Internet gelten." (Uhl 2011; vgl. auch ZDF 2011)

In der Folge verändert sich nationalstaatliches Handeln in einem Kernbereich der Staatstätigkeit – bei der Herstellung und Gewährleistung innerer Sicherheit.[2] Die Digitalisierung und partielle Enträumlichung des Alltagshandelns verändert die sicherheitspolitischen Inhalte und Ziele – und auch das gesamte Politikfeld – nachhaltig. Neue Möglichkeiten des Überwachens und Strafens sind emergent (inhaltliche und strukturelle Telekommunikationsanalysen, Netzzugangssperren, neue Pönalisierung u.ä.) und wirken ins analoge Leben zurück (realweltliche Strafverfolgung, ggf. verändertes Alltagshandeln u.ä.).

In diesem Schnittfeld ist eine der zentralen Debatten im Politikfeld Innere Sicherheit zu sehen – die Debatte um die *Vorratsdatenspeicherung*.[3] Dieses Instrument wird im

[2] Vgl. zur Begriffsgenese, zur normativen Aufladung und zur Frage „innere, Innere oder öffentliche Sicherheit" Bukow (2005b: 43-48).

[3] Der Begriff „*Vorratsdatenspeicherung*" wird bisweilen als politisch-normativ aufgeladen kritisiert. In diesem Beitrag wird der Begriff wertneutral verwendet, zumal auch die Europäische Union von der „Vorratsspeicherung von Daten" spricht und „Anforderungen an die Vorratsdatenspeicherung" formuliert (Richtlinie 2006/24/EG). Bei der Vorratsdatenspeicherung geht es darum, *Mindestfristen für die Speicherung von Telekommunikationsdaten* zu verfügen, um diese Daten für Strafverfolgungszwecke zu verwenden. Die Speicherung erfolgt dabei i.d.R. durch die Telekommunikationsanbieter, die diese im Bedarfsfall den staatlichen Sicherheitsbehörden zur Verfügung stellen. Diese zusätzliche Speicherung wird wichtiger, weil immer weniger Daten zu Abrechnungszwecken gespeichert werden müs-

nachfolgenden Beitrag genauer betrachtet, wobei es als *sicherheitspolitisches Instrument* verstanden und nicht etwa im Bereich *Binnenmarktregulierung* (dazu Abschnitt 4) oder *Netzpolitik*[4] verortet wird. Im Mittelpunkt steht die Überlegung, dass die Vorratsdatenspeicherung vor allem als Symbol des sicherheitspolitischen Wandels und des zivilgesellschaftlichen Protests untersucht werden sollte. Die Vorratsdatenspeicherung steht, so die These, stellvertretend–exemplarisch für die allgemeinen Entwicklungen im Feld der inneren Sicherheitspolitik. Das heißt, die politische Relevanz der Vorratsdatenspeicherung ist auch und gerade jenseits der konkreten Regelungsbereiche begründet – sie ist paradigmatisch und symbolisch von größter Bedeutung.
Bevor auf diese Überlegung weiter eingegangen werden kann, sind nachfolgend zunächst grundlegende politikwissenschaftliche Forschungsperspektiven zur *Inneren Sicherheit* zu skizzieren, um dann die Grundzüge einer *neuen deutschen Sicherheitsarchitektur* aufzuzeigen. Diese dient als Bezugspunkt für die Betrachtung der Vorratsdatenspeicherung, so dass dann die These, dass die Vorratsdatenspeicherung vor allem als Symbol des sicherheitspolitischen Wandels und des zivilgesellschaftlichen Protests untersucht werden sollte, fundiert diskutiert werden kann. Den Abschluss bildet ein Ausblick auf offene Forschungsfragen. Diese Fokussierung führt zwangsläufig zu einer selektiven Analyseperspektive, nur ausgewählte Aspekte der Vorratsdatenspeicherung können thematisiert werden. Damit ist keine Wertung verbunden, weitere Aspekte sind gleichfalls von wissenschaftlicher Relevanz, werden jedoch an anderer Stelle diskutiert (vgl. die Beiträge in diesem Band sowie bspw. Szuba 2011).[5]

---

sen (z.B. bei Flatrate-/Prepaid-Tarifen, bei eingehenden Verbindungen, weitere Informationen) – nur die additive Speicherung erhält damit diese Daten für weitere Analysezwecke seitens der Sicherheitsbehörden. Alternativ wird – vor allem von Befürwortern – der Begriff „*Mindestspeicherfristen*" verwendet. Diese Formulierung findet sich bereits in den frühen Versuchen, eine derartige Regelung einzuführen, bspw. seitens des Bundesrats (z.B. 1996, BRat-Drs. 80/96: 48).

[4] Dies wäre sinnvoll, wenn der Analysefokus auf den Bereich Online-Kommunikation gerichtet und das Instrument bspw. analog zur Debatte um Internetsperren u.ä. diskutiert werden soll. Diese verengte Perspektive vernachlässigt jedoch den ebenfalls betroffenen Bereich der Telefonkommunikation und damit verbundene Rückwirkungen auf das Alltagshandeln.

[5] Es unterbleibt z.B. eine tief greifende rechtswissenschaftliche Betrachtung (u.a. Zulässigkeit und verfassungsrechtliche Hürden) ebenso wie eine politische oder kriminologische Bewertung der Vorratsdatenspeicherung (bspw. Erforderlichkeit, Verhältnismäßigkeit, Wirkung, Wert des Instruments) - wobei letztere Aspekte mit Blick auf die Nichtverfügbarkeit valider Daten (und in Folge des Naturells der zu bekämpfenden Straftatbestände im Bereich der Gefahrenabwehr) generell nicht vollumfänglich empirisch untersucht werden können.

2. Politikwissenschaftliche Perspektiven auf die Innere Sicherheit

Angesichts der das Feld prägenden Begriffsunbestimmtheit ist zu Beginn zu präzisieren, was unter dem *Politikfeld Innere Sicherheit* verstanden wird bzw. hier verstanden werden soll, schließlich gibt es keine eindeutige Definition bzw. kein einheitliches Verständnis davon, was in das Politikfeld einzubeziehen ist und wo eine Feldbegrenzung zu ziehen ist. Diese Unschärfe des Sicherheitsbegriffs ist für eine ausgreifende politische Argumentation vorteilhaft, wie die Forschung zur Versicherheitlichung („Securitization"; v.a. Forschungsfeld Internationale Beziehungen) verdeutlicht. Sicherheit wird hier nicht mehr als objektiv messbar verstanden, sondern als Sprechakt gedeutet, wobei „Sicherheit" im politischen Gebrauch sehr unbestimmt sein kann: „(…) given the political function of the word security, the wider agenda extends the call for state mobilization to a broad range of issues." (Buzan et al. 1998: 4) Durch die Versicherheitlichung eines Themas wird dabei einer Sache besonderes Gewicht verliehen:

> „In security discourse, an issue is dramatized and presented as an issue of supreme priority; thus, by labeling it as security, an agent claims a need for and a right to threat it by extraordinary means. (…) the task is not to assess some objective threats that "really" endanger some object to be defended or secured; rather it is to understand the process of constructing a shared understanding of what is to be considered and collectively responded to as a threat." (Buzan et al. 1998: 26)

Das heißt, es ergibt sich so die Möglichkeit, Politikbereiche und Handlungsinteressen als sicherheitsrelevante (und damit ggf. alternativlose) Handlungserfordernisse darzustellen, durch- und umzusetzen. Forschungstechnisch gesehen ist die Begriffsunbestimmtheit ungünstig, es besteht das Problem, dass der Forschungsgegenstand im Ungefähren verbleibt. Wie kann man sich also dem *Politikfeld Innere Sicherheit* theoretisch-konzeptionell annähern?

Betrachtet man zunächst nur die politisch-mediale Debatte, so gehört Sicherheitspolitik – hinsichtlich der inneren und vor allem der äußeren Sicherheit, soweit diese noch trennbar sind (zur Auflösung der Grenzen zwischen innerer und äußerer Sicherheit bspw. Glaeßner 2003: 145-148; aktuelle Verflechtungstendenzen vgl. Werkner 2011) – nicht unbedingt zu den zentralen Debatten, insbesondere eine Debatte über den strategischen Rahmen, über präferierte Politikansätze und Instrumente ist eher eine Eliten- bzw. Expertenveranstaltung, wie Böckenförde/Gareis (2009: 7) betonen. Gleich-

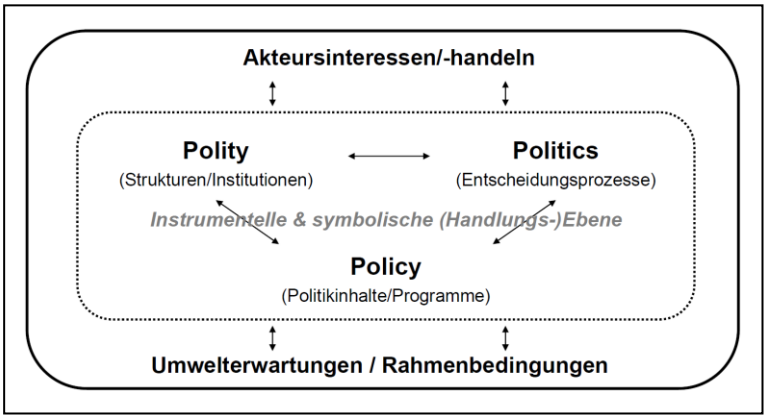
wohl findet der Diskurs um die *Innere Sicherheit* seit einigen Jahrzehnten sehr regelmäßig einen breiten medial-öffentlichen Widerhall. Die Debatte entzündet sich meist an konkreten Anlässen und Policy-Aspekten – im Zentrum stehen inhaltliche Fragen etwa nach der materiellen Rechtsausgestaltung einzelner Maßnahmen oder der Einführung neuer Instrumente und Straftatbestände. Seltener sind Diskussionen um Organisations- und Strukturfragen, doch auch diese gibt es und sie sind nicht weniger kontrovers, wie die (zwischenzeitlich ausgesetzte) Debatte um die Reform der Bundespolizei und deren Zusammenlegung mit dem Bundeskriminalamt gezeigt hat (sog. Werthebachkommission, vgl. Kommission "Evaluierung Sicherheitsbehörden" 2010; DPolG 2010; Funk 2010a, 2010b). Nur in seltenen Fällen, meist anhand konkreter Ereignisse, wird in einer breiteren Öffentlichkeit die Frage nach der Verbesserung von sicherheitspolitischen, sozusagen netzwerkinternen Prozessen gestellt – was auch daran liegt, dass sich die konkreten Prozesse und Strukturen der breiteren Öffentlichkeit kaum erschließen.

In einer wissenschaftlichen Betrachtungsweise ist ein Politikfeld zunächst ganz allgemein als Teilbereich des Politischen Systems zu verstehen, wobei an dieser Stelle kein streng systemtheoretischer Systembegriff zu Grunde gelegt wird. Fokussiert man auf das Politikfeld Innere Sicherheit, so finden sich in der Literatur je nach Analyseperspektive bzw. Erkenntnisinteresse unterschiedlichste Forschungsansätze bzw. theoretische Bezugspunkte (u.a. institutionen-, akteurs-, handlungs-, system- & integrationstheoretische Bezüge). Das Politikfeld stellt dabei ein komplexes Teilsystem dar, für dessen fundierte Analyse unterschiedlichste Aspekte und Dimensionen von Interesse sein können und miteinander zu verbinden sind: Strukturen und Institutionen (Polity), Entscheidungsprozesse (Politics) sowie materielle Politikinhalte bzw. Programme (Policy) spielen ebenso eine Rolle wie die (meist kollektiven) handelnden Akteure selbst (die gerade für die Politikfeldgestaltung eine herausragende Bedeutung einnehmen (vgl. zu diesen Aspekten u.a. Lange 1999, 2006).

Mit Blick auf die hier herauszuarbeitenden Überlegungen sind vor allem neoinstitutionalistische Überlegungen relevant, weisen diese doch darauf hin, dass in vielen Bereichen nicht nur funktionale (Organisations-)Erwartungen das Feld prägen, sondern auch gesellschaftlich-normative Vorstellungen Einfluss darauf haben,

wie bspw. (semi-)öffentliche Institutionen organisiert werden. Übertragen auf das Politikfeld Innere Sicherheit heißt dies, dass neben dem Akteurshandeln auch gesellschaftlich-normative Erwartungen die Politikfeldgestaltung prägen und dementsprechend zu berücksichtigen sind. In der Fortführung dieser Überlegung ist davon auszugehen, dass die Politikfeldgestaltung neben einer materiellen Komponente, welche auf die instrumentelle Zielsetzung abstellt, auch eine symbolische Komponente enthält (vgl. Schulte 2008: 225-226; allg. Hitzler 1998). Abbildung 1 verdeutlicht diesen Zusammenhang bzw. skizziert den Rahmen, innerhalb dessen die Politik der Inneren Sicherheit betrieben und gestaltet wird.

Abbildung 1: Analyseaspekte im Politikfeld Innere Sicherheit



Damit ist der Handlungsrahmen skizziert, innerhalb dessen die Politikgestaltung darauf ausgerichtet ist, innere Sicherheit herzustellen und zu gewährleisten. Dieses Sicherheitsversprechen ist von grundlegender Bedeutung für den (national-)staatlichen Machtanspruch und die damit verknüpfte Inanspruchnahme des Gewaltmonopols.[6] Staatliches Handeln in diesem Politikfeld zielt dabei vorrangig auf die innerstaatliche Ausübung öffentlicher Gewalt im Rahmen des Rechts zur Sicherstellung der verfassten Ordnung und der Gewährleistung von nicht nur körperlicher Sicherheit innerhalb des Staatsgebietes. Denn auch wenn in der öffentlichen Debatte oft ein anderer Eindruck entsteht: Innere Sicherheit ist mehr als die Bekämpfung von organisierter Kriminalität oder Terrorismus, innere Sicherheit erfasst bspw. auch die alltägliche Sicherheit vor (einfacher) Kriminalität und die Aufrechterhaltung der öffentlichen Ordnung.

[6] Gerade im politischen Diskurs ist nicht nur die objektive Sicherheitslage Ziel des Sicherheitsversprechens, sondern auch das subjektive Sicherheitsgefühl. Lage und Gefühl sind mitnichten deckungs-

Keineswegs selbstverständlich ist, dass hierbei der moderne Staat als einzig legitimer Sicherheitsgarant auftritt. Im internationalen Vergleich ist erkennbar, dass das Verständnis von *Innerer Sicherheit* stark differiert und damit auch das Verständnis davon, wer für die Sicherheitsgewährleistung zuständig bzw. verantwortlich ist. Handelt es sich um eine vorrangig oder gar ausschließliche Staatsaufgabe, oder ist nicht auch die Gesellschaft selbst für ihre Sicherheit mitverantwortlich, und welche Rolle spielt hierbei die lokale bzw. kommunale Ebene? Für den hier interessierenden Fall Deutschland ist eine seit dem Kaiserreich tief in der deutschen Staatstradition verwurzelte Staatsorientierung zu konstatieren. Versuche der Alliierten (in der britischen und amerikanischen Besatzungszone), nach 1945 einen kulturell-strukturellen Wandel herbeizuführen und nach angloamerikanischem Vorbild Sicherheitsleistungen (auch) als gesellschaftliche Aufgabe (etwa über kommunal finanzierte Polizeikräfte) zu etablieren, blieben weitgehend erfolglos (Lange 2006: 90-91; Lange/Frevel 2009: 115-116). Spätestens in den 1970ern ging der Trend wieder klar zur staatlichen Sicherheitsgewährleistung, erste Kompetenzerweiterungen für die staatliche Polizei im Zuge der innerdeutschen Terrorismusbekämpfung waren die Folge (vgl. Lange 2006: 90). In Verbindung mit den föderalstaatlichen Strukturen überrascht es daher nicht, dass in Deutschland konservativ gezählt rund 40 Akteure auf Bundes- und Landesebene mit-, neben- und auch gegeneinander agieren, um die innere Sicherheit zu gewährleisten (vgl. bspw. Möllers 2009; Lange/Frevel 2009; Bukow 2009). Allein diese Zahl macht deutlich, dass es sich hier um ein hochkomplexes (und zudem exekutivlastiges) Mehrebenensystem handelt.

Die in Deutschland so dominante Staatsnähe jedweder Politik der inneren Sicherheit bringt es mit sich, dass die Frage nach der *Inneren Sicherheit* stets auch das Verhältnis von Staat und Bürger (bzw. Gesellschaft) berührt, wobei im deutschen Fall ein starker Staat meist mit einem starken Sicherheitsgaranten gleichgesetzt wird. Schon aus diesem Grund prägt bis heute der Dualismus Staat vs. Gesellschaft das Akteurshandeln in diesem Kernbereich nationalstaatlichen Handelns, eine Koopera-

---

gleich, oftmals bestehen große Unterschiede (bspw. faktische Gefährdung vs. Gefährdungswahrnehmung durch Terroranschlag/Straßenverkehr oder im Bereich der Jugendkriminalität, zu letzterem Pfeiffer 2011). Es gilt: „Innere Sicherheit [ist] nicht nur etwas, was objektiv festgestellt oder gewährleistet werden kann oder sollte, sondern sie ist ein *Konstrukt, das wesentlich von der individuellen Gefühlswelt der Bürger definiert* wird" (Feltes 2009: 106).

tion zwischen staatlichen und zivilgesellschaftlichen Akteuren findet kaum statt, obwohl die innere Sicherheit, so die aktuelle Forschung, stark vom „Engagement der Bürger und der lokalen Nachbarschaft" abhängt (Feltes 2009: 106).[7] Dieser Dualismus „Staat vs. Zivilgesellschaft" ist ein Grund dafür, dass in Deutschland der Begriff *Innere Sicherheit* hochgradig normativ aufgeladen ist. Dazu hat aber auch die Begriffsgenese selbst beigetragen (vgl. Bukow 2005b: 43-48): Der in den 1960ern aufkommende, vom Innenministerium etablierte Begriff wurde und wird oft als „Kampf-Erklärung" (Lange 1999: 108) des Staates an die bürgerlichen Freiheitsrechte verstanden. Bis heute ist das Feld eines der ideologisch am stärksten aufgeladenen Politikfelder, und dies in Zeiten, in denen andere polarisierende Großkonflikte zunehmend beigelegt werden (wie jüngst der Atomkonflikt). Diese normativ-ideologische Aufladung und die damit verbundene Polarisierung prägen den politischen Diskurs und das Politikfeld selbst. Und selbst die wissenschaftliche Forschung kann sich hier nicht immer völlig lösen: Interessenkonflikte sind nicht ausgeschlossen, wenn etwa Wissenschaftler nicht nur in diesem Themenfeld forschen, sondern zugleich in Beratungstätigkeiten involviert sind und dabei für am Politikgestaltungsprozess beteiligte Akteure Position ergreifen.

Prägend für das Politikfeld Innere Sicherheit ist, dass die politischen Konfliktlinien in diesem Feld quer zu den etablierten Koalitions- bzw. Lagerstrukturen verlaufen. Es stehen sich gerade nicht die traditionellen Lager (links/rechts bzw. rot/grün vs. schwarz/gelb), sondern eine faktische Große Koalition der Inneren Sicherheit (CDU/CSU und SPD) und eine faktische Allianz[8] der „Bürgerrechtsparteien" (v.a. Grüne und FDP) mehr oder minder unversöhnlich gegenüber (Bukow 2009: 350; Kutscha 1998). Diese (im Bund meist) regierungskoalitionsinterne Konfliktstrukturierung trägt ebenfalls dazu bei, dass sicherheitspolitische Debatten oft sehr umfassend geführt werden – denn hier bietet sich dem kleinen Koalitionspartner oftmals die Möglichkeit der (koalitionstechnisch legitimen) Profilierung.

[7] Ergänzend sei daran erinnert, dass private Sicherheitsdienstleister auch im (semi-)öffentlichen Raum (in Kaufhäusern, im öffentlichen Nahverkehr usw.) zuletzt stark an Bedeutung gewinnen. Auch ist an die Rolle privater Unternehmen etwa im Bereich der Datenspeicherung zu erinnern, dazu kommt bisweilen die Forderung nach Bürgerwehren als Beitrag zu einer neuen lokal-kommunalen Sicherheitspartnerschaft (vgl. Berliner Morgenpost 2011).

[8] Dies bezieht sich nur auf die inhaltliche Nähe von Grünen und FDP in diesem Politikfeld, aus Wettbewerbsgründen findet eine allzu enge Kooperation dieser Parteien in diesem Bereich nicht statt.

Fasst man diese knappe Betrachtung des Politikfelds Innere Sicherheit zusammen, so sind drei wesentliche Aspekte festzuhalten: Erstens ist zu bedenken, dass das Feld stark durch die (sicherheitsproduzierenden) Akteure bzw. deren Akteursnetzwerke geprägt ist. Daher ist hinsichtlich der sicherheitspolitischen Entwicklung der Blick auf Akteursinteressen, aber auch auf gesellschaftlich-kulturelle Erwartungen und Paradigmen, die auf die Akteure einwirken, zu richten. Zweitens handelt es sich um ein komplexes und vielschichtiges Feld, weshalb sich in der Forschung je nach Erkenntnisinteresse unterschiedliche Analyseperspektiven und differente theoretische Zugänge finden – zu nennen sind insbesondere politisch-normative (Freiheit vs. Sicherheit), verwaltungswissenschaftliche (Institutionenentwicklung, bspw. Polizeiorganisation) wie vor allem rechtswissenschaftliche (Policy- und Gesetzesanalyse) Arbeiten. In diesem Zusammenhang wird oftmals auf einen Gegensatz von Freiheit und Sicherheit abgestellt, beide werden jeweils als Endpunkte einer Achse verstanden. Prägend ist in diesem Zusammenhang die Konstruktion eines „Grundrechts auf Sicherheit" (Isensee 1983), das sich nach Isensee als Gegenpol zur verfassungsrechtlich eindeutig verankerten freiheitsrechtlichen Dimension aus dem Grundgesetz ebenfalls ableiten lässt und damit etwa im (verfassungs-)rechtlichen Abwägungsprozess sicherheitspolitischer Maßnahmen eine Rolle spielt. In der neueren Literatur wird einer dualistischen Annahme („Sicherheit vs. Freiheit") aber auch widersprochen, beide Aspekte werden eng miteinander verbunden und gerade nicht konfligierend verstanden („Sicherheit in Freiheit", Glaeßner 2003). Drittens ist stets zu beachten, dass gerade in Deutschland die *Innere Sicherheit* ein hochgradig normativ durchwirktes Feld ist – die medial-politischen Debatten verlaufen oft nach einem reflexbehafteten, stark polarisierenden Freund-Feind-Schema. Eine distanziert-sachliche Debatte ist nicht immer gegeben.

3. Die neue deutsche Sicherheitsarchitektur

3.1 Zwei Dekaden ‚Sicherheitspolitik im Wandel'

Die Politik der inneren Sicherheit hat sich in den letzten 20 Jahren stark verändert. Dieser Veränderungsprozess hat seinen Ausgangspunkt bereits vor dem Fall des Eisernen Vorhangs, erste konzeptionelle Überlegungen datieren in die späten 1980er

Jahre. Durchsetzungsrelevant sind gleichwohl zunächst die Integrationsentwicklungen der 1990er Jahre. Eine massive Beschleunigung des Wandels bewirkten die terroristischen Anschläge in den USA 2001. Die 9/11-Anschläge sowie die nachfolgenden Anschläge (u.a. Madrid, London) hatten in diesem Transformationsprozess vor allem eine katalytische Wirkung als „exogener Verstärker" (Lange 2006: 98). Denn erst diese medial omnipräsenten, nunmehr im kollektiven Gedächtnis fest verankerten Anschläge haben in vorher nicht erahnter Weise ein Durchsetzungsfenster für neue sicherheitspolitische Maßnahmen geöffnet, das bis heute nicht wieder geschlossen wurde. Insbesondere der 11. September 2001 dominiert seitdem die (innerdeutsche) sicherheitspolitische Debatte und wirkt – ganz im Sinne einer Versicherheitlichung – weit in nur bedingt verwandte Politikfelder wie bspw. die Asyl- und Migrationspolitik hinein.

Die deutschen sicherheitspolitischen Gesetzgebungsrunden nach 9/11 sind in der rechts- und politikwissenschaftlichen Forschung breit thematisiert und kritisiert worden (u.a. Ambos 2006; Lange/Frevel 2009; Bukow 2005a; Haubrich 2005; Lepsius 2004, 2006), weshalb hier nur drei zentrale Befunde anzuführen sind. Erstens ist festzuhalten, dass es sich in vielen Punkten um eine Ausweitung konzeptionell bereits bekannter Ermittlungsinstrumente handelt, d.h. viele der Maßnahmen, die nach 9/11 umgesetzt wurden, waren schon zuvor geplant (bspw. die Abschaffung des Religionsprivilegs (§ 2 Vereinsgesetz) oder die Strafbarkeit der Bildung von beziehungsweise die Mitgliedschaft in einer terroristischen Vereinigung im Ausland (§129b StGB)). Damit steht zweitens in Verbindung, dass viele der „neuen" Instrumente schon aus den 1970er-Jahren bekannt und rechtlich etabliert sind. Damals galt es, den innerdeutschen Linksterrorismus (und später die organisierte Kriminalität) zu bekämpfen, heute soll mit denselben umgewidmeten bzw. hinsichtlich der Anwendungszulässigkeit ausgeweiteten Instrumenten der transnationale Terrorismus bekämpft werden, wobei fraglich ist, in wie weit diese Instrumente tatsächlich geeignet sind. Drittens ist zu betonen, dass insbesondere diejenigen Gesetzesänderungen, die die Kompetenzen der Sicherheitsbehörden massiv ausgeweitet haben, von größter Bedeutung sind, da hier – mehr oder weniger verdeckt – das sicherheitspolitische Institutionensystem in seinen Grundzügen verändert wurde. Diese Maßnahmen und

die damit verbundenen institutionellen Veränderungen haben das deutsche Gefüge im Politikfeld Innere Sicherheit nicht nur der neuen Zeit angepasst, sondern grundlegend verändert. Daher ist es mittlerweile angebracht, von einer „neuen deutschen Sicherheitsarchitektur" zu sprechen, wie sie erstmals (damals noch wenig erfolgreich) der damalige Innenminister Schily gefordert hat (vgl. bspw. RP Online 2004).

3.2 Grundzüge einer neuen deutschen Sicherheitsarchitektur

Doch was genau ist, bezogen auf den Bereich der Inneren Sicherheit, neu an der *neuen deutschen Sicherheitsarchitektur*? Vier Merkmale sind zu benennen, die in Abgrenzung zum alten bundesrepublikanischen Modell den in den 1990ern beginnenden Wandel und die daraus resultierenden Konsequenzen für das Politikfeld Innere Sicherheit verdeutlichen (vgl. auch Bukow 2008, 2009).

(1) In einer Institutionenperspektive ist das erste wesentliche Merkmal die umfassende *Neudefinition institutioneller Aufgaben* bzw. Zuständigkeiten bis hin zur Neuausrichtung einzelner Sicherheitsproduzenten, womit teilweise erweiterte Ermittlungsbefugnisse einhergehen. Beispielhaft zu nennen ist etwa die Stärkung des Bundeskriminalamtes. Das ehemals nur zusammenführend-koordinierende Amt ist nunmehr in spezifischen Teilbereichen (insb. der Bekämpfung des internationalen Terrorismus) faktisch eine echte Bundeskriminalpolizei mit eigenen präventiv-ermittlungspolizeilichen Kompetenzen (Art. 73 I Nr. 9a GG). Mit dieser Neuausrichtung, die im Zuge der Föderalismusreform I ermöglicht und grundgesetzlich festgeschrieben wurde, wird die tradierte föderale Ordnung durchbrochen, waren doch derartige polizeiliche Aufgaben zuvor eine ausschließliche Länderangelegenheit. Wegweisend ist in diesem Zusammenhang zudem der weitgehend abgeschlossene Reorganisationsprozess des früheren Bundesgrenzschutzes zu einer nun im Inland operierenden Bundespolizei. Dieser Wandlungsprozess ist nicht nur institutionell von Bedeutung, sondern weist auch auf die neue Präventionsorientierung hin, die in enger Verbindung mit dem Reorganisationsprozess steht. In Zeiten des Grenzschutzes bestand lange Zeit eine direkte Verknüpfung von Anlass (Grenzübertritt) und polizeilicher Handlung (Kontrolle). Mit der Europäischen Integration, dem Wegfall der Grenzkontrollen und der Umwidmung des Bundesgrenzschutzes zu einer im

Inland operierenden bundeseigenen Polizei wurde dieser Zusammenhang entkoppelt – erstmals wurden in größerem Umfang anlassunabhängige Kontrollen ermöglicht, was nichts anderes heißt als dass präventiv und verdachtsunabhängig polizeiliche Kontrollmaßnahmen durchgeführt werden. Genau diese Entkopplung spielt in einem präventionsorientierten Sicherheitsmodell eine fundamentale Rolle.

(2) Die beiden nächsten anzusprechenden Veränderungen sind erkennbar, wenn man die einzelinstitutionellen Veränderungen im Gesamtverbund betrachtet, also eine Systemperspektive einnimmt. Zunächst ist diesbezüglich eine deutlich *verstärkte nationale Kooperation und informationelle Zusammenführung der Sicherheitsbehörden* zu nennen. Dazu wurde etwa das Gemeinsame Terrorismusabwehrzentrum (GTAZ, seit 2004) in Berlin eingerichtet und die dort angesiedelte Anti-Terror-Datei (seit 2007 im Einsatz) eingeführt. Diese doppelte Vernetzung – zwischen den verschiedenen Ebenen und zwischen den polizeilichen und nachrichtendienstlichen Akteuren – wird zu Teilen sehr kritisch diskutiert: Insbesondere wird die Gefahr gesehen, dass mit der zunehmenden Vernetzung das in Deutschland nach überwiegender Meinung verfassungsrechtlich festgeschriebene innerstaatliche Trennungsgebot von Polizeien und Nachrichtendiensten durchlöchert bzw. unterminiert wird (bspw. Gusy/Pohlmann 2007). In den Bereich der technisch-informationellen Zusammenarbeit fallen jedoch auch weitere Aspekte wie das Projekt „Reengineering der Plattformen Innere Sicherheit" (RISP) zur Verbesserung der Interoperabilität von Datenbanksystemen im Bereich der Inneren Sicherheit (dazu BT-Drs. 16/9987).

(3) Nicht nur die zunehmende Vernetzung verändert die Sicherheitsarchitektur des Landes auf der Systemebene, es findet damit verknüpft auch eine faktische und formalrechtliche Stärkung der bundesstaatlichen Ebene statt. Diese *fortschreitende Zentralisierung* durchbricht die traditionell dezentral-föderale Sicherheitsarchitektur. Diese innerstaatliche Machtverschiebung erfolgt einerseits über die Neuausrichtung der bundeseigenen Sicherheitsakteure und andererseits über die nunmehr (auch) zentral direkt verfügbaren Datenbestände. Bemerkenswert ist hierbei, dass (vor allem medial) vorrangig die Risiken einer solchen Zentralisierung, nicht jedoch die Chance auf eine verbesserte Transparenz und Datenkontrolle, die sich durch die Zentralisierung ebenfalls ergeben könnte, diskutiert werden.

(4) In Zeiten einer fortschreitenden Europäischen Integration und einer nicht mehr rein nationalstaatlichen Bedrohung der Inneren Sicherheit durch internationale Kriminalität und transnationalen Terrorismus ist viertens auch eine *verstärkte internationale Kooperation* der deutschen Sicherheitsproduzenten mit ausländischen Sicherheitsinstitutionen feststellbar – vor allem, aber nicht nur, im innereuropäischen Raum. Innere Sicherheitspolitik gleicht damit immer stärker einer „Innenpolitik in Europa" (Bundesministerium des Innern 2004: 4), die verfassungsrechtlich fixierten Grenzen von innerer und äußerer Sicherheit verschwimmen. Hinter dieser nationalstaatlichen Entgrenzung der inneren Sicherheit sind mehrere Prozesse verborgen, etwa eine fortschreitende Integration einzelner Handlungsfelder (insb. im Bereich Migrations- und Rechtspolitik), mit der auch der Aufbau neuer europäischer Institutionen bzw. Agenturen verbunden ist. Gerade für die EU-Ebene ist der mit Amsterdam beschlossene „Raum der Freiheit, der Sicherheit und des Rechts" von Bedeutung, wobei in jüngster Zeit eine Dominanz der Sicherheit vor dem Recht konstatiert werden kann. Zu konstatieren ist darüber hinaus eine (im Ausmaß landesspezifisch unterschiedliche) Europäisierung der Inneren Sicherheit (vgl. Glaeßner/Lorenz 2005) sowie eine Verlagerung der innenpolitischen Entscheidungsarenen in den europäischen Raum, bspw. um über den Umweg Europa innenpolitisch streitige Maßnahmen durchzusetzen (bspw. biometrische Ausweispapiere). Deutschland tritt dabei gerade im Politikfeld Innere Sicherheit als starker und klar interessengeleiteter Akteur auf.

Ursächlich für die *neue deutsche Sicherheitsarchitektur* sind unterschiedliche Gründe. Zu nennen sind die eingangs bereits ausgeführten neuen technologischen Möglichkeiten im Zuge der informationellen Revolution. Die Entstehung des Cyberspace stellt den Staat vor neue Herausforderungen: Zum einen entsteht ein neuer Kommunikationsraum und zum anderen ergibt sich die Möglichkeit, in diesem neuen Raum „neue" Straftaten zu begehen. Zugleich werden neue (teils automatisierbare/-te) Ermittlungs- und Überwachungsverfahren und Erkenntnisse möglich, die weit über das analoge Beobachten hinausgehen und gerade im Bereich der Prävention als hilfreich erachtet werden, was seitens der Sicherheitsakteure Begehrlichkeiten weckt.

Möglicherweise entscheidender für die Reorganisation der Sicherheitsarchitektur dürfte jedoch die zunehmend als hinderlich wahrgenommene Fragmentierung der deutschen Sicherheitslandschaft sein, die gerade mit Blick auf die als verändert wahrgenommene Bedrohungslage als nicht mehr zeitgemäß diskreditiert wird. Schließlich haben sich die sicherheitspolitischen Rahmenbedingungen grundlegend geändert, neben der Europäischen Integration sind das Ende des Ost/West-Konfliktes und die Omnipräsenz des *Neuen* Terrorismus zu nennen. Gerade aus den veränderten Rahmenbedingungen resultieren für die Sicherheitsakteure neue Interessenlagen und Notwendigkeiten, die über die verbesserte Sicherheitsproduktion hinausgehen. So stellt sich durch den externen Wandel teilweise die Frage des Institutionenerhalts (bspw. Bundesgrenzschutz wird Bundespolizei als Reaktion auf den Wegfall der Binnengrenzen). Zudem ist eine Veränderung in der Mehrebenenarithmetik feststellbar, schließlich tritt mit der Europäischen Union ein neuer, gewichtiger Spieler in das bislang innenpolitisch-föderal geprägte Netzwerk ein. Auch deshalb hat der Bundesstaat ein zunehmendes Interesse an einer Zentralisierung spezifischer Ressourcen, um hier bspw. mit den europäischen Partnern besser interagieren zu können. Festzuhalten ist an dieser Stelle, dass die Entwicklungen hin zu einer neuen deutschen Sicherheitsarchitektur nicht immer funktional erforderlich oder gar alternativlos waren bzw. sind. Es handelt sich vielmehr um eine Mischung aus verschiedenen politisch für erforderlich gehaltenen (und empirisch nicht immer nachgewiesenen) Notwendigkeiten, politischen Handlungslogiken, von Institutionen- und Akteursinteressen sowie einer politisch-institutionellen Reaktion auf gesellschaftlich-normative Erwartungen. Gerade in diesem Kontext ist bedeutsam, dass der Neue Terrorismus nicht nur als reale Bedrohung eine sicherheitspolitische Reaktion erforderte, sondern auch als Narrativ der Legitimation neuer Gesetze dient.

3.3 Der sicherheitsorientierte Präventionsstaat

Die institutionell-architektonische Neugestaltung geht mit einem normativ-paradigmatischen Wandel einher. In der wissenschaftlichen Literatur wird eine Transformation des freiheitlichen Rechtsstaates hin zum sicherheitsorientierten Präventionsstaat diskutiert, wobei die Gesetzgebung der letzten zehn Jahre eine klare

Verschiebung der Grenzen des Rechtsstaates erkennen lässt: Zu Gunsten der Sicherheit wird auf Kosten der Freiheit der Rechtsstaat beschnitten (zur Debatte u.a. Huster/Rudolph 2008; Gusy/Pohlmann 2007; Klingst 2007; Gusy 2007; Graulich 2007; Bukow 2009). Auch wenn Befürworter einer Sicherheitsorientierung Freiheitsrechte bereits als „Mode" diskreditieren, die übermäßig „in den Vordergrund" gestellt würden (so bspw. Siegfried Kauder, Vorsitzender des Rechtsausschusses des Deutschen Bundestages, vgl. ZDF 2011) - bei einer genaueren Analyse wird die politisch intendierte Hinwendung zum Präventionsstaat gleichwohl deutlich, wobei zwei Grundtendenzen aufscheinen: eine substanzielle Erosion des Rechtsstaates und ein Paradigmenwandel im staatlichen Bürger-/Bevölkerungsverständnis.

Zur Gefahr einer fortschreitenden Erosion des Rechtsstaates finden sich in der Literatur zahlreiche Einzelbefunde (u.a. Klingst 2007; Gusy 2007; Kutscha 2003, 2008). Neben der Aufweichung bzw. Durchbrechung des Trennungsgebots wird das verfassungsgerichtlich entwickelte Grundrecht auf informationelle Selbstbestimmung als zunehmend gefährdet erachtet, darauf deutet auch die Argumentation Kauders hin, in deren Konsequenz Freiheitsrechte eher als nachrangige „Luxusrechte" zu deuten wären. Weitere Problemlagen für den freiheitlichen Rechtsstaat ergeben sich aus der bis dato nicht abschließend geklärten Frage der Zulässigkeit von so genannten „verschärften Verhörmethoden", also der Folteranwendung. Dabei ist die staatliche Anwendung von Folter für die deutschen Sicherheitsproduzenten keine Problemlage, Folter ist eindeutig unzulässig (zur Debatte um die "Rettungsfolter" bspw. Kutscha 2008), auch wenn Vorschläge unterbreitet wurden, sie in Extremsituationen für zulässig zu erklären (so etwa Brugger 2004). Problematisch wird es im deutschen Fall in der Frage der Informationsverwertung von aus Folter gewonnenen, sicherheitsrelevanten Informationen. Dieses Problem verschärft sich insbesondere durch die zunehmende Vernetzung der deutschen Sicherheitsproduzenten mit anderen, bspw. US-amerikanischen Nachrichtendiensten. Der Rechtsstaat gerät hier in die Gefahr, über die Hintertür unzulässig erlangte Informationen zumindest zur Gefahrenabwehr zu nutzen bzw. nutzen zu müssen (zu diesem Ansinnen bspw. Spiegel Online 2005). Rechtsstaatlich fragwürdig sind zudem die so genannten „Terrorlisten" der Europäischen Union und der Vereinten Nationen, die im Zuge des Anti-Terror-

Kampfes eingeführt wurden (vgl. bspw. Schulte 2010). Ohne rechtsstaatlichen Standards zu genügen greifen diese Listen tief in die Freiheits- und Persönlichkeitsrechte der betroffen Personen und Organisationen ein. Dabei werden die Betroffenen weder umfassend informiert noch finden sie rechtliches Gehör (vgl. Art. 103 I GG; §§ 33, 33a StPO), da eine rechtsstaatliche Kontrolle bzw. Überprüfung faktisch nicht vorgesehen ist. Die „Verurteilung" erfolgt quasi auf dem Dienstweg, und dies bei einer Wirkung, die Europarats-Ermittler Dick Marty als „zivile Todesstrafe" bewertet (vgl. bspw. Kruse 2007). Auch in anderen Fällen wirke sich die Terrorismusbekämpfung bereits „negativ auf die Chancen für ein faires Verfahren aus" (Heinz 2004: 38). Es zeigt sich, dass die westlichen Rechtsstaaten bereits erste Defekte aufweisen, wenn nämlich (vermeintlichen) „Systemfeinden" rechtsstaatliche Fundamentalrechte verweigert werden bzw. sogar explizit noch weitergehend verweigert werden sollen. In diese Richtung zielen Überlegungen, die im Rahmen der Debatte um ein „Feindstrafrecht" kontrovers diskutiert werden (u.a. Jakobs 2004; Uwer 2006).

Nicht nur die fortschreitende Erosion des Rechtsstaates wird als Folge eines sicherheitsorientierten Präventionsstaates diskutiert, sondern auch eine mit der Präventionsorientierung zusammenhängende veränderte Sicht des Staates auf seine Bürger bzw. seine Bevölkerung. Man kann in diesem Zusammenhang von einem normativen und technisch umgesetzten Ende der Unschuldsvermutung in Zeiten des homegrown terrorism sprechen. Diese Neubewertung der Bevölkerung ist aus Sicht des zur Sicherheitsgewährleistung verpflichteten Staates nachvollziehbar, ist es doch gerade ein kennzeichnendes Merkmal der „neuen Terroristen", bis zur (einmaligen) Terrortat als unauffällige „Schläfer" nicht ins Fahndungsraster zu geraten. Ein deutliches Indiz für diese (überspitzt formuliert) „Normalisierung des Generalverdachts" mit dem Ziel der (Terrorismus-)Prävention ist die umfassende Ermöglichung bzw. der Einsatz verdeckter, teilweise anlassunabhängiger Überwachungs- und Ermittlungsstrategien/-instrumente. Letztlich stellt sich mit der Orientierung hin zum Präventionsstaat die Frage, wie weit das Sicherheitsversprechen des Staates noch reicht (vgl. Bull 2007) und wie viel (gefühlte) Unsicherheit die freiheitliche Demokratie erträgt.

In diesem Diskurs und in dieser Abwägungslage ist die hochgradig polarisierte und ideologisch aufgeladene Debatte um die Vorratsdatenspeicherung zu sehen. Am Fallbeispiel „Vorratsdatenspeicherung" werden die beschriebenen Politikfeld-Entwicklungslinien bzw. die paradigmatische Neuausrichtung besonders deutlich, die Vorratsdatenspeicherung steht quasi stellvertretend für die mit der neuen deutschen Sicherheitsstruktur einhergehenden Veränderungen und symbolisiert wie kein anderes Ermittlungs(ermöglichungs)instrument das (neue) Überwachungspotenzial – nicht die tatsächliche Überwachung – eines präventionsorientierten Staates. Dadurch ist die Vorratsdatenspeicherung zu einem wirkmächtigen Symbol im politischen und vor allem medialen Diskurs geworden, weshalb ihr eine ebenso übertriebene wie unterschätzte Bedeutung zugeschrieben wird, die es nun zu beleuchten gilt.

4. Speicherung von Telekommunikationsverbindungsdaten (Vorratsdatenspeicherung)

Fragen nach der Bedeutung, Wirkung und Zulässigkeit der Vorratsdatenspeicherung werden seit einiger Zeit vorrangig in der rechtswissenschaftlichen Forschung untersucht und bereits vom Bundesverfassungsgericht hinsichtlich der Verfassungsvereinbarkeit geprüft (insb. 1 BvR 256/08 vom 2.3.2010). Vor allem aber findet die Debatte um die Vorratsdatenspeicherung im politisch-medialen bzw. gesellschaftlichen Raum statt (insb. bezogen auf die europ. Richtlinie bspw. Europäische Kommission 2011; European Digital Rights 2011; Albrecht 2011; Becher/Deutscher Bundestag Wissenschaftliche Dienste 2011; BT-Drs. 16/11139), wobei vergleichsweise feste Konfliktfronten und die üblichen politisch-medialen Aufmerksamkeitswellen erkennbar sind. Letztere hängen eng mit der wechselhaften Geschichte der Vorratsdatenspeicherung in Deutschland zusammen, die es zunächst kurz zu betrachten gilt (für einen Überblick der relevanten Beschlüsse vgl. bspw. FoeBud e.V.). Gerade in dieser Debatte spiegelt sich sehr deutlich die Kontroverse um eine Policy-Neuausrichtung im Sinne einer zunehmenden Präventionsorientierung wider, die argumentativ vor allem von der Terrorismusbekämpfung getragen wird.

4.1 Die Einführung der Vorratsdatenspeicherung in Deutschland als europäisch flankierter Politikwechsel

Deutschland ist im Falle der Vorratsdatenspeicherung im europäischen Kontext kein Vorreiter. Zu Beginn wurden Mindestspeicherungsfristen für Telekommunikationsverkehrsdaten breit abgelehnt, u.a. von der Bundesregierung 1996 in der Debatte um ein Telekommunikationsgesetz (vgl. BRat-Drs. 80/96). Hier wurde im Ergebnis erfolglos von Seiten der Länder versucht, die vorgesehenen Höchstspeicherfristen „für die Speicherung von personenbezogenen Daten der an der Telekommunikation beteiligten Personen" (BT-Drs. 13/4438: 39) um Mindestspeicherfristen zu ergänzen (BRat-Drs. 80/96: 48). Weitere Versuche, eine Mindestspeicherfrist einzuführen, folgten und wurden alternativ mit der Bekämpfung der organisierten Kriminalität oder der Strafverfolgung im Bereich Kinderpornographie begründet. Die Versuche gingen sowohl von CDU- (bspw. 2001: BT-Drs. 14/6834) als auch von SPD-Vertretern (bspw. 2002: BRat-Drs. 275/02) aus, blieben jedoch ohne Erfolg (zur Rolle der Länder bzw. des Bundesrats als Befürworter von Mindestspeicherfristen u.a. Krempl 2001; Heise online 2002). Der Bundestag widersetzte sich diesen Ansinnen mehrfach, u.a. 2004 (TKG-Novelle) und 2005 (Behandlung des Tätigkeitsberichts des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BT-Drs. 15/5252), Beschluss BT-Drs. 15/4597, Beschluss S. 14733C, einstimmig angenommen am 17.02.2005):

> „Der Deutsche Bundestag bekräftigt seine (…) Ablehnung einer Mindestspeicherungsfrist für Verkehrsdaten und fordert die Bundesregierung auf, einen etwaigen Beschluss in den Gremien der Europäischen Union (…) nicht mitzutragen." (BT-Drs. 15/4597)

Dass es schon wenig später zu einem Politikwechsel in Deutschland kam, ist einerseits der innenpolitischen Debatte nach den terroristischen Anschlägen von Madrid und London (vgl. BT-Drs. 15/3901: 2), andererseits der europäischen Ebene geschuldet, die gerade im Bereich der Vorratsdatenspeicherung maßgeblich zur Neuausrichtung der Politikfeldgestaltung in Deutschland beigetragen hat (vgl. Abschnitt 3.2 sowie insb. 4.2). Im Zuge dieser Richtlinien-Debatte hat der Bundestag – mittels CDU/CSU/SPD-Mehrheit[9] – seine Position neu gefasst und nun für die Einführung

[9] Noch 2002 hatte sich der CDU-Bundesvorstand gegenteilig positioniert: „Die von der Bundesregierung geplante generelle Verpflichtung von Providern zur Einhaltung einer Mindestspeicherfrist von Daten ist aus rechtsstaatlichen wie auch aus wirtschaftlichen Gründen nicht tragbar." (Beschluss des CDU-Bundesvorstands am 3. Juni 2002)

einer Mindestspeicherfrist für Telekommunikationsverbindungsdaten votiert (explizit ohne Kommunikationsinhalte; Bt-Drs. 16/545; 16/690):

> „Der Bundesregierung ist es – gestärkt durch die bisherige restriktive Beschlusslage des Deutschen Bundestages – in intensiven Verhandlungen auf europäischer Ebene gegen teils erhebliche Widerstände seitens einer Vielzahl anderer Mitgliedstaaten gelungen, sowohl im Europäischen Parlament als auch im Rat die nötigen Mehrheiten für eine Regelung mit Augenmaß zu gewinnen, so dass die in Kürze zur Annahme stehende Richtlinie nunmehr eine Umsetzung unter Wahrung verfassungsrechtlicher Vorgaben erlaubt. (…) Der Deutsche Bundestag fordert die Bundesregierung auf, (…) dem in der Sitzung der EU-Justizminister am 2. Dezember 2005 gefundenen Kompromisstext für eine Richtlinie über die Vorratsspeicherung (…) bei der abschließenden Befassung des Rates der Europäischen Union zuzustimmen; (…) alsbald den Entwurf eines Gesetzes zur gebotenen Umsetzung der Richtlinie in innerstaatliches Recht vorzulegen, dessen Regelungen sich in das nunmehr für Mitte 2007 angekündigte „harmonische Gesamtsystem" der verdeckten strafprozessualen Ermittlungsbefugnisse einfügen" (BT-Drs. 16/545).

Die Bundesregierung hat daraufhin Bundestag und Bundesrat im April 2007 einen *„Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG"* (Bt-Drs. 16/5846) zugeleitet, u.a. mit dem Ziel, ein „harmonisches Gesamtsystem der strafprozessualen heimlichen Ermittlungsmethoden" (BT-Drs. 16/5846) zu schaffen und die Richtlinie zur Vorratsdatenspeicherung umzusetzen. Formal notwendig wurde diese Neuregelung des Telekommunikationsgesetzes aus unterschiedlichen Gründen. Zum einen galt es, Urteile des Bundesverfassungsgerichts aufzugreifen (u.a. BVerfGE 113, 348, 391; BVerfGE 115, 166 ff.; vgl. BT-Drs. 16/5846). Für den Aspekt der Vorratsdatenspeicherung – nur ein Teilbereich der Gesetzesnovellierung – war insbesondere die europäische Richtlinie 2006/24/EG maßgeblich. Es folgten im Gesetzgebungsprozess u.a. zwei öffentliche Anhörungen des Rechtsausschusses (19./21.09.2007), bei denen zum einen die Maßnahmen zur Telekommunikationsüberwachung allgemein sowie zur Vorratsdatenspeicherung im Besonderen diskutiert wurden. Hier zeigt sich bereits der hohe Stellenwert, der der Datenspeicherung beigemessen wurde. Im Ergebnis hat der Deutsche Bundestag das Gesetz im November 2007 verabschiedet (entspr. Buchstabe a der Beschlussempfehlung BT-Drs. 16/6979; BGBl. I, Nr. 70, S. 3198ff. vom 31.12.2007). Es ist zum 1. Januar 2008 in Kraft getreten, woraufhin in der Nachfolge die innerdeutsche Debatte etwas zur Ruhe gekommen ist (vgl. Biermann 2009; Schweda 2011). Erst mit der Aussetzung der Speicherung durch das Karlsruher Urteil im März 2010 (BVerfGE 125, 260; 1 BvR 256/08

vom 2.3.2010) verschärfte sich die Debatte wieder. Besonders deutlich wurde die unterschiedliche Positionierung innerhalb der Bundesregierung. Während Bundesjustizministerin Leutheusser-Schnarrenberger (FDP; zugleich Klägerin in besagtem Verfahren) das Urteil begrüßt, da nun dem „einseitigen Stakkato an Sicherheitsgesetzen der vergangenen Jahre (…) erneut eine Absage erteilt" worden sei, sieht die Kanzlerin ein durch das Urteil entstehendes „Vakuum" (jew. zit. nach Müller 2010). Dieser Dissens besteht bis heute fort, im Zuge der Diskussion um die Terrorismusbekämpfung betont etwa die Bundeskanzlerin: „Auf das Instrument der Vorratsdatenspeicherung können wir im Zuge der Terror- und Verbrechensbekämpfung nicht verzichten." (Merkel 2011). Diese konträre Position führte in der aus vielerlei Gründen bereits fragilen Bundesregierung zu einer ernsthaften Krise (bspw. Höll 2011), womit die im Bereich der Inneren Sicherheit „üblichen" Konfliktlinien fortgeschrieben werden.

4.2 Der europäische Weg zur Vorratsdatenspeicherung

Um die zentrale Rolle der europäischen Ebene für die grundlegende Neubewertung der Vorratsdatenspeicherung zu verdeutlichen, ist ein kurzer Blick auf die europäische Debatte hilfreich. Entscheidend für die Durchsetzbarkeit auf europäischer Ebene sind die Anschläge in Madrid (04/2004), anhand derer sich in der EU (erneut) eine Debatte um ein gemeinsam-kohärentes Vorgehen in Sachen Vorratsdatenspeicherung entwickelte. Auf Initiative Frankreichs, Irlands, Schwedens und Großbritanniens wurde daraufhin ein Entwurf für einen „*Rahmenbeschluss über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus*" an den Rat der Europäischen Union übermittelt (Ratsdrucksache 8958/04; damals gemäß Art. 31 I c und 42 II b EUV). Ein solcher Rahmenbeschluss (3. Vertragssäule) war jedoch nicht durchsetzbar, u.a. weil die erforderliche Einstimmigkeit nicht erreicht werden konnte. Die Londoner Anschläge (07/2005) führten jedoch in Verbindung mit der damaligen britischen Ratspräsidentschaft zu einer Wiederbelebung der Debatte (vgl. bspw.

Bug et al. 2011), im Ergebnis legte die Kommission im September 2005 einen Richtlinien-Entwurf (1. Vertragssäule) vor. Diese Richtlinie (2006/24/EG) wurde nach raschen, aber konfliktreichen Beratungen mit Änderungen (etwa hinsichtlich der zu speichernden Datenarten) beschlossen (Amtsblatt der EU, L 105/54 DE vom 13.04.2006), auch wenn Zweifel an der Rechtmäßigkeit der gewählten Grundlage (Richtlinie statt Rahmenbeschluss) laut wurden (bspw. in Deutschland: BT-Drs. 16/545). Der europäische Gesetzgeber allerdings sieht den Regelungsbedarf vor allem aus Gründen der *Binnenmarktregulierung* als gegeben an, weshalb der Weg über eine Richtlinie erforderlich, gangbar und zulässig sei:

> „Einige Mitgliedstaaten haben Rechtsvorschriften über eine Vorratsspeicherung von Daten durch Diensteanbieter zum Zwecke der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten erlassen. Diese nationalen Vorschriften weichen stark voneinander ab. (…) Die rechtlichen und technischen Unterschiede zwischen den nationalen Vorschriften zur Vorratsdatenspeicherung zum Zwecke der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten beeinträchtigen den Binnenmarkt für elektronische Kommunikation, da Diensteanbieter mit unterschiedlichen Anforderungen in Bezug auf die zu speichernden Arten von Verkehrs- und Standortdaten, die für die Vorratsspeicherung geltenden Bedingungen und die Dauer der Vorratsspeicherung konfrontiert sind." (Richtlinie 2006/24/EG: 54)[10]

Diese später vom Europäischen Gerichtshof als zulässig beurteilte formalrechtliche Einschätzung (vgl. Urteil C-301/06 vom 10.02.2009)[11] stellt damit zwar ein maßgebliches Motiv für die Richtlinie dar, trifft jedoch nicht den Kern bzw. das eigentliche Ziel. Die Vorratsdatenspeicherung zielt auf Prävention und Strafverfolgung, weshalb sie der Sache nach primär als sicherheitspolitische bzw. polizei- und nachrichtendienstliche Ermittlungs- und Überwachungsmaßnahme verstanden wird:[12]

> „In seinen Schlussfolgerungen vom 19. Dezember 2002 betont der Rat „Justiz und Inneres", dass die beträchtliche Zunahme der Möglichkeiten bei der elektronischen Kommunikation dazu geführt hat, dass Daten über die Nutzung elektronischer Kommunikation besonders wichtig sind und daher ein wertvolles Mittel bei der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten und insbesondere der organisierten Kriminalität darstellen. (…)Am 13. Juli 2005 hat der Rat in seiner Erklärung, in der die Terroranschläge von London verurteilt wurden, nochmals auf die Notwendigkeit hingewiesen, so

[10] Wobei zu betonen ist, dass zu diesem Zeitpunkt in vielen Ländern keine Vorschriften bestanden bzw. das Instrument nicht vorgesehen/zulässig war.

[11] Irland reichte am 6. Juli 2006 gegen die EG-Richtlinie zur Vorratsdatenspeicherung Klage vor dem Europäischen Gerichtshof ein (C-301/06), da es die gewählte Rechtsgrundlage für unzulässig hielt: Schließlich gehe es vorranging um eine verbesserte Strafverfolgung (Dritte Säule) und nicht um eine Binnenmarktfrage (Erste Säule). Der EuGH wies die Klage am 10. Februar 2009 ab, wobei er betonte, dass ausschließlich die Frage der gewählten Rechtsgrundlage beurteilt wurde – grundrechtliche Aspekte waren nicht Teil der Klage.

[12] Weshalb im politischen Diskurs insbesondere die Innenminister, die staatlichen Sicherheitsproduzenten und (tw. als Gegenspieler) die Justizminister eine zentrale Rolle einnehmen.

> rasch wie möglich gemeinsame Maßnahmen zur Vorratsspeicherung von Telekommunikationsdaten zu erlassen." (Richtlinie 2006/24/EG: 54; 55)

Verdeutlicht wird dieses Argument auch in der ersten Bewertung des Richtlinienerfolgs, die die Kommission 2011 (verspätet) vorgelegt hat. Darin heißt es:

> „Darüber hinaus führten Trends bei Geschäftsmodellen und Dienstangeboten wie Flatrate-Tarifen, vorausbezahlten und kostenlosen elektronischen Kommunikationsdiensten dazu, dass die Betreiber immer weniger Verkehrs- und Standortdaten für die Gebührenabrechnung speicherten. Damit standen auch immer weniger derartige Daten für die Strafjustiz und die Strafverfolgung zur Verfügung. Die 2004 in Madrid und 2005 in London verübten Terroranschläge machten die Diskussionen zur Lösung dieser Probleme auf EU-Ebene noch dringlicher.
> Vor diesem Hintergrund verpflichtete die Richtlinie über die Vorratsdatenspeicherung Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste und Betreiber öffentlicher Kommunikationsnetze, Kommunikationsdaten „zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten, wie sie von jedem Mitgliedstaat in seinem nationalen Recht bestimmt werden", auf Vorrat zu speichern, und versuchte, bestimmte damit im Zusammenhang stehende Aspekte EU-weit zu harmonisieren." (Europäische Kommission 2011: 4)

Dieser Argumentationskontext verdeutlicht das eigentliche Motiv für die Richtlinie, und in gleicher Weise dominiert diese Zielsetzung den innerstaatlichen Diskurs. Gerade hier wird fast ausschließlich auf das daraus resultierende Überwachungs- bzw. Strafverfolgungs- und Präventionspotenzial abgestellt – sei es hinsichtlich der (in der Richtlinie) nicht näher spezifizierten Bekämpfung „schwerer Straftaten" (Aufklärungsfokus) oder von „Terrorismus" (Präventionsfokus).[13] Gleichwohl wirkte das formalrechtliche Argument der Gefahr einer Wettbewerbsverzerrung bzw. das Anliegen der innereuropäischen Harmonisierung von Rechtsvorschriften, so dass der deutsche Gesetzgeber der Richtlinie folgte und sich daraufhin mit der Einführung einer Vorratsdatenspeicherung befasst hat. Dies war zum Diskussionszeitpunkt jedoch bereits im Bundestag durch die Unterstützung von CDU, CSU und SPD mehrheitsfähig (BT-Drs. 16/545), so dass zwischenzeitlich eine Kohärenz in der Zielsetzung bestand (seit 2009 nur noch parlamentarisch bei Dissens in der Regierungskoalition). Diese parlamentarische Mehrheit ist insofern nicht unbedeutend, als dass sich andere Länder (bspw. Schweden) bis heute weigern, die Richtlinie trotz Strafandrohung umzusetzen (vgl. bspw. Altenbockum 2010; Schweda 2011).

[13] Eine Bewertung des Instruments, wie sie implizit in der Richtlinie zum Ausdruck kommt, unterbleibt in diesem Beitrag, da eine valide Bewertung im Rahmen dieses Beitrags weder beabsichtigt noch empirisch möglich ist und der kriminalistische Ertrag der Vorratsdatenspeicherung in der Literatur unterschiedlich gesehen wird (kritisch bspw. Arbeitskreis Vorratsdatenspeicherung 2011; Becher/Deutscher Bundestag Wissenschaftliche Dienste 2011).

4.3 Die Vorratsdatenspeicherung im Kontext der neuen deutschen Sicherheitsarchitektur

Verbindet man die Entwicklungsgeschichte der Vorratsdatenspeicherung in Deutschland mit den allgemeinen Befunden zur neuen deutschen Sicherheitsarchitektur, so wird deutlich, wie eng beide Aspekte miteinander verflochten sind. Dies gilt für die Perspektive der (europäischen) Harmonisierung und einer langfristig dadurch zu erreichenden Interoperabilität (wobei dieses zentrale Ziel der Richtlinie bis dato klar verfehlt wurde[14]) ebenso wie für die paradigmatische Neuausrichtung (dazu Abschnitt 4.4). Erkennbar ist die zunehmende Bedeutung einer informationellen Vernetzung, auch wenn die Daten nicht von den Sicherheitsbehörden gespeichert werden.[15] Die Verfügbarkeit bzw. die Abrufbarkeit von Daten ist im Rahmen der Vorratsdatenspeicherung für unterschiedliche staatliche Stellen (insb. Polizeien, Nachrichtendienste) und für vielfältige Zwecke (insb. Verfolgung von Straftaten und Abwehr von erheblichen Gefahren für die öffentliche Sicherheit) zulässig, so dass hier faktisch - hinsichtlich der Datennutzbarkeit – das Trennungsgebot durchbrochen wird bzw. werden kann. Letztendlich stellt die Vorratsdatenspeicherung ein im Umfang neuartiges Ermittlungsermöglichungsinstrument dar. Sie selbst ist dabei keine Ermittlungsmaßnahme: Sie schafft nur die technischen Voraussetzungen, um im Bedarfsfall auf verdachtsunabhängig gespeicherte Daten zugreifen zu können. Die Grundidee ist Prävention, es gilt, für alle Fälle, anlasslos Telekommunikationsverbindungsdaten zu speichern, die sonst nicht gespeichert würden (vgl. Fn. 3). Die technische Umsetzung (dezentrale Speicherung durch die Telekommunikationsdienstleister) steht dabei auf den ersten Blick im Gegensatz zur oben aufgezeigten Zentralisierung und Vernetzung im Bereich der inneren Sicherheit. Aber: Hinsicht-

[14] So die Europäische Kommission in ihrem ersten Bericht zur Umsetzung und Wirkung der Vorratsdatenspeicherung (Europäische Kommission 2011)). Es zeigen sich extreme Umsetzungsunterschiede, von der Nichtumsetzung/verfassungsgerichtlichen Aussetzung bis hin zur weit über die Richtlinie hinausgehenden Vorratsdatenspeicherung. Auch eine transnationale Datennutzung findet faktisch nicht statt, gerade ein Prozent aller Anfragen betraf Daten, „die in einem anderen Mitgliedstaat gespeichert waren. Die Strafverfolgungsbehörden gaben an, dass sie lieber Anfragen an inländische Betreiber richten“ (Europäische Kommission 2011: 27).

[15] Derzeit sind die Regelungen zur Vorratsdatenspeicherung nichtig, daher wird hier argumentativ auf die alte Regelung zurückgegriffen, da die hier relevanten Grundzüge vermutlich in ähnlicher Weise Bestand haben werden und vor allem die strukturellen Grundaspekte/die geschaffene Infrastruktur von Bedeutung sind.

lich der organisationalen Wirkung ist die dezentrale Speicherung und standardisierte Verfügbarmachung der Verbindungsdaten einer tatsächlich zentralen Speicherung funktional faktisch gleichzusetzen. Ähnlich wie bei der Antiterrordatei und anderen Informationsdatenbanken stehen den zentralen Einrichtungen im Rahmen der rechtlichen Vorgaben rasch verfügbare Informationen zur Verfügung, so dass diese im binnenstaatlichen Gefüge gestärkt werden können (hier bleiben die konkreten Nutzungsbefugnisse einer Neuregelung abzuwarten). Somit kann als Zwischenfazit die Annahme bestätigt werden, dass sich die Vorratsdatenspeicherung – unabhängig von der gegenwärtigen Nichtumsetzung – prototypisch in die neue deutsche Sicherheitsarchitektur einfügt und den skizzierten Paradigmenwechsel offenbart. Dies bleibt, darauf ist nun einzugehen, nicht ohne Folgen für das Bürger-Staat-Verhältnis, und genau deshalb ist die Vorratsdatenspeicherung von großer symbolischer Bedeutung für das Politikfeld Innere Sicherheit.

4.4 Die Vorratsdatenspeicherung als Symbol der neuen Sicherheitspolitik und eines gewandelten Verhältnisses von Bürger/Gesellschaft – Staat – Wirtschaft

Gerade der Vorratsdatenspeicherung kommt in den sicherheitspolitischen und gesellschaftlichen Debatten eine große Aufmerksamkeit zu. So war beispielsweise die Klage gegen die Vorratsdatenspeicherung mit fast 35.000 Beschwerdeführern das bei weitem umfangreichste Massenklageverfahren in der Geschichte des Bundesverfassungsgerichts (vgl. Tagesschau online 2010). Auch der zivilgesellschaftliche Protest gegen staatliche Überwachungsmaßnahmen und für mehr Datenschutz findet seit einigen Jahren in unterschiedlichster Weise vermehrt Zulauf, die Protestbewegung hat sich vom Internet auf die Straßen bis in die Popkultur vorgearbeitet (vgl. Hornung et al. 2010: 151). Zu nennen sind hier etwa das Aufkommen der Piratenpartei (als vor allem urbanes Phänomen, besonders auffällig bei der Berlin-Wahl 2011), die „Freiheit statt Angst" – Demonstrationen als „Loveparade für Bürgerrechte" mit bis zu ca. 20.000 Teilnehmenden (vgl. Reißmann 2009) oder – als Ausdruck der zivilgesellschaftlichen Problematisierung – der Grimme Online Award Spezial 2011 für die Zeit online-Reportage „Was Vorratsdaten über uns verraten", bei der anhand von Telekommunikationsverbindungsdaten für jedermann leicht nachvollziehbar das

persönliche Bewegungsprofil des Grünen-Politikers Spitz visualisiert wurde (Grimme Institut 2011; Biermann 2011). Das Thema ist offensichtlich dazu geeignet, Befürworter und Gegner zivilgesellschaftlich und medial zu mobilisieren. Doch woran liegt das, warum manifestiert sich gerade an diesem Instrument der Protest?

Bereits das letztgenannte Beispiel verdeutlicht, warum trotz der sehr technischen Prägung der Vorratsdatenspeicherung die Erfassung und Speicherung von Telekommunikationsdaten als Symbol des Protests so gut geeignet sind. Es ist gerade nicht das konkrete Ermittlungs- und Überwachungsinstrument bzw. die tatsächliche Nutzung der so erfassten Daten, vielmehr mobilisieren die Breite der anlasslosen Datenspeicherung und das abstrakte Potenzial der dann überhaupt erst gespeicherten Daten zum Protest. Nicht (nur) die objektive Komponente der Vorratsdatenspeicherung ist Gegenstand des Protests, sondern (auch) die subjektive Wahrnehmungsseite und der im Instrument zum Ausdruck gebrachte Paradigmenwechsel. Auf das Potenzial der so gesammelten Daten – das die prämierte Zeit-Reportage für jedermann verständlich aufgezeigt hat – stellt auch das Bundesverfassungsgericht in seiner Bewertung der Vorratsdatenspeicherung ab:

> „Allerdings handelt es sich bei einer solchen Speicherung um einen besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt. Auch wenn sich die Speicherung nicht auf die Kommunikationsinhalte erstreckt, lassen sich aus diesen Daten bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse ziehen. Adressaten, Daten, Uhrzeit und Ort von Telefongesprächen erlauben, wenn sie über einen längeren Zeitraum beobachtet werden, in ihrer Kombination detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönlichen Vorlieben, Neigungen und Schwächen. Je nach Nutzung der Telekommunikation kann eine solche Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers ermöglichen. Auch steigt das Risiko von Bürgern, weiteren Ermittlungen ausgesetzt zu werden, ohne selbst hierzu Anlass gegeben zu haben. Darüber hinaus verschärfen die Missbrauchsmöglichkeiten, die mit einer solchen Datensammlung verbunden sind, deren belastende Wirkung.“ (Bundesverfassungsgericht 2010)

In dieser technischen Vorbereitung einer neuen Kontrollkultur manifestiert sich die Transformation zur präventionsorientierten Sicherheitspolitik, bei der auch im polizeilichen Bereich verstärkt auf verdeckte geheimdienstliche Ermittlungsverfahren mittels anlasslos generierter Daten gesetzt wird. Die – bei derartigen Instrumenten notwendige – Nichtnachvollziehbarkeit der Datennutzung ist allerdings nicht nur, wie bereits bei der Telefonüberwachung nachgewiesen wurde (vgl. Albrecht et al. 2003), kaum zu kontrollieren, sondern führt vor allem auch dazu, dass der Bürger die

Kontrolle über die Kontrolle verliert. Er weiß zwar, dass sämtliche Kommunikationsvorgänge gespeichert werden, jedoch nicht, ob und in welchem Umfang die Daten Verwendungen finden. Damit ist ihm eine rechtsstaatliche Kontrolle einer etwaigen Datenverwendung verwehrt. Es entsteht so mutmaßlich ein diffuses Gefühl der Unsicherheit, das zivilgesellschaftliches Partizipationsverhalten und die Wahrnehmung von Grundrechten beeinflussen könnte.[16] Dabei ist anzunehmen, dass die Wirkung nicht in der breiten Bevölkerung, wohl aber in der Teilgruppe der informierten Aktivbürgerschaft eine wichtige Rolle spielt. Hier ist künftig eine umfassende, valide Forschung geboten (erste Untersuchungen liegen jedoch vor, bspw. Lüdemann/Schlepper 2011); vorerst kann über die Wirkung der nichtbeobachtbaren Vollerfassung nur – optimistisch (BReg) oder kritisch (BVerfG) – gemutmaßt werden:

> „Die Bundesregierung ist der Auffassung, dass die Speicherungspflichten keinen unzulässigen „Einschüchterungseffekt" erzeugen. Ein solcher Einschüchterungseffekt wurde auch früher nicht wahrgenommen, obwohl (…) viele Daten im Rahmen privatrechtlicher Vertragsverhältnisse zwischen Kunden und Telekommunikationsunternehmen gespeichert wurden, für die gesetzliche Zugriffsmöglichkeiten der Behörden bestanden." (BT-Drs. 16/11139: 6)

> „Zumal die Speicherung und Datenverwendung nicht bemerkt werden, ist die anlasslose Speicherung von Telekommunikationsverkehrsdaten geeignet, ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann." (Bundesverfassungsgericht 2010)

Gewicht erhält diese (postulierte) Gefahr vor allem dadurch, dass ein Opting-Out aus der Kontrolle nicht möglich ist. Ein genereller Verzicht auf Telekommunikation ist in der digitalen Gesellschaft nicht möglich, käme dieser doch faktisch einem Partizipationsausschluss gleich. Schon der temporäre Verzicht – etwa die Nicht-Mitnahme eines Mobiltelefons – wird zunehmend diskreditiert und im Einzelfall von staatlicher Seite bereits als konspiratives Verhalten und damit verdachtsgenerierend gewertet (vgl. Vorsamer 2007), und Sennet/Sassen befürchten, dass „persecution seems to have taken the place of prosecution" (Sennett/Sassen 2007). Die Verbindung dieses

[16] Zu einem solchen Unbehagen tragen auch verdeckte Maßnahmen wie die vermutlich rechtswidrige Erfassung und Auswertung von Handydaten bei Anti-Nazi-Demonstrationen in Dresden bei (vollständig erfasst wurden eingehende/ausgehende Anrufe/SMS sowie die jeweilige Position von Teilnehmern, Anwohnern, Journalisten und Politikern). Die Funkzellenauswertungen, bei denen im Februar 2011 über eine Million Handy-Verbindungsdaten aufgezeichnet wurden, wurden erst nachlaufend durch die taz aufgedeckt (vgl. bspw. die tageszeitung 2011) und führten zu einer umfassenden Debatte, die noch andauert. Der Dresdner Polizeipräsident wurde im Juni 2011 als Reaktion auf die Maßnahme und die Debatte abberufen.

Gefühls mit der allumfassenden Kommunikationsverbindungsdatenspeicherung ist damit maßgeblich für das Symbol- und Mobilisierungspotenzial, wobei das Problem der Unvermeidbarkeit einer solchen kommunikativen Totalerfassung noch an Bedeutung gewinnen dürfte, wenn man an die aktuell diskutierte Einführung von statischen IP-Adressen (IPv6) oder Klarnamen im Internet denkt (Social Networks wie Google+ verlangen dieses bereits, vgl. Ihlenfeld 2011; Forderung u.a. des Bundesinnenministers, vgl. Zeit online/dpa). Auch wenn der letztgenannte Punkt (noch) wenig Chancen auf Durchsetzung hat: Entscheidend ist der dahinter liegende staatliche Präsenz-, Kontroll- und Durchgriffsanspruch. Schon aus diesem Grund wird die Debatte um eine stärkere staatliche Überwachung der Telekommunikation weitergehen, und schon aus diesen Gründen generiert gerade die Einführung von Mindestspeicherfristen eine derart große Aufmerksamkeit.[17] Wurde in den 1990ern Jahren noch die Einführung von CCTV (Videoüberwachung) im öffentlichen Raum intensiv diskutiert, so hat sich diese nunmehr flächendeckend durchgesetzt (und zwar unabhängig von der Frage der Wirksamkeit bzw. Effizienz). In die Nachfolge ist die Debatte um die Vorratsdatenspeicherung getreten. Ähnlich wie die Bildüberwachung des öffentlich-realen Raums diskutiert wurde, wird nun um die (letztlich sehr viel weitreichendere) Überwachung des virtuellen Raums gestritten. Wie allerdings diese staatliche Inbesitznahme und wie Einzelmaßnahmen wie die Vorratsdatenspeicherung von der Gesellschaft rezipiert und bewertet werden, ist bislang nicht umfassend erforscht.

Ein abschließendes Argument für die Symbolbedeutung der Vorratsdatenspeicherung bzw. der Proteste gegen die Erfassung und Analyse der Kommunikationsströme im Auftrag des Staates ist die hinsichtlich der Sichtbarkeit gelungene, hinsichtlich der politisch-historischen und personalisierenden Zuspitzung jedoch fragwürdige Ikonografie, derer sich die Proteste gegen die Vorratsdatenspeicherung (und die Onlinedurchsuchung) bedienen. Die von Dirk Adler entwickelte „Schäublone“ (vgl. Löwisch 2007) verbildlicht den Protest-Claim „Stasi 2.0“ mittels eines Schäuble-Konterfeis (als leicht anwendbare Sprühschablone) und erregt als Protestzeichen

[17] Diskutiert wird auch die Frage der „Überwachungsgesamtrechnung“, dazu bspw. Roßnagel (2010).

Aufmerksamkeit (vgl. Moorstedt 2007). Mit dieser „Stasi 2.0“ – Ikonografie dürfte eines der innenpolitisch präsentesten Bilder der 2000er-Jahre geschaffen worden sein.

5. Die Vorratsdatenspeicherung: über- und unterschätzt zugleich

Die neue deutsche Sicherheitsarchitektur hat das Politikfeld Innere Sicherheit verändert, Deutschland entwickelt sich zum sicherheitsorientierten Präventionsstaat. In der Vorratsdatenspeicherung manifestiert sich diese Veränderung. Die Bedeutung der Vorratsdatenspeicherung selbst wird dabei im politisch-medialen Diskurs einerseits *überschätzt*: Es handelt sich schließlich in erster Linie um eine Datenspeicherung, nicht um eine Datennutzung oder eine Generalüberwachung der Bürger. Das Instrument hat zudem eine demokratisch-parlamentarische Mehrheit gefunden und ist bei einer adäquaten gesetzlichen Ausgestaltung verfassungskonform (Bundesverfassungsgericht 2010). Und auch wenn die Vorratsdatenspeicherung als Symbol des zivilgesellschaftlichen Protests heraussticht – eine neue, tief greifende gesellschaftliche Konfliktlinie ist nicht erkennbar. Im Vergleich zu bedeutsameren Defekten des Rechtsstaates steht die Debatte um Mindestspeicherfristen im Verhältnis zu ihrem rechtsstaatlichen Gefährdungspotenzial unverhältnismäßig stark im Vordergrund. Schließlich geht die eigentliche Gefahr für den Datenschutz vor allem vom privaten Datenumgang aus: „Wer glaubt, der Staat wisse viel über seine Bürger, täuscht sich. Soziale Netzwerke und Versandhändler kennen uns längst besser.“ (Skalli 2011) Dieser Datenschutz-Selbstverzicht reicht vom Verzicht auf Datensparsamkeit über die Veröffentlichung persönlicher (Bewegungs-)Daten bei sozialen Netzwerken (bspw. Veröffentlichung von namensgetaggten Fotos der Freiheit-statt-Angst-Demos) bis hin zur Post-Privacy-Diskussion.

Andererseits sprechen einige Punkte dafür, dass die Bedeutung der Vorratsdatenspeicherung im Diskurs *nicht überschätzt* wird: Mit der Vorratsdatenspeicherung wird vor allem eine überwachungsermöglichende Infrastruktur eingeführt, womit die Gefahr besteht, dass schon bald die Forderung nach einer erweiterten Nutzung dieser (dann „bereits vorhandenen“) Daten laut werden könnte. Ähnliche Forderungen wurden bereits in der Vergangenheit laut, etwa bei den Mautdaten (für Strafverfolgungszwecke). Nicht die Analyse der gespeicherten Daten selbst ist somit das Prob-

lem, sondern die gesetzlich-legitimatorische und technische Datenspeicherungsermöglichung. Dazu kommen rechtsstaatliche Kontrolldefizite und Zweifel an der (technischen) Datensicherheit (Europäische Kommission 2011: 22).[18]

Die technisch-infrastrukturelle Perspektive ist jedoch nur ein Aspekt. Problematischer und bislang kaum untersucht ist Langfristwirkung des sicherheitsorientierten Präventionsstaates, insbesondere die Rückwirkung auf die Legitimation des Staates selbst:

> „The liberal state is changing. (…) Today (…) the state of emergency prevails. The laws meant for real threats are invoked to counter shapeless fear; in place of real police work, the authorities want to put a name - any name - to what they should dread. States of emergency are dangerous to the legitimacy of states." (Sennett/Sassen 2007)

Entscheidend ist dabei, dass die sicherheitspolitische Neuausrichtung den staatlichen Blick auf die Bevölkerung verändert – die gesamte Bevölkerung ist nunmehr für die Sicherheitsbehörden bedeutsam. Besonders augenfällig wird dies an der Vorratsdatenspeicherung, weshalb Kritiker gerade hier vom „Generalverdacht" sprechen. Unabhängig von der (politisch-normativen) Bewertung des Instruments: Die Beziehung zwischen Staat und Bevölkerung verändert sich. Doch wie wirkt sich diese Veränderung empirisch messbar auf das Verhältnis zwischen Staat und Bevölkerung aus, welche Konsequenzen ergeben sich für die Legitimation staatlichen Handelns? Wie kann das Vertrauen der Bevölkerung in den Staat erhalten werden, wenn der Staat das Vertrauen in die Bevölkerung strukturell hinterfragt (bzw. hinterfragen muss)? Die Vorratsdatenspeicherung offenbart in diesem Diskurs den sicherheitspolitischen Paradigmenwechsel und dient daher einer kritischen Bevölkerungsgruppe als Symbol des Protests. Sichtbar wird dies im Rahmen verfasster und nichtverfasster zivilgesellschaftlicher Interventionen. Die symbolische Bedeutung der Vorratsdatenspeicherung wird dabei in der politik- und sozialwissenschaftlichen Forschung künftig ebenso zu untersuchen sein wie die Wirksamkeit und die (nicht nur materiellen) Folgekosten der Vorratsdatenspeicherung. Zu untersuchen ist darüber hinaus, wie sich

[18] Auch die Bevölkerung ist in Punkto Datensicherheit allgemein skeptisch (vgl. BITKOM 2011a). Bei der Vorratsdatenspeicherung ist problematisch, dass die Telekommunikationsdienstleister die Daten speichern, und diesen sind jüngst mehrfach Pannen unterlaufen (vgl. heise.de, u.a. „Telekom-Sicherheitslücke offenbart 30 Millionen Handydaten" (10/2008); „Wirbel um Aufzeichnung von Ortungsdaten im iPhone" (04/2011)).

das veränderte Verhältnis von Staat und Citoyen auf die politische Partizipation und die Legitimation des politischen Systems auswirkt.

Literatur

Albrecht, Hans-Jörg/Dorsch, Claudia/Krüpe, Christiane 2003: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen, Max-Planck-Institut für ausländisches und internationales Strafrecht: 17, Freiburg im Breisgau.

Albrecht, Jan-Philipp 2011: Vorratsdatenspeicherung - notwendig, effektiv und verhältnismäßig?, Brüssel: Die Grünen/Europäische Freie Allianz im Europäischen Parlament.

Altenbockum, Jasper von 2010: Die Richtlinie, nach der sich nicht alle richten, FAZ online 04.03.2010, in: http://www.faz.net/-00lskj; 04.03.2010.

Ambos, Kai 2006: Terrorismusbekämpfung seit dem 11. September 2001, in: Becker, Michael/Zimmerling, Ruth (Hrsg.): Politik und Recht (PVS-Sonderheft 36/2006), Wiesbaden: VS Verlag für Sozialwissenschaften, 416-448.

Arbeitskreis Vorratsdatenspeicherung 2011: Data Retention Effectiveness Report: Serious criminal offences, as defined in sect. 100a StPO, in Germany according to police crime statistics.

ARD/ZDF 2011: ARD/ZDF-Onlinestudie 2011: 3 von 4 Deutschen sind online – starker Zuwachs bei den Über-60-Jährigen, ARD/ZDF, 04.07.2011, in: http://www.ard-zdf-onlinestudie.de; 08.07.2011.

Becher, Johannes/Deutscher Bundestag Wissenschaftliche Dienste 2011: Die praktischen Auswirkungen der Vorratsdatenspeicherung auf die Entwicklung der Aufklärungsquoten in den EU-Mitgliedsstaaten (WD 7-3000-036/11), Berlin: Deutscher Bundestag Wissenschaftliche Dienste.

Berliner Morgenpost 2011: Hilfspolizisten. CDU will Bürgerwehr in Berlin wieder einführen, Berliner Morgenpost online, 28.02.2011, in: http://www.morgenpost.de/berlin-aktuell/article1559593/CDU-will-Buergerwehr-in-Berlin-wieder-einfuehren.html; 22.05.2011.

Biermann, Kai 2011: Was Vorratsdaten über uns verraten, Zeit online, 02.02.2011, in: www.zeit.de/vorratsdaten; 24.2.2011.

Biermann, Kai 2009: Warum die Vorratsdatenspeicherung uns bedroht, ZEIT online, 20.02.2011, in: http://www.zeit.de/online/2009/28/vorratsdaten-ccc-verfassungsgericht; 07.07.2009.

BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.) 2011a: Schutz der persönlichen Daten ist Kernaufgabe von Politik und Wirtschaft. Pressemitteilung (08.02.2011), BITKOM, 08.02.2011, in: http://www.bitkom.org/de/presse/8477_66819.aspx; 20.04.2011.

BITKOM (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.) 2011b: SMS beliebt wie nie zuvor, 18.05.2011, in: http://www.bitkom.org/de/markt_statistik/64046_67951.aspx; 18.05.2011.

Böckenförde, Stephan/Gareis, Sven Bernhard 2009: Vorwort, in: Böckenförde, Stephan/Gareis, Sven Bernhard (Hrsg.): Deutsche Sicherheitspolitik: Herausforderungen, Akteure und Prozesse, Opladen: Barbara Budrich, 7-8.

Brugger, Winfried 2004: Freiheit und Sicherheit, Baden-Baden: Nomos.

Bug, Mathias/Enskat, Sebastian/Fischer, Susanne/Klüfers, Philipp/Röllgen, Jasmin/Wagner, Katrin 2011: Strategien gegen die Unsicherheit. Europäische Sicherheitsmaßnahmen nach 9/11, in: Die Friedens-Warte 86: 3-4, 53-82.

Bukow, Sebastian 2005a: Verschärfte Kontinuität im Kampf gegen den Terrorismus?, in: Kommune: Forum für Politik, Ökonomie, Kultur 23: 5, 23-26.

Bukow, Sebastian 2005b: Deutschland: Mit Sicherheit weniger Freiheit über den Umweg Europa, in: Glaeßner, Gert-Joachim/Lorenz, Astrid (Hrsg.): Europäisierung der inneren Sicherheit. Eine vergleichende Untersuchung am Beispiel von organisierter Kriminalität und Terrorismus, Wiesbaden: VS Verlag für Sozialwissenschaften, 43-62.

Bukow, Sebastian 2008: Zentralisiert und vernetzt. Die neue deutsche Sicherheitsarchitektur, in: Vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik: 184 (4/2008), 15-22.

Bukow, Sebastian 2009: Die neue deutsche Sicherheitsarchitektur: Wandel und Entwicklung der inneren Sicherheit in Deutschland im europäischen Kontext, in: Lorenz, Astrid/Reutter, Werner (Hrsg.): Ordnung und Wandel als Herausforderung für Staat und Gesellschaft, Opladen: Barbara Budrich, 349-370.

Bull, Hans-Peter 2007: Wie weit reicht das Sicherheitsversprechen des Staates gegenüber seinen Bürgern?, in: Graulich, Kurt/Simon, Dieter (Hrsg.): Terrorismus und Rechtsstaatlichkeit. Analysen, Handlungsoptionen, Rechtsstaatlichkeit (Interdisziplinäre Arbeitsgruppen. Forschungsberichte, Band 17.

Berlin-Brandenburgische Akademie der Wissenschaften), Berlin: Oldenbourg Akademie Verlag, 303-314.

Bundesministerium des Innern 2004: Frei und sicher leben - Deutsche Innenpolitik in Europa, Berlin.

Bundesverfassungsgericht 2010: Konkrete Ausgestaltung der Vorratsdatenspeicherung nicht verfassungsgemäß. (Pressemitteilung 11/2010 vom 02.03.2010; Urteil vom 02.03.2010; 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08), Bundesverfassungsgericht, 02.03.2010, in: http://www.bverfg.de/pressemitteilungen/bvg10-011; 02.03.2010.

Buzan, Barry/Waever, Ole/Wilde, Jaap de 1998: Security. A New Framework for Analysis, Boulder/Colorado: Lynne Rienner.

CDU/CSU-Fraktion im Deutschen Bundestag (Arbeitsgruppe Innen) 2011: Die Freiheit des Internet sichern und erhalten. Positionspapier der Arbeitsgruppe Innen der CDU/CSU-Fraktion im Deutschen Bundestag. Beschluss der Arbeitsgruppe Innen vom 20. September 2011, CDU/CSU-Fraktion im Deutschen Bundestag (bei netzpolitik.org veröffentlicht), 21.09.2011, in: http://netzpolitik.org/2011/eine-anonyme-teilhabe-am-politischen-meinungs-und-willensbildungsprozess-ist-abzulehnen; 21.09.2011.

die tageszeitung 2011: Dresdner Handydaten bleiben unter Verschluss, in: die tageszeitung (21.07.2011).

DPolG 2010: Positionen der DPolG, Fachverband Bundespolizei, zur Zusammenführung der Sicherheitsbehörden im Bund. Werthebachkommission, DPolG, 17.12.2010, in: http://www.dpolg-bundespolizei.de/downloads/positionspapierdpolgfachverbandbundespolizeiwe.pdf; 17.12.2010.

Europäische Kommission 2011: Bericht der Kommission an den Rat und das Europäische Parlament. Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung (Richtlinie 2006/24/EG) (Drucksache KOM(2011) 225 endgültig), Europäische Kommission,, 18.04.2011, in: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:DE:PDF; 25.04.2011.

European Digital Rights 2011: Shadow evaluation report on the Data Retention Directive (2006/24/EG), Brüssel: European Digital Rights.

Feltes, Thomas 2009: Akteure der Inneren Sicherheit: Vom Öffentlichen zum Privaten, in: Lange, Hans-Jürgen/Ohly, H. Peter/Reichertz, Jo (Hrsg.): Auf der Suche nach neuer Sicherheit, Wiesbaden, 105-113.

FoeBud e.V. Materialien, 01.08.2011, in: http://www.vorratsdatenspeicherung.de/content/view/77/85/lang,de; 01.08.2011.

Forschungsgruppe Wahlen 2011: Internet-Strukturdaten. Repräsentative Umfrage - II. Quartal 2011, Forschungsgruppe Wahlen, 26.07.2011, in: http://www.forschungsgruppe.de/Umfragen/Internet-Strukturdaten/web_II_11.pdf; 26.07.2011.

Funk, Albert 2010a: Deutschland braucht kein FBI, Zeit online, 10.12.2010, in: http://www.zeit.de/politik/deutschland/2010-12/bundespolizei-zentralisierung-macht; 10.12.2010.

Funk, Albert 2010b: Länder revoltieren gegen de Maizières Polizeireform, Zeit online, 30.12.2010, in: http://www.zeit.de/politik/2010-12/polizeireform-widerstand-bruch-bouffier; 30.12.2010.

Glaeßner, Gert-Joachim 2003: Sicherheit in Freiheit. Die Schutzfunktion des demokratischen Staates und die Freiheit der Bürger, Opladen: Leske + Budrich.

Glaeßner, Gert-Joachim/Lorenz, Astrid (Hrsg.) 2005: Europäisierung der inneren Sicherheit. Eine vergleichende Untersuchung am Beispiel von organisierter Kriminalität und Terrorismus, Wiesbaden: VS Verlag für Sozialwissenschaften.

Graulich, Kurt 2007: Terrorismus und Terrorismusbekämpfung - Folgt der Auflösung der rechtlichen Angriffsform die Auflösung der rechtlichen Verteidigungsform?, in: Graulich, Kurt/Simon, Dieter (Hrsg.): Terrorismus und Rechtsstaatlichkeit. Analysen, Handlungsoptionen, Rechtsstaatlichkeit (Interdisziplinäre Arbeitsgruppen. Forschungsberichte, Band 17. Berlin-Brandenburgische Akademie der Wissenschaften), Berlin: Oldenbourg Akademie Verlag, 389-414.

Grimme Institut 2011: Preisträger 2011, in: http://www.grimme-institut.de/html/index.php?id=1122#c8530; 01.08.2011.

Gusy, Christoph 2007: Präventionsstaat zwischen Rechtsgüterschutz und Abbau von Freiheitsrechten in Deutschland, in: Graulich, Kurt/Simon, Dieter (Hrsg.): Terrorismus und Rechtsstaatlichkeit. Analysen, Handlungsoptionen, Rechtsstaatlichkeit (Interdisziplinäre Arbeitsgruppen. Forschungsberichte, Band 17. Berlin-Brandenburgische Akademie der Wissenschaften), Berlin: Oldenbourg Akademie Verlag, 273-294.

Gusy, Christoph/Pohlmann, Kristine 2007: Wächst zusammen, was nicht zusammengehört? Die zunehmende Vernetzung zwischen Polizei und Verfassungsschutz weicht das Trennungsgebot auf, in: Vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik 46: 2, 53-63.

Haubrich, Dirk 2005: Anti-Terrorismusgesetze und Freiheitsrechte nach dem 11. September: Großbritannien, Frankreich und Deutschland im Vergleich, in: Jäger, Thomas/Höse, Alexander/Oppermann, Kai (Hrsg.): Transatlantische Beziehungen, Wiesbaden: VS Verlag für Sozialwissenschaften, 287-304.

Heinz, Wolfgang S. 2004: Internationale Terrorismusbekämpfung und Achtung der Menschenrechte, in: Aus Politik und Zeitgeschichte: 3-4/2004, 32-40.

Heise online 2002: Bundesrat entscheidet am Freitag über schärfere Internet-Überwachung, Heise online, 27.05.2002, in: http://heise.de/-61896; 27.05.2002.

Hitzler, Ronald (Hrsg.) 1998: Inszenierung Innere Sicherheit. Daten und Diskurse, Opladen: Leske & Budrich.

Höll, Susanne 2011: Vorratsdatenspeicherung. Union keilt gegen FDP-Ministerin. Leutheusser-Schnarrenbergers Pläne zur Datenspeicherung sorgen für einen "veritablen Konflikt" in der schwarz-gelben Koalition, Süddeutsche Zeitung 18.01.2011, in: http://www.sueddeutsche.de/politik/vorratsdatenspeicherung-union-keilt-gegen-fdp-ministerin-1.1047750; 18.01.2011.

Hornung, Gerrit/Bendrath, Ralf/Pfitzmann, Andreas 2010: Surveillance in Germany: Strategies and Counterstrategies, in: Gutwirth, Serge/Poullet, Yves/De Hert, Paul (Hrsg.): Data Protection in a Profiled World, Dordrecht: Springer, 139-156.

Huster, Stefan/Rudolph, Karsten (Hrsg.) 2008: Vom Rechtsstaat zum Präventionsstaat, Frankfurt/Main: Suhrkamp.

Ihlenfeld, Jens 2011: Web feuert auf Google wegen Klarnamenzwang, Handelsblatt online 27.07.2011, in: http://www.handelsblatt.com/technologie/it-tk/it-internet/web-feuert-auf-google-wegen-klarnamenzwang/4436908.html; 27.07.2011.

Initiative D21/TNS Infratest 2011: (N)Onliner Atlas 2011. Eine Topographie des digitalen Grabens durch Deutschland, Berlin: Initiative D21.

Isensee, Josef 1983: Das Grundrecht auf Sicherheit, Berlin u.a.: de Gruyter.

Jakobs, Günther 2004: Bürgerstrafrecht und Feindstrafrecht, in: HRRS: Onlinezeitschrift für Höchstrichterliche Rechtsprechung im Strafrecht 5. Jahrgang: 3/2004, 88-95.

Klingst, Martin 2007: Alle Macht dem Präventionsstaat?, in: Graulich, Kurt/Simon, Dieter (Hrsg.): Terrorismus und Rechtsstaatlichkeit. Analysen, Handlungsoptionen, Rechtsstaatlichkeit (Interdisziplinäre Arbeitsgruppen. Forschungsberichte, Band 17. Berlin-Brandenburgische Akademie der Wissenschaften), Berlin: Oldenbourg Akademie Verlag, 325-331.

Kommission "Evaluierung Sicherheitsbehörden" 2010: Kooperative Sicherheit. Die Sonderpolizeien des Bundes im föderalen Staat, Kommission "Evaluierung Sicherheitsbörden"/Bundesministerium des Innern, 09.12.2010, in: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/Bundespolizei/werthebach_1.pdf?__blob=publicationFile; 09.12.2010.

Kraftwerk 1981: Computerwelt, London: KlingKlang/EMI/Capitol Records.

Krempl, Stefan 2001: Verstärkter Datenhunger der Bundesländer, Heise online, 07.10.2001, in: http://heise.de/-51773; 07.10.2001.

Kruse, Birgit 2007: Dick-Marty-Bericht zu Terrorlisten. "Zivile Todesstrafe" (Süddeutsche Zeitung online, 12.11.2007), Süddeutsche Zeitung online (12.11.2007), 12.11.2007, in: http://www.sueddeutsche.de/politik/dick-marty-bericht-zu-terrorlisten-zivile-todesstrafe-1.344886; 04.05.2011.

Kutscha, Martin 1998: Große Koalition der Inneren Sicherheit?, in: Bürgerrechte & Polizei/CILIP 59: 1, 57-69.

Kutscha, Martin 2003: Mehr Innere Sicherheit durch weniger Freiheit?, in: Humanistische Union (Hrsg.): Innere Sicherheit als Gefahr, Berlin: Humanistische Union, 32-47.

Kutscha, Martin 2008: Innere Sicherheit und bürgerrechtliche Freiheit Von der „Rettungsfolter“ bis zur elektronischen Rundumüberwachung in: Lange, Hans-Jürgen/Ohly, H. Peter/Reichertz, Jo (Hrsg.): Auf der Suche nach neuer Sicherheit, Wiesbaden: VS Verlag für Sozialwissenschaften, 309-319.

Lange, Hans-Jürgen 1999: Innere Sicherheit im politischen System der Bundesrepublik Deutschland, Opladen: Leske + Budrich.

Lange, Hans-Jürgen 2006: Innere Sicherheit und der Wandel von Staatlichkeit, in: Schmidt, Manfred G./Zohlnhöfer, Reimut (Hrsg.): Regieren in der Bundesrepublik Deutschland, Wiesbaden: VS Verlag für Sozialwissenschaften, 87-112.

Lange, Hans-Jürgen/Frevel, Bernhard 2009: Innere Sicherheit im Bund, in den Ländern und in den Kommunen, in: Lange, Hans-Jürgen/Ohly, H. Peter/Reichertz, Jo (Hrsg.): Auf der Suche nach neuer Sicherheit. Fakten, Theorien und Folgen, Wiesbaden: VS Verlag für Sozialwissenschaften, 115-148.

Lepsius, Oliver 2004: Freiheit, Sicherheit und Terror: Die Rechtslage in Deutschland, in: Leviathan: Zeitschrift für Sozialwissenschaft 32: 1, 64-88.

Lepsius, Oliver 2006: Die Terrorismusgesetzgebung und das Verhältnis von Freiheit und Sicherheit in Deutschland, in: Rosenzweig, Beate/Eith, Ulrich (Hrsg.): Islamistischer Terrorismus. Hintergründe und Gegenstrategien (Wiesnecker Beiträge zu Politik und politischer Bildung: 4), Bad Schwalbach: Wochenschau Verlag, 119-149.

Löwisch, Georg 2007: Der Mann hinter der Schäublone, in: die tageszeitung (09.11.2007).

Lüdemann, Christian/Schlepper, Christina 2011: Der überwachte Bürger zwischen Apathie und Protest - Eine empirische Studie zum Widerstand gegen staatliche Kontrolle, in: Zurawski, Nils (Hrsg.):

Überwachungspraxen - Praktiken der Überwachung. Analysen zum Verhältnis von Alltag, Technik und Kontrolle, Opladen: Barbara Budrich, 119-138.

Merkel, Angela 2011: Bedrohung durch Terrorismus besteht fort. (Interview mit Passauer Neue Presse, 07.05.2001), in: http://www.bundesregierung.de/Content/DE/Interview/2011/05/2011-05-07-merkel-pnp.html; 10.05.2011.

Möllers, Martin H. W. 2009: Innenpolitische Dimension der Sicherheitspolitik in Deutschland, in: Böckenförde, Stephan/Gareis, Sven Bernhard (Hrsg.): Deutsche Sicherheitspolitik: Herausforderungen, Akteure und Prozesse, Opladen: Barbara Budrich, 131-172.

Moorstedt, Michael 2007: Schäublone auf dem Auto - Thomas im Visier der bayerischen Polizei, in: Süddeutsche Zeitung/Jetzt (17.09.2007).

Müller, Reinhard 2010: Merkel warnt vor einem „Vakuum", Frankfurter Allgemeine Zeitung, 02.03.2010, in: http://www.faz.net/artikel/C30923/karlsruhe-stoppt-vorratsdatenspeicherung-merkel-warnt-vor-einem-vakuum-30073936.html; 02.03.2010.

Pfeiffer, Christian 2011: Das Märchen von der brutalen Jugend, in: Süddeutsche Zeitung (23.05.2011).

Reißmann, Ole 2009: Demo gegen Überwachung. Loveparade für Bürgerrechte, Spiegel Online 01.08.2011, in: http://www.spiegel.de/netzwelt/netzpolitik/0,1518,648638,00.html; 12.09.2009.

Roßnagel, Alexander 2010: Die "Überwachungs-Gesamtrechnung" - Das BVerfG und die Vorratsdatenspeicherung, in: Neue Juristische Wochenschrift (NJW): 18, 1238-1242.

RP Online 2004: Februar: Von Siegen und Niederlagen, RP Online, in: http://www.rp-online.de/public/bildershowinline/aktuelles/panorama/4839?skip=0&refback=/|home; 21.05.2007.

Schulte, Dominik 2008: Terrorismus und Anti-Terrorismus-Gesetzgebung. Eine rechtssoziologische Analyse, Münster u.a.: Waxmann.

Schulte, Dominik 2010: Der Schutz individueller Rechte gegen Terrorlisten. Internationale, europäische und nationale Menschenrechtsstandards im Spannungsverhältnis zwischen effektiver Terrorbekämpfung und notwendigem Individualrechtsschutz, 1. Auflage. Baden-Baden: Nomos.

Schweda, Sebastian 2011: Umsetzungsunterschiede der Vorratsdatenspeicherungsrichtlinie in Europa - ein Bericht aus dem Forschungsprojekt InVoDaS im Mai 2011, in: Innere Sicherheit - auf Vorrat gespeichert? Tagungsband 2. SIRA Conference Series, 56-86.

Sennett, Richard/Sassen, Saskia 2007: Guantánamo in Germany. In the name of the war on terror, our colleagues are being persecuted - for the crime of sociology, 21.08.2007, in: http://www.guardian.co.uk/education/2007/aug/21/highereducation.uk1/print; 03.02.2011.

Skalli, Sami 2011: Zensus 2011. Inventur im Staat, Zeit online, 09.08.2011, in: http://www.zeit.de/zeit-wissen/2011/05/Zensus-Datenschutz; 09.08.2011.

Spiegel Online 2005: Schäuble will Foltergeständnisse nutzen, Spiegel Online, in: http://www.spiegel.de/politik/deutschland/0,1518,390708,00.html; 16.12.2005.

Szuba, Dorothee 2011: Vorratsdatenspeicherung. Der europäische und deutsche Gesetzgeber im Spannungsfeld zwischen Sicherheit und Freiheit, Baden-Baden: Nomos.

Tagesschau online 2010: Regelung verstößt gegen Grundgesetz. Karlsruhe kippt Vorratsdatenspeicherung, Tagesschau online 02.03.2010, in: http://www.tagesschau.de/inland/bundesverfassungsgericht144.html; 02.03.2010.

Uhl, Hans-Peter 2011: Grundsätze unserer Rechtsordnung gelten auch im Internet (Pressemitteilung 08.08.2011), CDU/CSU, 08.08.2011, in: http://www.cducsu.de/Titel__grundsaetze_unserer_rechtsordnung_gelten_auch_im_internet/TabID__6/SubTabID__7/InhaltTypID__1/InhaltID__19462/Inhalte.aspx; 10.08.2011.

Uwer, Thomas (Hrsg.) 2006: Bitte bewahren Sie Ruhe. Leben im Feindrechtsstaat, Berlin: Strafverteidigervereinigungen Organisationsbüro.

Vorsamer, Barbara 2007: Wie man unter Terrorverdacht gerät. Die Gedanken sind Freiwild, Süddeutsche Zeitung online 02.05.2011, in: http://www.sueddeutsche.de/politik/wie-man-unter-terrorverdacht-geraet-die-gedanken-sind-freiwild-1.881719; 22.08.2007.

Werkner, Ines-Jaqueline 2011: Die Verflechtung innerer und äußerer Sicherheit. Aktuelle Tendenzen in Deutschland im Lichte europäischer Entwicklungen., in: Zeitschrift für Außen- und Sicherheitspolitik 4: 1, 65-87.

ZDF 2011: Streit um Kontrolle des Internets ZDF heute journal 04.08.2011, in: http://www.zdf.de/ZDFmediathek/#/beitrag/video/1400390/Streit-um-Kontrolle-des-Internets; 01.08.2011.

Zeit online/dpa 2011: Politiker sehen im Internet eine Terrorgefahr, Zeit online 07.08.2011, in: http://www.zeit.de/politik/deutschland/2011-08/friedrich-anonymitaet-internet; 07.08.2011.

Sebastian Bukow ist wissenschaftlicher Mitarbeiter am Lehrstuhl für vergleichende Politikwissenschaft und Politikfeldanalyse (Politik I) an der Heinrich-Heine Universität Düsseldorf.
E-Mail: Sebastian.Bukow@uni-duesseldorf.de.

Sebastian Schweda

Umsetzungsunterschiede der Vorratsdatenspeicherungsrichtlinie in Europa - ein Bericht aus dem Forschungsprojekt InVoDaS im Mai 2011

Abstract

Durch die Richtlinie 2006/24/EG werden die Mitgliedstaaten der EU verpflichtet, nationale Regelungen zu schaffen, mit denen sichergestellt ist, dass bestimmte Telekommunikations-verbindungsdaten für einen gewissen Zeitraum auf Vorrat gespeichert werden. Die Richtlinie ist für alle EU-Mitgliedstaaten verbindlich, belässt jedoch schon innerhalb ihres Anwendungsbereichs erhebliche Umsetzungsspielräume. Zudem sind wesentliche Fragen im Zusammenhang mit der Vorratsdatenspeicherung, z. B. Abruf und Verwendung der gespeicherten Daten durch die Behörden, von der Richtlinie nicht geregelt. Dieser Beitrag gibt einen Überblick über die Unterschiede der nationalen Regelungen zur Vorratsspeicherung von Telekommunikationsdaten in den Mitgliedstaaten. Dargestellt werden der aktuelle Stand der Richtlinienumsetzung sowie die konkrete nationale Ausgestaltung ausgewählter Problemfelder mit Blick auf Titel und Ziel des vom EMR in Kooperation mit der Universität Kassel durchgeführten Forschungsprojekts „Interessenausgleich im Rahmen der Vorratsdatenspeicherung" (InVoDaS).

1. Einleitung

Es war das schnellste Rechtsetzungsverfahren in der Geschichte der Europäischen Union: Unter dem Eindruck der Bombenanschläge von London am 7.7.2005 und dem massiven Druck des Rates verabschiedete[1] das Europäische Parlament am 14.12.2005 den endgültigen Text der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung[2] (VDS-RL) – nur knapp drei Monate, nachdem ihm die Europäische Kommission den ersten Entwurf übermittelt hatte.[3]

[1] Legislative Entschließung des Europäischen Parlaments 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, 14.12.2005, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2005-0512+0+DOC+XML+V0//DE#BKMD-1.

[2] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 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, ABl. EU Nr. L 105 v. 13.4.2006, S. 54, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:DE:PDF.

[3] 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 endgültig. Zum Rechtsetzungsverfahren vgl. die Übersicht bei PreLex: http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=de&DosId=193330.

Bereits kurze Zeit nach den Terroranschlägen von Madrid am 11.3.2004 hatten Frankreich, Irland, Schweden und das Vereinigte Königreich dem Rat einen Vorschlag für einen Rahmenbeschluss vorgelegt, mit dem die Speicherung von Telekommunikationsdaten „für die Zwecke der Vorbeugung, Ermittlung, Aufdeckung und Verfolgung von Straftaten, einschließlich Terrorismus" geregelt werden sollte.[4] Der Entwurf stützte sich auf die Art. 31 Abs. 1 lit. c und 34 Abs. 2 lit. b EU[5], welche den Erlass von Rahmenbeschlüssen zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten im Bereich der justiziellen Zusammenarbeit vorsahen. Nachdem die Kommission jedoch darauf hingewiesen hatte, dass ein solcher Rahmenbeschluss nicht den gemeinschaftlichen Besitzstand, insbesondere nicht die Richtlinien 95/46/EG[6] (Datenschutzrichtlinie) und 2002/58/EG[7] (Datenschutzrichtlinie für elektronische Kommunikation), berühren dürfe, legte sie am 21.9.2005 einen eigenen Vorschlag für eine Richtlinie auf der Grundlage des Art. 95 EG vor.[8] Der Rat verfolgte die Annahme des Rahmenbeschlusses daraufhin nicht weiter, sondern beschloss – nachdem das Parlament hierzu Stellung genommen hatte – am 21.2.2006 die Richtlinie gegen die Stimmen Irlands und der Slowakischen Republik.[9]

---

[4] Dokument des Rates Nr. 8958/04 v. 28.4.2004, http://register.consilium.eu.int/pdf/de/04/st08/st08958.de04.pdf. Zur Entstehungsgeschichte der Vorratsdatenspeicherung in der EU vgl. Sebastian Bukow, Voratsdatenspeicherung in Deutschland - Symbol des sicherheitspolitischen Wandels und des zivilgesellschaftlichen Protests?, Tagungsband 2. SIRA Conference Series, 41ff.

[5] Soweit nicht anders vermerkt, sind mit den mit „EU" bzw. „EG" bezeichneten Verträgen der Vertrag über die Europäische Union bzw. der Vertrag zur Gründung der Europäischen Gemeinschaft in der Fassung des Vertrags von Nizza (ABl. EG Nr. C 80 v. 10.3.2001, S. 1, http://eur-lex.europa.eu/de/treaties/dat/12001C/pdf/12001C_DE.pdf) gemeint.

[6] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG Nr. L 281 v. 23.11.1995, S. 31, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html.

[7] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. EG Nr. L 201 v. 31.7.2002, S. 37, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:DE:PDF.

[8] KOM(2005) 438 endg., a. a. O. (Fn. 3).

[9] Dokument des Rates Nr. 6598/06 ADD 1 v. 27.2.2006, 2709, Tagung des Rates der Europäischen Union (Justiz und Inneres) am 21. Februar 2006 in Brüssel, Addendum zum Entwurf eines Protokolls, http://register.consilium.europa.eu/pdf/de/06/st06/st06598-ad01.de06.pdf.

Zu diesem Zeitpunkt existierten in einigen Mitgliedstaaten bereits verpflichtende Regelungen zur Vorratsspeicherung von Telekommunikationsverkehrs- und –standortdaten, die im Rahmen von Art. 15 Abs. 1 Richtlinie 2002/58/EG erlassen worden waren. Die Vorschrift erlaubt es den Mitgliedstaaten, unter anderem von der Pflicht des Art. 6 Richtlinie 2002/58/EG abzuweichen, nach der Verkehrsdaten zu löschen oder zu anonymisieren sind, sobald sie nicht mehr für die dort genannten Zwecke benötigt werden.[10] In anderen Mitgliedstaaten gab es derartige Speicherpflichten dagegen nicht. Mit dem Argument, die Bedingungen im Binnenmarkt angleichen zu wollen, hatte die Kommission ihren Richtlinienvorschlag deshalb auf Art. 95 EG gestützt.

Die beiden Staaten, die bei der Abstimmung im Rat gegen die Annahme der Richtlinie gestimmt hatten, hatten sich gegen die Wahl dieser Rechtsgrundlage gewandt. Sie kritisierten, die Richtlinie diene nicht schwerpunktmäßig der Angleichung von nationalen Rechtsvorschriften zur Förderung des Binnenmarktes, sondern der leichteren Verbrechensbekämpfung. Die Regelung hätte daher durch einen – im Unterschied zur Richtlinie einstimmig anzunehmenden – Rahmenbeschluss auf der o. g. Rechtsgrundlage erfolgen müssen. Irland erhob deshalb – mit Unterstützung durch die Slowakische Republik – Nichtigkeitsklage vor dem Gerichtshof der Europäischen Union (EuGH). Antragsgemäß befasste sich der Gerichtshof bei seiner Urteilsfindung lediglich mit der Wahl der Rechtsgrundlage und wies die Klage mit der Begründung ab, Art. 95 EG stelle eine tragfähige Rechtsgrundlage für die Richtlinie dar.[11] Der EuGH war nach materieller Prüfung der Richtlinienbestimmungen zu dem Schluss gelangt, dass sich diese „im Wesentlichen auf die Tätigkeiten der Diensteanbieter“ im Binnenmarkt beschränke und die Angleichung der nationalen Rechtsvorschriften in diesem Bereich

[10] Art. 15 Abs. 1 Satz 2 Richtlinie 2002/58/EG erlaubt ausdrücklich mitgliedstaatliche Rechtsvorschriften, nach denen Daten über einen begrenzten Zeitraum aufbewahrt werden. Voraussetzung ist, dass dies „für die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit oder die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist“, Art. 15 Abs. 1 Satz 1 Richtlinie 2002/58/EG.

[11] EuGH, Urt. v. 10.2.2009, Irland ./. Rat und Parlament, Rs. C-301/06, Slg. 2009, I-593, http://curia.europa.eu/jurisp/cgi-

bezwecke.[12] Im Unterschied zum Abkommen über die Weitergabe von Fluggastdaten an die USA (über das der EuGH bereits wenige Wochen vor Klageeinreichung geurteilt hatte[13]) enthalte die Richtlinie „keine Regelung der Handlungen staatlicher Stellen zu Strafverfolgungszwecken". Damit falle die Datenverarbeitung in den Anwendungsbereich der ebenfalls auf der Grundlage von Art. 95 EG erlassenen Richtlinie 95/46/EG.[14]

Zu den Zweifeln an der Wahl der richtigen Kompetenznorm gesellten sich jedoch schon während der Debatte um den Ratsbeschluss massive Zweifel hinsichtlich der Vereinbarkeit der Vorratsdatenspeicherung mit höherrangigem EU-Recht, insbesondere den Grundrechten, wie sie sich gemäß Art. 6 Abs. 2 EU aus der EMRK und den Verfassungsüberlieferungen der Mitgliedstaaten ergeben. Nach dem Inkrafttreten des Vertrags von Lissabon treten hierzu auch die Grundrechte der Europäischen Grundrechtecharta[15], insbesondere die Grundrechte auf Privatsphäre (Art. 14) und Datenschutz (Art. 15). Die Übereinstimmung der Richtlinie mit diesen Grundrechten ist gerichtlich bislang nicht umfassend geklärt. Unabhängig von der Frage der Grundrechtsfestigkeit der Richtlinie selbst verlangt auch ihre Umsetzung in den 27 EU-Mitgliedstaaten eine sorgfältige Abwägung der nach dem nationalen (Verfassungs-)Recht gewährten Grundrechte im Spannungsfeld der beteiligten Freiheits- und Sicherheitsinteressen.

2. Das Projekt InVoDaS

2.1 Überblick

Wie eine solche Abwägung in Deutschland bestmöglich gelingen kann, ist Gegenstand des Forschungsprojekts InVoDaS („Interessenausgleich im Rahmen der Vorratsdatenspeicherung"), das derzeit von der Projektgruppe verfassungs-

---

bin/gettext.pl?where=&lang=de&num=79909789C19060301&doc=T&ouvert=T&seance=ARRET_SOM.

[12] EuGH Urt. v. 10.2.2009, a. a. O. (Fn. 11), Rn. 80 ff.

[13] EuGH, Urt. v. 30.5.2006, Parlament ./. Rat und Kommission, Rs. C-317/04 und C-318/04, Slg. 2006, I-4721, http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=de&num=79939469C19040317&doc=T&ouvert=T&seance=ARRET.

[14] EuGH, Urt. v. 10.2.2009, a. a. O. (Fn. 11), Rn. 86 ff.

[15] Charta der Grundrechte der Europäischen Union, ABl. EU Nr. C 303 v. 14.12.2007, S. 1, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0001:0016:DE:PDF.

verträgliche Technikgestaltung (provet) der Universität Kassel und dem Institut für Europäisches Medienrecht (EMR) in Saarbrücken gemeinsam durchgeführt wird.

Das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte[16] Vorhaben nähert sich der Problematik von zwei Seiten: Einerseits wird durch provet analysiert, welchen verfassungsrechtlichen Beschränkungen ein erneuter Umsetzungsversuch[17] in Deutschland unterworfen wäre. Dabei setzt sich die Untersuchung insbesondere kritisch mit dem Urteil des Bundesverfassungsgerichts (BVerfG) vom 2.3.2010 auseinander, geht jedoch darüber hinaus auch auf dort nicht abschließend behandelte Fragen, etwa die einer möglichen Beeinträchtigung von Grundrechten der zur Speicherung verpflichteten Unternehmen, ein.

Andererseits wird die Studie durch einen Rechtsvergleich mit den Umsetzungsbestimmungen in den übrigen 26 EU-Mitgliedstaaten Lösungsansätze identifizieren, die im Hinblick auf den gewünschten Interessenausgleich besonders vielversprechend erscheinen (sog. „best practices"). Dazu wurden für jeden der Mitgliedstaaten Experten ausgewählt, die mit den nationalen Umsetzungsvorschriften besonders gut vertraut sind. Sie liefern in zwei Runden Antworten auf die vom EMR erarbeiteten Fragebögen, in denen die konkrete Nutzung der Regelungsspielräume in dem jeweiligen Mitgliedstaat sowie die verfassungsrechtlichen Grundlagen und die soziale Einbettung der Problematik erfragt werden. Die ausgefüllten Fragebögen werden durch das EMR ausgewertet und anhand einer gewichteten Matrix miteinander verglichen. Aus dem Rechtsvergleich werden zum einen „Steckbriefe" zu allen 26 analysierten EU-Mitgliedstaaten hervorgehen, die einen schnellen Überblick über die nationalen Regelungen zur Umsetzung der Richtlinie 2006/24/EG geben. Zum anderen wird aus der Vielzahl der nationalen Lösungen zu den unterschiedlichen Fragestellungen eine Zusammenstellung der identifizierten „best practices" erarbeitet, die für die weiteren Projektschritte zur Verfügung stehen wird.

---

[16] Die Finanzierung durch das BMBF erfolgt aus Mitteln des Forschungsprogramms „Forschung für die zivile Sicherheit" der Bundesregierung im Rahmen der Förderbekanntmachung „Gesellschaftliche Dimensionen der Sicherheitsforschung"; vgl. http://www.bmbf.de/foerderungen/13124.php, http://www.bmbf.de/de/13979.php.

[17] Zur Vorgeschichte der deutschen Umsetzungsbemühungen sogleich (vgl. Abschnitt 3).

Ziel ist es, durch beide Projektteile den von der VDS-RL grundsätzlich belassenen Gestaltungsspielraum genauer zu definieren und auf Lösungen zu verengen, die das Interesse an einer effizienten Gewährleistung ziviler Sicherheit einerseits und das Interesse an einem effektiven Schutz der betroffenen Freiheitsrechte andererseits zu einem bestmöglichen Ausgleich bringen. Aus diesen Ergebnissen wird das Projekt Gestaltungsempfehlungen ableiten, die für den Fall einer Neuregelung der Vorratsdatenspeicherung in Deutschland eine möglichst grundrechtsschonende Verwirklichung der Richtlinienvorgaben ermöglichen. Es ist vorgesehen, das im Mai 2010 gestartete Projekt bis Ende Oktober 2011 abzuschließen.

2.2 Der Rechtsvergleich

Der vorliegende Beitrag beschränkt sich im Wesentlichen auf die Darstellung der vorläufigen Ergebnisse aus dem zweiten Projektteil. In den nachfolgenden Abschnitten wird zunächst auf die Situation in Deutschland eingegangen (3.). Im Anschluss wird ein Überblick über die verschiedenen Lösungsansätze in den übrigen Mitgliedstaaten gegeben (4.). In einem abschließenden Ausblick (5.) werden die zu erwartenden Entwicklungen auf EU-Ebene, die auch die weitere Debatte in Deutschland prägen werden, dargestellt.

3. Situation in Deutschland

Art. 15 Abs. 1 VDS-RL sieht eine Pflicht zur Umsetzung der Richtlinienbestimmungen in den Mitgliedstaaten bis 15.9.2007 vor. Sofern ein Mitgliedstaat dies bei Verabschiedung der Richtlinie gemäß Art. 15 Abs. 3 VDS-RL erklärt hat, durfte er die Anwendung der VDS-RL auf die Speicherung von Internetdaten[18] gemäß Art. 15 Abs. 3 Satz 1 VDS-RL bis zum 15.3.2009 aufschieben.

Mit leichter Verspätung trat in Deutschland am 1.1.2008 ein Gesetz[19] in Kraft, mit dem u. a. das Telekommunikationsgesetz (TKG) und die Strafprozessordnung (StPO) geändert wurden. Das Gesetz sah – in einem neu einzuführenden § 113a TKG – die

[18] Mit „Internetdaten" sind die in Art. 15 Abs. 3 VDS-RL genannten „Kommunikationsdaten betreffend Internetzugang, Internet-Telefonie und Internet-E-Mail" gemeint.

[19] Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, BR-Drs. 798/07 v. 9.11.2007, http://dipbt.bundestag.de/dip21/brd/2007/0798-07.pdf.

Speicherung der in Art. 5 VDS-RL genannten Daten für einen Zeitraum von sechs Monaten vor. Das Inkrafttreten der Vorschriften über die Speicherung von Internetdaten war gemäß § 150 Abs. 12 TKG bis zum 1.1.2009 aufgeschoben worden.
Die Verwendung der Daten war nach dem – durch das Gesetz ebenfalls neu geschaffenen – § 113b TKG nicht nur zur Verfolgung von Straftaten, sondern grundsätzlich auch „zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit" (Satz 1 Nr. 2) und „zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes" (Satz 1 Nr. 3) zulässig. Eine Rechtsgrundlage für den Datenzugriff stellte diese Vorschrift nicht dar; eine solche war in den jeweiligen das Behördenhandeln regelnden Gesetzen vorzusehen. Für Datenerhebungen zum Zwecke der Strafverfolgung etwa enthielt diese § 100g StPO i. d. F. des Umsetzungsgesetzes. Entsprechende Befugnisnormen wurden für den Bereich der Gefahrenabwehr in den Polizeigesetzen einiger Länder geschaffen.[20]
Auf die Verfassungsbeschwerde von mehr als 34.000 Personen[21] hin hat das Bundesverfassungsgericht (BVerfG) zunächst in mehreren, zeitlich aufeinanderfolgenden einstweiligen Anordnungen die Verwendung der gespeicherten Daten stark eingeschränkt.[22] Mit Urteil vom 2.3.2010[23] erklärte das Gericht das Umsetzungsgesetz schließlich für nichtig, da es gegen das in Art. 10 GG geregelte Telekommunikationsgeheimnis verstoße. Das Gericht führte aus, bei der anlasslosen Speicherung von Telekommunikationsverbindungsdaten handle es sich um einen „besonders schweren Eingriff mit einer Streubreite, wie sie die

[20] Vgl. BVerfG, Beschluss v. 28.10.2008, 1 BvR 256/08, BGBl. I 2008, 2239, http://www.bverfg.de/entscheidungen/rs20081028_1bvr025608.html, Rn. 8 ff.
[21] Die Beschwerdeschrift und weitere Verfahrensdokumente sind veröffentlicht unter: http://www.vorratsdatenspeicherung.de/content/view/51/70/lang,de/. Angaben des Arbeitskreises Vorratsdatenspeicherung zufolge ist dies die Verfassungsbeschwerde mit der bislang größten Anzahl an Beschwerdeführern in der Geschichte des Bundesverfassungsgerichts.
[22] BVerfG, Beschluss v. 11.3.2008, 1 BvR 256/08, BGBl. I 2008, 659, http://www.bundesverfassungsgericht.de/entscheidungen/rs20080311_1bvr025608.html, wiederholt durch Beschluss v. 1.9.2008, BGBl. I 2008, 1850, wiederholt und erweitert durch Beschluss v. 28.10.2008, a. a. O. (Fn. 20), zuletzt wiederholt mit Beschluss v. 15.10.2009, BGBl. I 2009, 3704.
[23] BVerfG, Urt. v. 2.3.2010, 1 BvR 256/08, BGBl. I. 2010, 272, http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html.

Rechtsordnung bisher nicht kennt".[24] Eine derart breit angelegte Speicherung ohne konkreten Anlass schaffe beim Bürger ein „diffus bedrohliches Gefühl des Beobachtetseins".[25] Zugleich stellte das BVerfG jedoch fest, dass eine verfassungskonforme Umsetzung der VDS-RL durchaus möglich sei. In ungewohnter Detailtiefe beschreibt das Urteil sodann, welchen Kriterien eine solche Umsetzung genügen muss. Dabei geht das Gericht auch auf zu ergreifende technische und organisatorische Maßnahmen ein, mit denen Datenschutz und Datensicherheit zu gewährleisten sind.[26] Darüber hinaus seien verhältnismäßige gesetzliche Regelungen zu den Verwendungszwecken der Daten sowie zu Transparenz, effektivem Rechtsschutz und effektiven Sanktionen vorzusehen.[27] Mit Blick auf die Kostentragungspflicht der zur Speicherung verpflichteten Unternehmen sah das Gericht keinen unverhältnismäßigen Eingriff in das Recht auf Berufsfreiheit gemäß Art. 12 GG.[28] Auf eine Vorlage unionsrechtlicher Fragen an den EuGH, auf die verschiedentlich spekuliert worden war, verzichtete das BVerfG, weil die Wirksamkeit der VDS-RL „nicht entscheidungserheblich" sei.[29] Die Richtlinie könne „ohne Verstoß gegen die Grundrechte des Grundgesetzes umgesetzt werden".[30] Die Verfassungswidrigkeit des Umsetzungsgesetzes ergibt sich dem Urteil zufolge nicht aus der Umsetzung zwingender VDS-RL-Bestimmungen, sondern aus der konkreten Ausfüllung des von der VDS-RL belassenen Gestaltungsspielraums.

4. Rechtsvergleich

Die bisherige Analyse der rechtlichen Situation in den übrigen 26 EU-Mitgliedstaaten im Rahmen von InVoDaS hat erhebliche Abweichungen sowohl hinsichtlich des Umsetzungsstands als auch hinsichtlich der konkreten Ausgestaltung der nationalen Regelungen gezeigt. Letztere beziehen sich einerseits auf die von der Richtlinie explizit eröffneten Spielräume – etwa bei der Speicherungsfrist –, andererseits auf diejenigen Teile einer umfassenden Regelung der Vorratsdatenspeicherung, die von

[24] BVerfG, Urt. v. 2.3.2010, a. a. O. (Fn. 23), Rn. 210.
[25] BVerfG Urt. v. 2.3.2010, a. a. O. (Fn. 23), Rn. 212.
[26] BVerfG, Urt. v. 2.3.2010, a. a. O. (Fn. 23), Rn. 221 ff.
[27] BVerfG, Urt. v. 2.3.2010, a. a. O. (Fn. 23), Rn. 226 ff., 239 ff.
[28] BVerfG, Urt. v. 2.3.2010, a. a. O. (Fn. 23), Rn. 293 ff.
[29] BVerfG, Urt. v. 2.3.2010, a. a. O. (Fn. 23), Rn. 186.

der Richtlinie gar nicht umfasst sind – etwa die Frage, welche staatlichen Stellen unter welchen Voraussetzungen zur Erhebung der auf Vorrat gespeicherten Daten berechtigt sind. Erwägungsgrund 25 VDS-RL schließt Rechtsvorschriften über den Zugang zu den Vorratsdaten und deren Nutzung explizit vom Regelungsbereich der Richtlinie aus, da die Verarbeitung dieser Daten durch nationale Behörden zu Zwecken der Strafverfolgung zum Zeitpunkt der Verabschiedung der Richtlinie nicht vom Anwendungsbereich des Gemeinschaftsrechts umfasst war. Auf diesen Bereich durfte sich eine Harmonisierung auf der Grundlage von Art. 95 EG also nicht erstrecken. Das Inkrafttreten des Vertrags von Lissabon hat dies geändert; die bisher in der sog. „Dritten Säule" verorteten Regelungsgegenstände sind nun „unionisiert", eine reformierte Richtlinie könnte diese Fragen daher nun regeln.

Der folgende Abschnitt (4.1) gibt einen Überblick über den aktuellen Umsetzungsstand. Sodann wird zu einer Auswahl verschiedener Regelungskriterien auf dem Gebiet der Vorratsdatenspeicherung die Bandbreite der identifizierten Lösungsansätze in den übrigen 26 EU-Mitgliedstaaten dargestellt (4.2).

4.1. Umsetzungsstand

In 24 der 26 untersuchten Mitgliedstaaten bestand seit dem Inkrafttreten der VDS-RL zumindest zeitweise eine nationale Umsetzungsregelung. Während in Belgien bereits vor Inkrafttreten der Richtlinie eine teilweise Speicherung von Verbindungsdaten vorgenommen wurde, die allerdings nicht vollständig mit den Vorgaben der VDS-RL übereinstimmt, hat sich Schweden der Umsetzung bislang komplett entzogen. In einem Vertragsverletzungsverfahren, das die Europäische Kommission am 27.11.2007 gegen den Mitgliedstaat eingeleitet hatte, stellte der EuGH mit Urteil vom 4.2.2010 fest, dass Schweden seinen Verpflichtungen aus der VDS-RL nicht nachgekommen war.[31] Im Dezember desselben Jahres legte die schwedische Regierung nach einem weiteren Aufforderungsschreiben der Kommission dem

[30] BVerfG, Urt. v. 2.3.2010, a. a. O. (Fn. 23), Rn. 187.
[31] EuGH, Urt. v. 4.2.2010, Kommission ./. Schweden, Rs. C-185/09, http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=fr&num=79899795C19090185&doc=T&ouvert=T&seance=ARRET.

Riksdag einen Gesetzentwurf[32] vor, mit dem dieser Vertragsverletzung abgeholfen werden sollte. Auf der Grundlage eines verfassungsrechtlichen Schutzinstruments[33] beschloss das schwedische Parlament jedoch in seiner Sitzung vom 16.3.2011, das Gesetzgebungsverfahren wegen verfassungsrechtlicher Bedenken für ein Jahr ruhen zu lassen. Bei der Abstimmung war die für eine Fortsetzung notwendige 5/6-Mehrheit knapp verfehlt worden.[34] Damit ist eine Umsetzung der Richtlinie in Schweden nicht vor dem März 2012 möglich. Das Parlament nahm in Kauf, dass der Mitgliedstaat in einem zweiten, von der Kommission kurz darauf eingeleiteten Verfahren vor dem EuGH zur Zahlung eines Bußgeldes für jeden Tag der Nichtumsetzung verurteilt wird. Die Kommission fordert in ihrer Klageschrift die Festsetzung einer pauschalen Geldbuße von EUR 9.597 täglich für den Zeitraum zwischen den Verkündungen des ersten und des zweiten Urteils. Für jeden weiteren Tag der Nichtumsetzung nach dem zweiten Urteil verlangt sie die Zahlung eines Zwangsgeldes von EUR 40.947,20.[35]

Als nicht umgesetzt lässt sich auch die in Belgien bislang bestehende Rechtslage beschreiben: In dem Mitgliedstaat bestand eine Regelung über die Vorratsdaten-speicherung in engen Grenzen zwar bereits vor der Verabschiedung der VDS-RL[36],

---

[32] *Regeringens proposition* 2010/11:46 v. 3.12.2010, *Lagring av trafikuppgifter för brottsbekämpande ändamål – genomförande av direktiv 2006/24/EG*,
http://www.sweden.gov.se/content/1/c6/15/74/33/3dc07bbd.pdf.

[33] Mit der sog. *„underställning"*, die in Kap. 2 § 22 Abs. 2 Regeringsformen (einem Teil der schwedischen Verfassung) geregelt ist, kann ein Gesetzentwurf, der Eingriffe in bestimmte Grundrechte vorsieht, für mindestens zwölf Monate zurückgestellt werden, wenn mindestens zehn Abgeordnete dies verlangen und der *Riksdag* sich nicht mit einer 5/6-Mehrheit gegen diesen Antrag ausspricht.

[34] *Riksdag*, Sitzungsprotokoll v. 16.3.2011,
http://www.riksdagen.se/webbnav/?nid=101&bet=2010/11:73.

[35] Europäische Kommission, Klageschrift v. 31.5.2011, Kommission ./. Schweden, Rs. C-270/11,
http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?where=&lang=de&num=79889284C19110270&doc=T&ouvert=T&seance=REQ_COMM.

[36] Königliche Verordnung v. 9.1.2003, *Moniteur belge* v. 10.2.2003, S. 6625,
http://www.ejustice.just.fgov.be/mopdf/2003/02/10_2.pdf (*Arrêté royal déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques*) i. d. F. der Königlichen Verordnung v. 8.2.2011 (*Arrêté royal modifiant l'arrêté royal du 9 janvier 2003 portant exécution des articles 46bis, § 2, alinéa 1er, 88bis, § 2, alinéas 1er et 3, et 90quater, § 2, alinéa 3 du Code d'instruction criminelle ainsi que de l'article 109ter , E , § 2, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques*), *Moniteur belge* v. 23.2.2011, S. 12962,
http://www.ejustice.just.fgov.be/mopdf/2011/02/23_1.pdf. Streng genommen ist die Rechtsgrundlage für diese Verordnung bereits entfallen, da Art. 109ter, E, § 2, Gesetz v. 21.3.1991 aufgehoben wurde. Dennoch findet die Verordnung in der Praxis weiter Anwendung, wohl unter Verweis auf den 2005 in Kraft getretenen Art. 126 des Gesetzes über elektronische Kommunikation.

diese entspricht jedoch in ihrem Umfang bei weitem nicht den Vorgaben der VDS-RL. Art. 126 des belgischen Gesetzes über elektronische Kommunikation enthält eine Ermächtigungsgrundlage für den Erlass einer Rechtsverordnung zur Umsetzung der Richtlinienvorgaben, was bislang jedoch nicht geschehen ist. Heftige Kritik seitens der Zivilgesellschaft und der von einer Speicherungspflicht betroffenen Unternehmen hatte die Verabschiedung eines ersten, sehr weitreichenden und teils über die Richtlinie hinausgehenden Entwurfs aus dem Jahre 2008 verhindert. Mit einer Verabschiedung der neuen, bereits weit fortgeschrittenen Entwürfe ist erst nach der Bildung einer neuen Föderalregierung zu rechnen, die in dem Land bereits über ein Jahr andauert. Seit April 2010 ist die amtierende Regierung in ihrer Gestaltungsmacht auf die „laufenden Angelegenheiten" beschränkt.

Mit Beschlüssen vom 28.4.2011 und 12.5.2011 haben in Österreich Nationalrat und Bundesrat Gesetzesvorlagen zur Änderung des Telekommunikationsgesetzes[37] (TKG 2003), der Strafprozessordnung und des Sicherheitspolizeigesetzes[38] (SPG) angenommen, mit denen die Vorgaben der VDS-RL erfüllt und der Zugang zu den auf dieser Grundlage gespeicherten Daten geregelt werden sollen. Die Änderungsgesetze treten allerdings erst zum 1.4.2012 in Kraft. Durch diese Legisvakanz hat das Land, in dem die Vorratsdatenspeicherung seit Anbeginn sehr kritisch gesehen worden war, Zeit gewonnen und gleichzeitig die Verurteilung zur Zahlung eines Bußgeldes in einem weiteren[39] Vertragsverletzungsverfahren vorerst abgewendet. Es ist zu vermuten, dass das Parlament durch diesen Schachzug die weitere Entwicklung der Thematik auf europäischer Ebene abwarten wollte, um hohe Kosten – insbesondere vor dem Hintergrund ihrer gesetzlich vorgesehenen

[37] Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird, BGBl. I Nr. 27/2011 v. 18.5.2011, http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA_2011_I_27

[38] Bundesgesetz, mit dem die Strafprozessordnung 1975 und das Sicherheitspolizeigesetz geändert werden, BGBl. I Nr. 33/2011 v. 20.5.2011, http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA_2011_I_33. Das SPG regelt die Befugnisse der Polizei im Bereich der Gefahrenabwehr.

[39] In einem ersten Verfahren hatte der EuGH bereits festgestellt, dass Österreich durch die Nichtumsetzung gegen Unionsrecht verstoßen hat; vgl. EuGH, Urt. v. 29.7.2010, Kommission ./. Österreich, Rs. C-189/09, http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?where=&lang=de&num=79899173C19090189&doc=T&ouvert=T&seance=ARR_COMM.

partiellen Erstattung durch den Staat[40] – für die Installation von Speicherungsanlagen, die sich bei einer späteren Reform der Richtlinie als ungeeignet herausstellen könnten, zu vermeiden.

In zwei Mitgliedstaaten hat das nationale Verfassungsgericht – ähnlich wie in Deutschland – eine bereits erfolgte Umsetzungsregelung wieder gekippt: Bereits am 8.10.2009 entschied das rumänische Verfassungsgericht, dass das Gesetz Nr. 298/2008, mit dem in dem Land eine Vorratsdatenspeicherung eingeführt worden war, mit in der Verfassung verankerten Grundrechten und mit Art. 8 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) nicht vereinbar sei.[41]

In Tschechien urteilte das Verfassungsgericht am 31.3.2011, dass Teile der nationalen Regelung zur Vorratsdatenspeicherung (Art. 97 Abs. 3 und 4 Gesetz Nr. 127/2005 Coll. über elektronische Kommunikation, geändert durch Gesetz Nr. 247/2008, und die auf dieser Grundlage erlassene Verordnung Nr. 485/2005) gegen die Verfassung verstoßen, und ordnete ihre Aufhebung an.[42] Das Gericht hält die Vorschriften für zu unpräzise; insbesondere seien keine ausreichenden Bestimmungen zur Gewährleistung der Datensicherheit vorhanden. Die Regelung entspreche daher nicht den Erfordernissen des Rechtsstaats ("rule of law") und stelle einen nicht verfassungsgemäßen Eingriff in das Grundrecht auf Privatheit in der Ausprägung des Rechts auf informationelle Selbstbestimmung, wie aus Art. 10 Abs. 3 und Art. 13 der tschechischen Grundrechtecharta abgeleitet, dar. Dies ergebe sich aus dem Verhältnismäßigkeitsgrundsatz.

Eine verfassungsrechtliche Prüfung in Frankreich durch den *Conseil constitutionnel* hatte dagegen ergeben, dass die französische Umsetzungsregelung im Wesentlichen verfassungskonform war. Insbesondere sah das Gericht keinen Verstoß gegen das Verhältnismäßigkeitsprinzip.[43]

---

[40] Siehe dazu Abschnitt 4.2.5.

[41] Verfassungsgerichthof Rumäniens (*Curtea Constituțională a României*), Entscheidung Nr. 1258 v. 28.10.2009, http://www.ccr.ro/decisions/pdf/ro/2009/D1258_09.pdf, deutsche Übersetzung abrufbar unter: http://www.vorratsdatenspeicherung.de/content/view/342/1/lang,de/#Urteil.

[42] Verfassungsgerichtshof der Tschechischen Republik (*Ústavní Soud*), Urt. v. 22.3.2011, Pl. ÚS 24/10, http://www.concourt.cz/clanek/GetFile?id=5075 (tschech. Orig.-Fsg.), http://www.concourt.cz/view/pl-24-10 (engl. Übers.).

[43] Verfassungsrat (*Conseil constitutionnel*), Entscheidung Nr. 2005-532 v. 19.1.2006, *Journal officiel* v. 24.1.2006, S. 1138, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-

Nach einem Urteil des bulgarischen Obersten Verwaltungsgerichts[44], das die Definition der Verwendungszwecke sowie der Datenkategorien, auf die zugegriffen werden darf, als zu vage angesehen und daher für verfassungswidrig erklärt hatte, wurde die Regelung überarbeitet.

Unklar ist die Rechtslage in Zypern. Dort hatte der Oberste Gerichtshof am 1.2.2011 in einem verbundenen Verfahren entschieden, dass mehrere gerichtliche Anordnungen zur Herausgabe auf Vorrat gespeicherter Daten an die Polizei gegen das Kommunikationsgeheimnis gemäß Art. 17 der Zyprischen Verfassung verstoßen.[45] Art. 17 Abs. 2 zufolge durfte das Kommunikationsgeheimnis nur eingeschränkt werden in Bezug auf die Kommunikation von Häftlingen, geschäftliche Korrespondenz und die Kommunikation von Zahlungsunfähigen während der Insolvenzverwaltung. Nach einer Entscheidung des Gerichts von 1983 darf das Kommunikationsgeheimnis darüber hinaus auch bei privaten Kommunikationen mit Einwilligung des Betroffenen sowie bei Kommunikationen, die unter Verwendung verbotener Kommunikationsmittel durchgeführt werden, beschränkt werden. Diese engen verfassungsrechtlichen Vorgaben reduzieren die praktischen Verwendungsmöglichkeiten für die auf Vorrat gespeicherten Daten erheblich. Das Gericht entschied, dass die genannten Voraussetzungen in den gegenständlichen Fällen nicht vorlagen und eine Herausgabe der Daten daher verfassungswidrig war.

Die gerichtlichen Anordnungen, um die es in dem Fall ging, waren auf der Grundlage von Art. 4 und 5 des zyprischen Umsetzungsgesetzes zur VDS-RL (Gesetz Nr. 183(1)/2007) ergangen. Diese Bestimmungen über den Zugang zu den Vorratsdaten liegen nach Auffassung des Gerichts außerhalb des Regelungsbereichs der VDS-RL, da diese nur Vorschriften zu den Speicherpflichten der

---

decisions/acces-par-date/decisions-depuis-1959/2006/2005-532-dc/decision-n-2005-532-dc-du-19-janvier-2006.979.html.

[44] Bulgarisches Oberstes Verwaltungsgericht (*Върховен административен съд*), Entscheidung Nr. 13627 v. 11.12.2008, Verw.-Rs. Nr. 11799/2008, http://www.econ.bg/law86421/enactments/article153902.html. Das Gericht rügte eine Verletzung von Art. 8 EMRK sowie von Art. 32 (Recht auf Unverletzlichkeit des persönlichen Lebens) und Art. 34 der bulgarischen Verfassung.

[45] Oberster Gerichtshof Zyperns (*Ανώτατο Δικαστήριο Κύπρου*), Urt. v. 1.2.2011, Zivil-Rs. Nr. 65/2009, 78/2009, 82/2009 und 15/2010-22/2010,

Telekommunikationsunternehmen enthält, nicht aber zu Fragen des Zugangs zu den Daten. Explizit hält das Gericht fest, dass die VDS-RL nur die Aktivitäten der Dienstanbieter im Binnenmarkt betrifft und keine staatlichen Tätigkeiten gemäß Titel VI EU (Polizeiliche und justizielle Zusammenarbeit in Strafsachen) regelt. Damit betrifft das Urteil die Richtlinienbestimmungen nicht und steht daher auch nicht in Konflikt mit dem Unionsrecht.

Die Entscheidung basierte allerdings auf der Fassung des Art. 17 der Zyprischen Verfassung vor einer am 4.6.2010 bekanntgemachten Änderung, derzufolge ein Eingriff in das Kommunikationsgeheimnis u. a. nun auch dann zulässig ist, wenn er den Zugang zu Verkehrs- oder Standortdaten betrifft und gerichtlich angeordnet wird zur Untersuchung schwerer Straftaten, die mit einer Freiheitsstrafe von mehr als fünf Jahren bedroht sind. Es ist daher anzunehmen, dass der Oberste Gerichtshof auf der Grundlage des Art. 17 der Zyprischen Verfassung in der aktuell geltenden Fassung den Fall anders entschieden hätte. Das Urteil hat jedoch Wirkung *erga omnes* und wirkt sich daher auch grundsätzlich auf die Geltung der nationalen Umsetzungsregelung aus.

Gerichtlich überprüft werden derzeit die Umsetzungsregime in Irland[46], Polen[47] und Ungarn[48]. Aus dem irischen Verfahren werden auch Impulse für die weitere Entwicklung der Vorratsdatenspeicherung in der EU insgesamt erwartet, da der mit dem Fall befasste High Court am 5.5.2010 die Vorlage des Falles zum EuGH zugelassen hat.[49] Seitdem bemüht sich das Gericht im Austausch mit den Parteien der Bürgerrechtsorganisation Digital Rights Ireland und der Regierung von Irland,

---

http://www.supremecourt.gov.cy/judicial/sc.nsf/All/5B67A764B86AA78EC225782F004F6D28/$file/65-09.pdf.

[46] *Digital Rights Ireland Ltd.*, Klage v. 14.9.2006, *Digital Rights Ireland Ltd. ./. The Minister for Communications, Marine and Natural Resources et al.*, http://www.mcgarrsolicitors.ie/wp-content/Files/Statement%20of%20claim.pdf.

[47] Die Verfassungsbeschwerde wurde am 28.1.2011 von einer Gruppe Parlamentsabgeordneter der Sozialdemokratischen Partei Polens beim Verfassungsgericht eingereicht. Die Beschwerdeschrift ist abrufbar unter: http://www.sld.org.pl/download/index/biblioteka/393.

[48] Die Verfassungsbeschwerde wurde am 15.3.2008 von der *Hungarian Civil Liberties Union* beim Verfassungsgericht eingereicht; vgl. http://tasz.hu/en/data-protection/constitutional-complaint-filed-hclu-against-hungarian-telecom-data-retention-regulat.

[49] *The High Court*, Beschluss v. 5.5.2010, *Digital Rights Ireland Ltd. ./. The Minister for Communications, Marine and Natural Resources et al.*, Az. 2006/3785P, im Entwurf abrufbar unter: http://www.scribd.com/doc/30950035/Data-Retention-Challenge-Judgment-re-Preliminary-Reference-Standing-Security-for-Costs.

um die richtige Formulierung der Vorlagefragen. Es ist unklar, wann mit der Einleitung des Vorabentscheidungsverfahrens zu rechnen ist.[50]

4.2. Ausgestaltung der Regelung

In diesem Abschnitt werden die bestehenden nationalen Umsetzungsunterschiede anhand von neun Regelungskategorien exemplarisch aufgezeigt. Dargestellt werden Abweichungen in den mitgliedstaatlichen Regelungen hinsichtlich der Speicherungsfrist, der zu speichernden Datenkategorien, der Wirkung von Beweisverboten auf Speicherungspflicht und Zugriffsrechte, des Kreises der Speicherungsverpflichteten, der Erstattung der mit der Vorratsdatenspeicherung verbundenen Kosten, des technischen Datenschutzes, der Zugriffsvoraussetzungen, der Rechte der Betroffenen sowie der zuständigen Aufsichtsbehörden. Soweit dies sinnvoll erscheint, sollen dabei bemerkenswerte Ansätze herausgegriffen und eingehender beschrieben werden.

4.2.1. Speicherungsfrist

Die Richtlinie selbst belässt den Mitgliedstaaten einen weiten Spielraum hinsichtlich der Frist, innerhalb derer die Daten von den TK-Unternehmen vorzuhalten sind: Gemäß Art. 3 VDS-RL müssen die Mitgliedstaaten vorsehen, dass die in Art. 5 VDS-RL spezifizierten Datenkategorien für einen Zeitraum gespeichert werden, der sechs Monate nicht unterschreiten und zwei Jahre nicht überschreiten darf. Die Mitgliedstaaten haben von dieser Spannbreite umfassend Gebrauch gemacht: Sieben Mitgliedstaaten sehen eine Pflicht zur Speicherung dieser Daten für sechs Monate vor[51]; in elf Mitgliedstaaten beträgt diese Frist zwölf Monate.[52] Eine achtzehnmonatige Frist sieht Lettland vor; für 24 Monate sind die Daten in Polen zu

[50] Im März 2011 berichtete der Vorsitzende von *Digital Rights Ireland*, man warte noch immer auf die Übermittlung der Fragen des *High Court* an den EuGH; vgl. http://www.tjmcintyre.com/2011/03/analysis-of-new-data-retention-act.html?showComment=1301138112801#c6880021108044179654.

[51] Litauen, Luxemburg, Österreich, Rumänien, Schweden, Tschechische Republik, Zypern. Bezüglich Rumänien, der Tschechischen Republik und Zypern bezieht sich diese Angabe auf die Rechtslage vor den unter 4.1 dargestellten Gerichtsentscheidungen, bezüglich Schweden auf den Regierungsentwurf. Die Regelung in Österreich tritt erst am 1.4.2012 in Kraft.

speichern. In einigen Mitgliedstaaten finden sich differenzierende Regelungen: So sind den gesetzlichen Vorgaben in Irland, Italien, Slowenien und der Slowakischen Republik zufolge Internetdaten für einen kürzeren Zeitraum (zwischen sechs und zwölf Monate) zu speichern als Verkehrs- und Standortdaten über Telefonie im Festnetz und Mobilfunknetz (zwischen zwölf und 24 Monate). Die maltesische Umsetzungsregelung sieht eine Speicherung von Internetzugangs- und Internet-Email-Daten für sechs Monate vor, während die übrigen Daten – inklusive Internet-Telefonie-Daten – für zwölf Monate gespeichert werden. Erfolglose Anrufversuche sind in Ungarn nur für sechs Monate zu speichern, während alle anderen Daten für ein Jahr vorzuhalten sind. In einigen Ländern kann die Speicherungsfrist auch verlängert oder verkürzt werden.[53] Dabei kann gemäß dem in Belgien derzeit diskutierten Entwurf grundsätzlich auch die Zwei-Jahres-Grenze überschritten werden, wenn die Kommission und die übrigen Mitgliedsstaaten hiervon benachrichtigt werden. Eine solche Verlängerung ist wohl als richtlinienkonform zu beurteilen: Art. 12 VDS-RL gestattet es einem Mitgliedstaat, für einen begrenzten Zeitraum „die notwendigen Maßnahmen" zu ergreifen, wenn „besondere Umstände" es rechtfertigen, die maximale Speicherungsfrist über die in Art. 6 VDS-RL genannte Höchstfrist hinaus zu verlängern. Der Mitgliedstaat hat die Europäische Kommission und die übrigen Mitgliedstaaten davon in Kenntnis zu setzen. Die Regelung gilt als gebilligt, wenn die Kommission innerhalb von sechs Monaten keine Entscheidung trifft. Im Falle einer Billigung „kann die Kommission prüfen, ob sie eine Änderung der Richtlinie vorschlägt" (Art. 12 Abs. 3 VDS-RL). Ein entsprechendes Verfahren für den Fall, dass ein Mitgliedstaat eine Verkürzung der Speicherungsfrist für gerechtfertigt hält, ist in der Richtlinie nicht vorgesehen.

4.2.2. Datenkategorien

In vielen Mitgliedstaaten besteht die Beschreibung der zu speichernden Datenkategorien in einer wörtlichen Übernahme des Art. 5 VDS-RL oder einer nur in

---

[52] Belgien, Bulgarien, Dänemark, Estland, Finnland, Frankreich, Griechenland, Niederlande Portugal, Spanien, Vereinigtes Königreich. Bezüglich Belgien bezieht sich diese Angabe auf den zuletzt diskutierten Regierungsentwurf.

[53] Entsprechende Regelungen bestehen z. B. in Belgien, Estland, Litauen, Spanien und Zypern.

Details (die zumeist mit Besonderheiten des jeweiligen nationalen Rechtsrahmens zu tun haben) abweichenden Formulierung. Teils bedurfte es jedoch auch einer aufwendigeren Einpassung in die mitgliedstaatliche Regelung. Materielle Abweichungen waren damit in der Regel jedoch nicht verbunden. Insgesamt dürften im Bereich der zu speichernden Datenkategorien die Unterschiede der nationalen Regelungen am geringsten sein, was auch an den in diesem Punkt vergleichsweise klaren Vorgaben der VDS-RL liegt.[54]

Eine Ausnahme in dieser Hinsicht stellt das französische Umsetzungsgesetz[55] dar: Es sieht lediglich eine grobe Unterteilung der zu speichernden Datenkategorien vor, die weniger spezifisch als die VDS-RL selbst bleibt. Für Anbieter von Internetzugangsdiensten und Hosting-Diensten bestehen dagegen weitere Speicherungspflichten, die über die Vorgaben von Art. 5 VDS-RL hinausgehen.[56] Diese umfassen etwa die verwendeten Nutzer- und Endgerätekennungen, Details zu

---

[54] Damit ist noch keine Aussage über die oftmals schwierige Frage getroffen, wie die einzelnen Begriffe angesichts der technischen Gegebenheiten in der Praxis zu interpretieren sind. Beispielsweise enthält die gesetzliche Definition der zu speichernden Datenkategorien in der Regel keine Festlegung, wann etwa von einer „An- und Abmeldung beim Internet-E-Mail-Dienst" gemäß Art. 5 Abs. 1 lit. c) Nr. 2 ii) VDS-RL gesprochen werden kann, insbesondere inwieweit hierbei die Kommunikation über Webmail-Schnittstellen und/oder Mail-Transportprotokolle wie POP3, IMAP und SMTP erfasst sind. Sofern diese Fragen auf nationaler Ebene zu klären sind, obliegt diese technische Aufgabe üblicherweise den mit der Implementierung der gesetzlichen Vorschriften betrauten Behörden. Mit der Konkretisierung der Begriffe befasst sich zudem auf EU-Ebene eine von der Kommission eingerichtete Expertengruppe; vgl. Beschluss der Kommission vom 25.3.2008 zur Einsetzung der Sachverständigengruppe „Vorratsspeicherung von elektronischen Daten zum Zwecke der Verhütung, Ermittlung, Feststellung und Verfolgung von schweren Straftaten", ABl. EU Nr. L 111 v. 23.4.2008, S. 11, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:111:0011:0014:DE:PDF.

[55] Vgl. Art. R10-13, R10-14 des Gesetzbuches für Post und elektronische Kommunikation (*Code des Postes et des Communications Electroniques*, konsolidierte Fassung unter: http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070987), eingefügt durch Dekret Nr. 2006-358 v. 24.3.2006 (*Décret n° 2006-358 relatif à la conservation des données des communications électroniques*, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000637071&dateTexte=), auf der Grundlage von Art. L34-1 des Gesetzbuches für Post und elektronische Kommunikation, geändert durch Gesetz Nr. 2004-669 v. 9.7.2004 (*Loi n° 2004-669 relative aux communications électroniques et aux services de communication audiovisuelle*, konsolidierte Fassung unter: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000439399). Ähnlich auch die belgische Regelung, die die wesentlichen Regelungen einer Verordnung überlässt, die bislang allerdings nicht in Kraft gesetzt wurde; vgl. Abschnitt 4.1.

[56] Art. 6 II Gesetz Nr. 2004-575 v. 21.6.2004 (*Loi n°2004-575 pour la confiance dans l'économie numérique*, konsolidierte Fassung unter: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005789847), Art. 1 Verordnung Nr. 2011-219 vom 25.2.2011 (*Décret n° 2011-219 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne*, konsolidierte Fassung unter: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023646013).

Verbindungsart und Zahlungsvorgängen sowie bestimmte Bestandsdaten, zu denen auch das aktuelle Passwort zählt. Es ist zumindest zweifelhaft, ob eine solche Regelung mit der VDS-RL, die jedenfalls für die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste eine grundsätzlich abschließende und harmonisierte Regelung treffen will, noch in Einklang zu bringen ist.

4.2.3. Beweisverbote

Die Straf- und Zivilprozessordnungen aller untersuchten Mitgliedstaaten räumen – ebenso wie die deutschen – bestimmten Personengruppen das Recht ein, die Aussage im Straf- bzw. Zivilverfahren zu verweigern. Diese Zeugnisverweigerungsrechte werden nicht nur z. B. Angehörigen des Angeklagten (bzw. der Klageparteien), sondern auch sog. Berufsgeheimnisträgern zugestanden, zu denen sich der Betroffene in einem besonderen Vertrauensverhältnis befindet. Zu diesem Kreis können, je nach Ausgestaltung der nationalen Regelung, beispielsweise Anwälte, Ärzte, Geistliche oder Journalisten zählen. Soweit diese Personengruppen einer gesetzlichen Verschwiegenheitspflicht unterliegen, stellt sich das Zeugnisverweigerungsrecht als logische Ergänzung hierzu dar, das ihre Stellung als Berufsgeheimnisträger stärkt: Durch das Zeugnisverweigerungsrecht sind sie in der Lage, ihrer Verschwiegenheitspflicht auch vor Gericht nachzukommen (vgl. im deutschen Recht z. B. § 53 StPO, § 383 ZPO als Ergänzung zu § 203 StGB).

Im Strafverfahren unterliegen Gegenstände, auf die sich das Zeugnisverweigerungsrecht der Geistlichen, Anwälte und Ärzte gemäß § 53 StPO bezieht, einschließlich schriftlicher Mitteilungen zwischen dem Beschuldigten und dem Geheimnisträger, gemäß § 97 StPO einem Beschlagnahmeverbot. Darüber hinaus sind sämtliche Ermittlungsmaßnahmen gegen einige der mit einem Zeugnisverweigerungsrecht ausgestatteten Berufsgeheimnisträger unzulässig, es sei denn, die Person ist selbst der Straftat oder einer Unterstützungstat verdächtig (§ 160a StPO).[57] Damit sind grundsätzlich auch Verbindungsdaten, die über

[57] § 160a StPO wurde mit Wirkung vom 1.2.2011 durch das Gesetz zur Stärkung des Schutzes von Vertrauensverhältnissen zu Rechtsanwälten im Strafprozessrecht (BGBl. I 2010, 2261, http://www.bundesgerichtshof.de/SharedDocs/Downloads/DE/Bibliothek/Gesetzesmaterialien/17_wp/Vertrauen/bgbl120102261.pdf) geändert und erweitert das bis dato nur für Geistliche, Strafverteidiger und Abgeordnete geltende Beweisverwertungsverbot auch auf Rechtsanwälte, die keine Strafverteidiger sind.

Telekommunikationsvorgänge Auskunft geben, die beispielsweise ein Anwalt mit dem Beschuldigten geführt hat, den strafrechtlichen Ermittlungen entzogen. Wie dies im Rahmen der Vorratsdatenspeicherung in der Praxis zu handhaben ist, ist allerdings unklar.

Konkrete Lösungsansätze aus anderen Mitgliedstaaten sind rar. Lediglich in Österreich sind zu dieser Frage im Rahmen der Gesetzgebungsverfahren verschiedene Möglichkeiten erörtert worden. Diskutiert wurde u. a. die Einrichtung einer „Clearing-Stelle", die überwachen sollte, ob die Abfragen auch Daten umfassen, die zu solchen Vertrauensbeziehungen gehören. Der Ansatz fand jedoch keinen Eingang in die beschlossenen Änderungsgesetze. Begründet wurde dies mit Datenschutzbedenken wegen der dafür erforderlichen zentralen Speicherung einer Liste aller Berufsgeheimnisträger bei einer einzigen Stelle. Statt dessen sieht § 93 Abs. 5 Satz 1 TKG 2003 nach der zum 1.4.2012 in Kraft tretenden Änderung vor, dass „(d)as Redaktionsgeheimnis (§ 31 Mediengesetz) sowie sonstige, in anderen Bundesgesetzen normierte Geheimhaltungsverpflichtungen ... nach Maßgabe des Schutzes der geistlichen Amtsverschwiegenheit und von Berufsgeheimnissen sowie das Verbot deren Umgehung gemäß §§ 144 und 157 Abs. 2 StPO zu beachten" sind. Die genannten Bestimmungen der StPO verbieten die Umgehung der Zeugnisverweigerungsrechte von Berufsgeheimnisträgern und der Amtsverschwiegenheit Geistlicher durch Beschlagnahme, Sicherstellung oder andere Ermittlungsmaßnahmen und stellen damit ein Beweiserhebungsverbot dar. Ob ein solches Verbot besteht, ist von der abfragenden Stelle bzw. dem anordnenden Gericht zu prüfen. Den Diensteanbieter trifft insoweit keine Prüfpflicht (vgl. § 93 Abs. 5 Satz 2 TKG 2003).

4.2.4. Kreis der zur Speicherung verpflichteten Personen

Der Kreis der zur Speicherung verpflichteten Personen ist von der Richtlinie mittelbar vorgegeben: Art. 3 Abs. 1 VDS-RL verpflichtet die Mitgliedstaaten sicherzustellen, „dass die in Artikel 5 der vorliegenden Richtlinie genannten Daten, soweit sie im Rahmen ihrer Zuständigkeit im Zuge der Bereitstellung der betreffenden Kommunikationsdienste von Anbietern öffentlich zugänglicher

elektronischer Kommunikationsdienste oder Betreibern eines öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, gemäß den Bestimmungen der vorliegenden Richtlinie auf Vorrat gespeichert werden." Die von den genannten Netzbetreibern bzw. Dienstanbietern erzeugten oder verarbeiteten Daten können in dieser Form auch nur von diesen zur Verfügung gestellt werden. In den meisten Mitgliedstaaten sind daher diese beiden Personengruppen als Verpflichtete der nationalen Umsetzungsregelungen genannt. Allerdings haben einige Mitgliedstaaten den Kreis der Verpflichteten weiter eingegrenzt: So verpflichten etwa Finnland und Österreich lediglich die Dienstanbieter, nicht aber die Netzbetreiber.[58] Im Vereinigten Königreich sieht Nr. 10 Abs. 1 der Data Retention (EC Directive) Regulations 2009 vor, dass nur die Unternehmen zur Speicherung verpflichtet sein sollen, die von der Regierung besonders benachrichtigt werden.[59] In allen genannten Fällen soll durch die Beschränkung – was auch die Richtlinie als Ziel nennt[60] – eine Doppelspeicherung derselben Daten bei mehreren Unternehmen vermieden werden. In vielen Mitgliedstaaten sind zudem Ausnahmen, etwa für kleinere Anbieter, vorgesehen. So sind in Österreich Anbieter von der Speicherungspflicht ausgenommen, „deren Unternehmen nicht der Verpflichtung zur Entrichtung des Finanzierungsbeitrages gemäß § 10 KommAustriaG unterliegen".[61] Derzeit sind dies Unternehmen mit einem Jahresumsatz von weniger als 315.000 EUR.

4.2.5. Kostenerstattung

Die Beschaffung und Installation der zur Speicherung erforderlichen Anlagen, aber auch der laufende Betrieb und die Auskunfterteilung an die abfrageberechtigten

---

[58] § 102a Abs. 1 Telekommunikationsgesetz 2003 i. d. F. des Bundesgesetzes, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird, a. a. O. (Fn. 37): „Anbieter von öffentlichen Kommunikationsdiensten".

[59] *Data Retentions (EC Directive) Regulations 2009*, Nr. 859, http://www.legislation.gov.uk/uksi/2009/859/contents/made. Gemäß Nr. 10 Abs. 2 *Data Retention (EC Directive) Regulations 2009* sind aber alle Unternehmen zu benachrichtigen, sofern nicht die Daten bereits durch ein anderes Unternehmen gespeichert werden. Zur Umsetzung der VDS-RL im Vereinigten Königreich Susanne Beck, Vorratsdatenspeicherung und aktuelle Entwicklungen in der Inneren Sicherheit im Vereinigten Königreich - eine Analyse im Mai 2011, Tagungsband 2. SIRA Conference Series, 87ff.

[60] Erwägungsgrund 13 VDS-RL.

[61] Art. § 102a Abs. 6 TKG 2003 i. d. F. des Bundesgesetzes, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird, a. a. O. (Fn. 37).

Stellen verursachen für die von der Speicherungspflicht betroffenen Unternehmen Aufwendungen. Insbesondere die beträchtlichen Kosten für die Anfangsinvestitionen in neue Speichertechnologie hatten bei den verpflichteten Unternehmen und Branchenvertretern in etlichen Mitgliedstaaten zu heftiger Kritik geführt.

In vielen Mitgliedstaaten erhalten die Unternehmen die Kosten im Zusammenhang mit der Vorratsdatenspeicherung vom Staat nicht ersetzt. Einige Staaten sehen zumindest eine Erstattung der für die Übermittlung der Daten an die Behörden im Einzelfall anfallenden Kosten vor. Eine Kostenerstattung für die Auskunfterteilung im Strafverfahren sieht auch eine am 1.7.2009 in Kraft getretene Änderung des deutschen Justizvergütungs- und –entschädigungsgesetz vor.[62] Für die Investition in neue Speicheranlagen und deren Betrieb existieren im deutschen Recht dagegen keine gesonderten Erstattungsregeln.

Dagegen werden diese Kosten vor allem in den Mitgliedstaaten erstattet, die zugleich auch bei der Definition der Speicherungsverpflichteten auf ein „Datenvermeidungsmodell" setzen: Dem reduzierten Kreis der Telekommunikationsunternehmen, die in Österreich, Finnland und dem Vereinigten Königreich der Speicherungspflicht unterliegen, werden die Aufwendungen im Zusammenhang mit der Anschaffung der neuen Speicherungsanlagen vollständig bzw. – im Falle Österreichs – zumindest zu einem wesentlichen Teil (80°%) vom Staat ersetzt. Auf diese Weise lässt sich Befürchtungen begegnen, eine Speicherungspflicht, die nur für einige Unternehmen gilt, könne zu Wettbewerbsverzerrungen führen.

Auch in der Tschechischen Republik wurden den verpflichteten Unternehmen die Kosten für Anfangsinvestitionen, laufenden Betrieb und Auskunftserteilung separat ersetzt. Um die Erstattungsregeln für die Unternehmen nachvollziehbar zu machen, wurden die Einzelheiten, einschließlich genau festgelegter Kalkulationsregeln für die

[62] Art. 1 Gesetz zur Neuordnung der Entschädigung von Telekommunikationsunternehmen für die Heranziehung im Rahmen der Strafverfolgung (TK-Entschädigungs-Neuordnungsgesetz - TKEntschNeuOG) vom 29.4.2009, BGBl. I S. 994, http://www.bgbl.de/Xaver/media.xav?SID=anonymous3130531291123&bk=Bundesanzeiger_BGBl&name=bgbl%2FBundesgesetzblatt%20Teil%20I%2F2009%2FNr.%2024%20vom%2006.05.2009%2Fbgbl109s0994.pdf.

Höhe der erstattungsfähigen Investitionskosten, in einer – Flexibilität und Rechtssicherheit zugleich bietenden – Verordnung geregelt.[63]

4.2.6. Bestimmungen zu Datenschutz und Datensicherheit

Art. 7 VDS-RL verlangt von den Mitgliedstaaten, dass sie „unbeschadet der zur Umsetzung der Richtlinien 95/46/EG und 2002/58/EG erlassenen Vorschriften" bestimmte Mindestvorgaben hinsichtlich Datenqualität, Datenintegrität, Zugang zu den Daten und ihrer sicheren Löschung machen. Die Vorschrift ist von etlichen Mitgliedstaaten mehr oder weniger wortgleich übernommen worden, ohne dabei näher zu spezifizieren, wie dies im Einzelnen geschehen soll. Auch freiwillige Leitlinien zu den speziell auf dem Gebiet der Vorratsdatenspeicherung zu beachtenden Bestimmungen für den technischen Datenschutz sind in den meisten Mitgliedstaaten nicht zu finden. So bleibt es letztlich den Unternehmen selbst überlassen, wie sie die sehr allgemein formulierten rechtlichen Vorgaben in der Praxis umsetzen. Die Regelungen in Belgien[64] und Luxemburg[65] verweisen zum Teil auf technische Vorschriften und Normen, die bereits für den Bereich der Telekommunikationsüberwachung geschaffen wurden. Die französische Datenschutzbehörde (*Commission Nationale de l'Informatique et des Libertés*, CNIL) hat einen umfangreichen Leitfaden zur Datensicherheit veröffentlicht, der allerdings weder spezielle Vorschriften zur Vorratsdatenspeicherung zu enthalten scheint noch rechtlich verbindlich ist.[66] Ausführliche Regeln im Bereich der Telekommunikationsüberwachung die auch auf die Vorratsdatenspeicherung angewandt werden, finden sich in Italien und Spanien; Die sichere

---

[63] § 150 Abs. 5 des Gesetzes Nr. 127/2005 Coll. über elektronische Kommunikation i. V. m. Verordnung Nr. 486/2005 vom 7.12.2005.

[64] Art. 6 Abs. 3 des Entwurfs für eine Königliche Verordnung zur Festlegung der Modalitäten der Pflicht zur rechtlichen Zusammenarbeit bei gerichtlichen Anfragen bezüglich elektronischer Kommunikation nennt zahlreiche ETSI-Normen zur rechtmäßigen Überwachung (*lawful interception*) und zur Definition von Schnittstellen für die Datenübermittlung an die Behörden, die in diesem Zusammenhang zu beachten sind.

[65] *Institut Luxembourgeois de Régulation* (ILR), Verordnung 08/134/ILR v. 1.12.2008 (*Règlement relatif aux spécifications techniques pour l'interception des communications électroniques au Luxembourg*), *Mémorial* – ABl. des Großherzogtums Luxemburg, A – Nr. 188, v. 18.12.2008, 2556, http://www.legilux.public.lu/leg/a/archives/2008/0188/a188.pdf#page=4.

[66] CNIL, *Guide – La Sécurité des Données Personelles*, 2010, http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite-VD.pdf.

Datenübermittlung ist Gegenstand untergesetzlicher Normen in Portugal und Slowenien. Die getroffenen Regelungen werden im Rahmen der zweiten Berichtsrunde einer vertieften Betrachtung unterzogen. Dennoch lässt sich schon jetzt sagen, dass die **vorgesehenen** technischen und organisatorischen Maßnahmen eine hilfreiche Vorlage auch für eine Umsetzung der Richtlinie in Deutschland unter Beachtung der diesbezüglichen Vorgaben des BVerfG sein könnenDie Regelungen sehen u. a. Maßnahmen vor, mit denen eine separate Speicherung der Vorratsdaten, ihr physischer Schutz sowie ihre sichere Verschlüsselung gewährleistet werden sollen. Darüber hinaus sind Regeln zur Begrenzung und Protokollierung des Zugriffs auf die Daten und zu deren revisionssicherer Löschung enthalten.

4.2.7. Besondere Zugriffsvoraussetzungen

Art. 1 VDS-RL zufolge sind die Daten „zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten" vorzuhalten. Auch die Richtlinie selbst erwähnt jedoch weitere Zwecke, zu denen diese Daten gespeichert werden können. Erwägungsgrund 4 verweist explizit auf die Ausnahmegründe des Art. 15 Richtlinie 2002/58/EG, nach denen u. a. vom grundsätzlichen Speicherungsverbot des Art. 6 Richtlinie 2002/58/EG zur Aufrechterhaltung der öffentlichen Ordnung abgewichen werden darf. Diese Gründe umfassen neben der Strafverfolgung auch die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit und die Verhütung von Straftaten. In zahlreichen Mitgliedstaaten wurde von dieser Möglichkeit Gebrauch gemacht und eine Speicherungspflicht etwa auch zu Präventionszwecken eingeführt.[67] Teilweise wird eine Speicherung zwar ausschließlich zur Strafverfolgung vorgeschrieben, die Daten können später aber auch für weitere Zwecke verwendet werden.[68] In anderen Mitgliedstaaten findet eine klare Zweckfestlegung bei der Speicherung überhaupt nicht statt.[69] Derartige Zweckerweiterungen bzw. -unbestimmtheiten sind unter dem Gesichtspunkt des

[67] So z. B. in Frankreich, Polen oder Ungarn.
[68] Ensprechende Regelungen bestehen in Luxemburg und Rumänien. Strikte Begrenzungen auf die Zwecke der Ermittlung, Feststellung und Verfolgung von Straftaten enthalten dagegen die Umsetzungsnormen in Dänemark, Italien, Litauen, Portugal, der Slowakischen Republik und Zypern
[69] So z. B. in Estland, in der Tschechischen Republik und im Vereinigten Königreich.

Zweckbindungsgrundsatzes gemäß Art. 6 Abs. 1 lit. c der Datenschutzrichtlinie (Richtlinie 95/46/EG) nicht unproblematisch.

Zu den Unterschieden bei der Zweckbestimmung kommen erhebliche Abweichungen bei den jeweiligen Zugriffsvoraussetzungen. Während der Zugriff in einigen Mitgliedstaaten überhaupt keinen ernstzunehmenden Einschränkungen unterliegt[70] oder jedenfalls keine Eingrenzung erfolgt ist hinsichtlich der Straftaten, zu deren Ermittlung, Feststellung bzw. Verfolgung auf die Daten zugegriffen werden kann,[71] existieren in anderen Mitgliedstaaten Definitionen des Begriffs der „schweren Straftat", die vorliegen muss, um eine Abfrage der Vorratsdaten zu rechtfertigen. Auch dieser Begriff ist jedoch nicht einheitlich definiert. Teils umfasst er enumerativ in einem besonderen Katalog aufgelistete Straftaten,[72] wobei diese Kataloge jedoch nicht länderübergreifend miteinander abgeglichen sind. Teils wird auf bestimmte Strafrahmen Bezug genommen. So fordert etwa die niederländische Regelung das Vorliegen einer Straftat, für die eine Höchstfreiheitsstrafe von mindestens vier Jahren vorgesehen ist.[73] In anderen Ländern orientiert sich der Begriff an bestimmten Mindeststrafen.[74]

---

[70] So etwa in Ungarn, wo der Zugriff auf die Vorratsdaten durch die jeweils berechtigten Behörden lediglich „zur Erfüllung ihrer Aufgaben" erforderlich sein muss (vgl. Art. 159/A Gesetz über elektronische Kommunikation), ohne dass in den die jeweilige behördliche Aufgabe regelnden Normen besondere Voraussetzungen für eine Datenabfrage geregelt sind.

[71] Im Vereinigten Königreich etwa existiert diesbezüglich keine nähere Eingrenzung. Art. 2 des „*Acquisition and Disclosure of Communications Data: Code of Practice*", der auf der Grundlage von § 71 des *Regulation of Investigatory Powers Act 2000* (RIPA 2000) ausgearbeitet wurde, verlangt lediglich allgemein, dass der Abruf von Kommunikationsdaten „notwendig und verhältnismäßig und im Einklang mit dem Gesetz" ist und dass die anfragende Stelle auch glaubt, dass diese Voraussetzungen vorliegen.

[72] Vgl. z. B. Art. 16 des (inzwischen insgesamt für verfassungswidrig erklärten) rumänischen Gesetzes Nr. 298/2008, das zur Rechtfertigung des Zugangs zu Vorratsdaten ernsthafte Informationen oder Anzeichen über die Vorbereitung einer schweren Straftat oder deren erfolgte Begehung erfordert. In Art. 2 Abs. 1 lit. f des Gesetzes ist der Begriff der „schweren Straftat" definiert als Straftat, die zu den in Art. 2 Abs. b des Gesetzes Nr. 39/2003 zur Verhütung und Verfolgung der organisierten Kriminalität (unabhängig von einer organisierten Begehungsweise), in Kap. 4 des Gesetzes Nr. 535/2004 zur Verhütung und Verfolgung des Terrorismus oder zu den in Titel I des Besonderen Teils des Gesetzes Nr. 15/1968 (Strafgesetzbuch) genannten Straftaten gegen die nationale Sicherheit zählen.

[73] Art. 67 des niederländischen Strafprozessgesetzbuchs (*Wetboek van Strafvordering*).

[74] So etwa in Malta, wo die Tat mit einer Freiheitsstrafe von mindestens einem Jahr bedroht sein muss; vgl. Art. 19 Abs. 1 i. V. m. Art. 17 der *Processing of Personal Data (Electronic Communications Sector) Regulations* (S.L. 440.01). Strengere Strafrahmenbestimmungen sehen z. B. die Regelungen in Dänemark und Litauen vor, die nur Straftaten umfassen, für deren Begehung eine Freiheitsstrafe von mindestens sechs Jahren vorgesehen ist.

Im Bereich der weiteren Verwendungszwecke war ein Muster überhaupt nicht auszumachen. In vielen Fällen sind die Zugriffsvoraussetzungen so weit formuliert, dass sie den Handlungsspielraum der zugriffsberechtigten Behörden nicht ernsthaft beschränken.

4.2.8. Rechte der Betroffenen

Um die Rechte der Personen, deren personenbezogene Daten bei einem Datenabruf betroffen sind, ausreichend zu gewährleisten, existieren in den Mitgliedstaaten unterschiedliche Schutzvorschriften. Die meisten Staaten verlangen vor dem Abruf der Daten zu Zwecken der Strafverfolgung den Erlass einer entsprechenden richterlichen Anordnung.[75] Auch dort, wo ein Zugriff auf die Daten in Zivilverfahren möglich ist, lässt das Gesetz dies regelmäßig nur nach vorherigem gerichtlichem Beschluss zu. Soweit auf die Daten allerdings auch zu anderen Zwecken zugegriffen werden darf, sind derartige Schutzvorkehrungen rar.[76] Zumeist bleibt es der abrufberechtigten Behörde in diesen Fällen selbst überlassen, die Rechtmäßigkeit einer Abfrage zu beurteilen; eine Überprüfung der behördlichen Entscheidung ist dann allenfalls nachträglich im Wege eines gerichtlichen Verfahrens möglich.[77]

Soweit der Betroffene zur Wahrung seiner Rechtsposition selbst handeln muss, ist Voraussetzung, dass er von dem Eingriff in seine Grundrechte überhaupt erfährt. Im Rahmen des Projekts wird daher auch untersucht, inwieweit nach dem nationalen Recht Anhörungsrechte vor einem Datenabruf sowie vorherige oder nachträgliche Benachrichtigungspflichten oder Auskunftsrechte bestehen. Nahezu ausnahmslos haben die Mitgliedstaaten von einem vorherigen Anhörungsrecht des Betroffenen abgesehen, wohl um den Zweck einer in der Regel verdeckt ablaufenden Ermittlungsmaßnahme nicht zu gefährden. Auch auf andere Weise findet eine Benachrichtigung vor dem Datenabruf in aller Regel nicht statt. Zumeist wird dem

[75] Ausgenommen sind in einigen Ländern (z. B. in Dänemark und Griechenland) Fälle besonderer Eilbedürftigkeit, in denen eine richterliche Bestätigung erst im Nachhinein innerhalb einer bestimmten Zeit erfolgen muss.

[76] Vgl. hierzu schon Abschnitt 4.2.7.

[77] Ein besonders prominentes Beispiel ist die französische Behörde HADOPI (*Haute Autorité pour la diffusion des œuvres et la protection des droits sur l'Internet*), die Urheberrechtsverletzungen im Internet ahnden soll. Die zur Etmittlung des Anschlussinhabers erforderlichen Verkehrsdaten kann die

Betroffenen frühestens in dem Moment, in dem er sich in einem Strafverfahren als Beschuldigter zu verteidigen hat, eröffnet, dass er auf der Grundlage einer Auswertung von Vorratsdaten einer Straftat verdächtig ist. Werden die Ermittlungen ohne Erhebung einer Anklage abgeschlossen, unterbleibt eine Benachrichtigung üblicherweise.

Nach Art. 12 Richtlinie 95/46/EG steht dem Betroffenen darüber hinaus zwar ein generelles datenschutzrechtliches Auskunftsrecht zur Seite. Dessen Anwendung unterliegt jedoch im nationalen Recht vielfach Ausnahmen, die gerade in den hier betreffenden Fällen eingreifen (wie auch von Art. 13 Richtlinie 95/46/EG zugelassen), nämlich im Bereich der Strafverfolgung und –verhütung sowie der nationalen Sicherheit. Eine Änderung könnte hier erst der aktuell laufende Prozess zur Reform des EU-Datenschutzrechts[78] herbeiführen. Der Europäische Datenschutzbeauftragte (EDPS) hat sich dafür ausgesprochen, Art. 13 ebenso restriktiv auszulegen wie andere Ausnahmebestimmungen. Die besonderen Schutzvorschriften der Richtlinie 95/46/EG müssten zudem auch im nationalen Recht zur polizeilichen und justiziellen Zusammenarbeit beachtet werden.[79]

Sofern dem Betroffenen die Ermittlungsmaßnahme bekannt wird, kann er sich zumeist rechtlich dagegen zur Wehr setzen. Neben häufig bestehenden datenschutz- oder telekommunikationsrechtlichen Rechtsbehelfen gegen eine Verletzung von Datenschutzvorschriften, die u. a. die Untersuchung durch den Datenschutzbeauftragten und die Verhängung von Bußgeldern vorsehen, können nach den mitgliedstaatlichen Vorschriften fast immer auch zivilrechtliche Schadensersatzansprüche geltend gemacht werden. Schwere Verstöße sind in einigen Ländern unter Strafe gestellt.[80] Zudem können verschiedentlich auch

---

Behörde ohne weitere Prüfung durch eine unabhängige Stelle von den speichernden Unternehmen abfragen.

[78] Vgl. Mitteilung der Europäischen Kommission v. 4.11.2010 an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Gesamtkonzept für den Datenschutz in der Europäischen Union, KOM(2010) 609, http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_de.pdf.

[79] EDPS, Stellungnahmen des Europäischen Datenschutzbeauftragten zur Mitteilung der Europäischen Kommission v. 4.11.2010, ABl. EU Nr. C 181 v. 22.6.2011, S. 1, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:181:0001:0023:EN:PDF.

[80] So z. B. in Finnland, Portugal, Rumänien und Schweden.

strafprozessuale Rechtsmittel (etwa eine Beschwerde) in einem gegen den Betroffenen laufenden Strafverfahren eingelegt werden.[81]

4.2.9. Aufsichtsbehörden

Grundsätzlich ist für die Einhaltung der telekommunikationsrechtlichen Vorschriften die nach Art. 8 Richtlinie 2002/21/EG[82] (Rahmenrichtlinie) einzurichtende nationale Regulierungsbehörde für elektronische Kommunikation (NRA) zuständig, während über die Beachtung der Datenschutzbestimmungen die gemäß Art. 28 Richtlinie 95/46/EG einzurichtende Datenschutzbehörde (DPA) des Mitgliedstaats wacht. Speziell für die Kontrolle der Anwendung der gemäß Art. 7 VDS-RL zu erlassenden Bestimmungen über Datenschutz und Datensicherheit verlangt Art. 9 VDS-RL die Benennung mindestens einer öffentlichen Stelle. Diese kann mit der DPA identisch sein (vgl. Art. 9 Abs. 1 Satz 2 VDS-RL). In jedem Fall muss aber gesichert sein, dass die Stelle ihre Aufgaben „in völliger Unabhängigkeit" wahrnimmt (Art. 9 Abs. 2 VDS-RL).

Einige Mitgliedstaaten sehen eine geteilte Zuständigkeit vor, bei der die DPA die Aufgabe der Kontrollstelle gemäß Art. 9 VDS-RL übernimmt, während die Umsetzung der Richtlinie im Übrigen von der NRA überwacht wird.[83] Andere Mitgliedstaaten haben die Datenschutzbehörde mit sämtlichen Kontrollaufgaben im Zusammenhang mit der Umsetzung der Richtlinie betraut und so eine einheitliche Aufsichtsbehörde für alle mit der Vorratsdatenspeicherung zusammenhängenden Fragen geschaffen.[84] Die faktische Unabhängigkeit der Aufsichtsbehörden wird sehr unterschiedlich bewertet, der vom Unionsrecht geforderte Unabhängigkeitsgrad (vgl. Art. 28 Abs. 1 UAbs. 2 Richtlinie 95/46/EG und Art. 3 Abs. 2 Richtlinie 2002/21/EG) scheint in der Praxis nicht in allen Mitgliedstaaten gewährleistet. Die Aufsichts- und Kontrollstrukturen im Tätigkeitsbereich der abrufberechtigten

[81] So z. B. in Luxemburg und den Niederlanden.
[82] Richtlinie 2002/21/EG über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und –dienste (Rahmenrichtlinie), ABl. EG Nr. L 108 v. 24.4.2002, S. 33, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:108:0033:0033:DE:PDF.
[83] So z. B. in Estland, Litauen (hier teilt sich die NRA die Zuständigkeit hinsichtlich der Einhaltung der Speicherungspflichten mit dem Staatssicherheitsministerium), Polen und den Niederlanden.
[84] So z. B. in Italien, Lettland, Malta und die vormalige Regelung in Rumänien.

Behörden sind derzeit Gegenstand weitergehender Untersuchung im Rahmen des Projekts InVoDaS.

4. Ausblick

Auch fünf Jahre nach ihrer Verabschiedung ist die Richtlinie in sechs Mitgliedstaaten noch nicht – oder nicht mehr – (vollständig) umgesetzt. Die Europäische Kommission hat deshalb gegen mehrere Mitgliedstaaten – darunter Österreich[85], Schweden[86], Rumänien und Deutschland[87] – Vertragsverletzungsverfahren eingeleitet. Im Falle Schwedens ist dies bereits das zweite Verfahren wegen der Nichtumsetzung der Richtlinie vor dem EuGH; diesmal muss das Land mit der Verhängung von Strafgeldern rechnen.[88]

Gleichzeitig hat die Kommission in ihrem Evaluationsbericht[89] vom 18.4.2011 auch in den Mitgliedstaaten, in denen die Richtlinie umgesetzt ist, erhebliche Defizite bei der Zielerreichung festgestellt. Insbesondere sei bislang weder eine ausreichende Harmonisierung der Rechtsvorschriften noch eine Angleichung der Wettbewerbsbedingungen der Telekommunikationsunternehmen festzustellen.[90] Dies liegt nicht nur an den weiten Spielräumen, die die Richtlinie in den von ihr geregelten Fragen belässt.[91] Viel schwerer wiegt, dass wesentliche Regelungsbereiche von der Richtlinie ausgeklammert blieben – und aufgrund der damaligen Rechtslage

---

[85] EuGH, Urt. v. 29.7.2010, Kommission ./. Österreich, Rs. C-189/09, http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?where=2006%2F24&lang=de&num=79899270C19090189&doc=T&ouvert=T&seance=ARRET.

[86] EuGH, Urt. v. 4.2.2010, Kommission ./. Schweden, Rs. C-185/09, http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?where=2006%2F24&lang=de&num=79899795C19090185&doc=T&ouvert=T&seance=ARRET_DR.

[87] Hierzu hat die Kommission Rumänien und Deutschland am 16.6.2011 ein Aufforderungsschreiben geschickt; vgl. http://ec.europa.eu/eu_law/eulaw/decisions/dec_20110616.htm.

[88] Zu beiden Verfahren siehe schon Abschnitt 4.1.

[89] Bericht der Kommission v. 18.4.2011 an den Rat und das Europäische Parlament – Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung (Richtlinie 2006/24/EG), KOM(2011), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:DE:PDF.

[90] Bericht der Kommission v. 18.4.2011, a. a. O. (Fn. 89), S. 38.

[91] Die Kommission weist in diesem Zusammenhang darauf hin, dass die Richtlinie selbst nicht garantiere, „dass auf Vorrat gespeicherte Daten in voller Übereinstimmung mit dem Recht auf Privatsphäre und Schutz personenbezogener Daten gespeichert, abgerufen und verwendet werden." Die Richtlinie verfolge „lediglich eine teilweise Harmonisierung", das Fehlen gemeinsamer Ansätze in den nicht geregelten Bereichen sei daher „nicht verwunderlich"; Bericht der Kommission v. 18.4.2011, a. a. O. (Fn. 89), S. 38.

ausgeklammert bleiben mussten: Welche Behörden etwa auf die auf Vorrat gespeicherten Daten Zugriff erhalten sollen, ist eine Frage, die vor dem Inkrafttreten des Vertrags von Lissabon nur im Rahmen der sog. „Dritten Säule" hätte geregelt werden können. Dies hätte eine einstimmige Entscheidung der Mitgliedstaaten vorausgesetzt, die sich seinerzeit jedoch nicht abgezeichnet hatte.[92]

Auch mit der Begründung der Erforderlichkeit der Vorratsdatenspeicherung insgesamt tat sich die Kommission schwer. Der Bericht verweist an mehreren Stellen auf den hohen Nutzen der gespeicherten Daten für strafrechtliche Ermittlungen und Strafverfolgungsmaßnahmen.[93] Die Berichte aus den Mitgliedstaaten hätten gezeigt, dass die Vorratsdatenspeicherung „zur Verhütung und Bekämpfung von Kriminalität ... zumindest wertvoll, in manchen Fällen sogar unverzichtbar sei".[94] Zugleich betont die Kommission, dass unter dem Aspekt der Vereinbarkeit mit Grundrechten jede Lösung „zur Verwirklichung eines Ziels von allgemeinem Interesse oder zum Schutz der Rechte und Freiheiten Dritter erforderlich sein" und „in einem angemessenen Verhältnis zu dem angestrebten Ziel stehen" müsse.[95] Einen Nachweis dafür, dass diese Kriterien von der derzeit geltenden Richtlinie erfüllt werden, enthält der Bericht nicht. Obwohl die Kommission in einer zweiten Runde diesbezüglich weitere Daten von den Mitgliedstaaten anforderte und sich die Veröffentlichung dadurch um mehr als sieben Monate verzögerte,[96] konnten die Mitgliedstaaten offenbar nicht alle angefragten Belege erbringen.

Die Kommission hat den Verbesserungsbedarf erkannt und angekündigt, den Rechtsrahmen für die Vorratsdatenspeicherung zu überarbeiten. Dazu will sie in Abstimmung mit den Vertretern relevanter Interessengruppen Optionen erarbeiten, die einer Folgenabschätzung unterzogen werden sollen. Dabei will die Kommission die öffentliche Wahrnehmung der Vorratsdatenspeicherung weiter beobachten.[97]

---

[92] Zur Chronologie des Legislativverfahrens vgl. Abschnitt 1.
[93] Bericht der Kommission v. 18.4.2011, a. a. O. (Fn. 89), S. 1, 28.
[94] Bericht der Kommission v. 18.4.2011, a. a. O. (Fn. 89), S. 28 m. w. N.
[95] Bericht der Kommission v. 18.4.2011, a. a. O. (Fn. 89), S. 34.
[96] Gemäß Art. 14 VDS-RL hätte die Kommission ihren Anwendungsbericht bereits am 15.9.2010 vorlegen müssen.
[97] Vgl. Bericht der Kommission v. 18.4.2011, a. a. O. (Fn. 89), S. 39.

Parallel dazu haben die Debatten über die Reform des Rechtsrahmens in Rat und Parlament bereits begonnen.[98] Der Presse ist zu entnehmen, dass etliche Mitgliedstaaten, darunter das Vereinigte Königreich, Frankreich, Spanien und Polen, auf der Fortsetzung der Vorratsdatenspeicherung bestehen. Dagegen habe sich insbesondere Österreich, unterstützt u. a. von Deutschland und Schweden, dafür stark gemacht, auch andere Alternativen wie das „Quick-freeze"-Modell in die Diskussion einzubeziehen.[99] Der EDPS ist dieser Auffassung in seiner Stellungnahme im Rahmen der von der Kommission zur Überarbeitung der Richtlinie durchgeführten Konsultation beigetreten: Er kritisiert den mangelhaften Grundrechtsschutz durch die gegenwärtige Regelung[100] und fordert, die „Quick-freeze"-Option nicht nur als Ergänzung zur Vorratsdatenspeicherung, sondern auch als ihren möglichen Ersatz „ernsthaft" zu prüfen.[101] Der Innenausschuss des Europäischen Parlaments äußerte sich ebenfalls kritisch.[102]

Auch der EuGH wird sich vermutlich bald in einem – erneut[103] aus Irland eingeleiteten – Verfahren mit der Frage der Einhaltung von Grundrechten auseinandersetzen müssen: Im Rahmen einer Klage[104] der Bürgerrechtsorganisation Digital Rights Ireland (DRI) hat der irische High Court am 5.5.2010 beschlossen, dem EuGH die Frage der materiellen Rechtmäßigkeit der Richtlinie vorzulegen.[105] Seit über einem Jahr nun arbeitet das Gericht bereits an der genauen Formulierung der Vorlagefragen. Mit einem Urteil ist somit kurzfristig nicht zu rechnen.

---

[98] Vgl. hierzu die Presseinformation des Rates von der Sitzung des Rates für Justiz und Inneres vom 12.5.2011, http://europa.eu/rapid/pressReleasesAction.do?reference=PRES/11/128&format=HTML&aged=0&lg=de&guiLanguage=en.

[99] Erich Moechel, Vorratsdaten: Österreich legt sich quer, 17.5.2011, http://fm4.orf.at/stories/1682829/.

[100] EDPS, Stellungnahme des Europäischen Datenschutzbeauftragten zum Evaluierungsbericht der Kommission an den Rat und das Europäische Parlament über die Richtlinie über die Vorratsdatenspeicherung (Richtlinie 2006/24/EG), 31.5.2011, Nr. 35 ff., 85.

[101] EDPS, a. a. O. (Fn. 100), Nr. 56 f., 86.

[102] Vgl. das Video von der Sitzung des Ausschusses für Bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments vom 15.6.2011, http://www.europarl.europa.eu/wps-europarl-internet/frd/vod/player?eventCode=20110615-1500-COMMITTEE-LIBE&language=en&byLeftMenu=researchcommittee&category=COMMITTEE&format=wmv#anchor1.

[103] Vgl. zur Nichtigkeitsklage Irlands Abschnitt 1.

[104] *Digital Rights Ireland Ltd.*, Klage v. 14.9.2006, a. a. O. (Fn. 46).

[105] Vgl. dazu Abschnitt 4.1.

Das Projekt InVoDaS begleitet die aktuellen Entwicklungen um Umsetzung wie Reform der Richtlinie aus rechtswissenschaftlicher Perspektive. Mit der Ermittlung von „best practices“ – Lösungsansätzen, die sich in anderen Mitgliedstaaten als vielversprechend im Sinne eines bestmöglichen Interessenausgleichs erwiesen haben – wird der Rechtsvergleich zur Erarbeitung von Gestaltungsvorschlägen für den deutschen Gesetzgeber beitragen. Darüber hinaus lassen sich aus den Ergebnissen der vergleichenden Analyse auch Hinweise auf möglichen Reformbedarf und Regelungsoptionen auf europäischer Ebene ableiten. InVoDaS versteht sich daher als wissenschaftlichen Debattenbeitrag zur kritischen Überprüfung und ggf. Fortentwicklung des Konzepts der Vorratsdatenspeicherung in Deutschland und Europa. Vorläufige Ergebnisse und Gestaltungsvorschläge für einen bestmöglichen Interessenausgleich wurden auf einer Tagung am 7.9.2011 in Berlin vorgestellt und mit den Teilnehmern breit diskutiert.[106]

Sebastian Schweda ist Rechtsanwalt mit Schwerpunkten im Medien-, Telekommunikations- und Datenschutzrecht und Wissenschaftlicher Mitarbeiter am Institut für Europäisches Medienrecht (EMR), Saarbrücken/Brüssel, E-Mail: s.schweda@emr-sb.de

[106] Die Tagung ist dokumentiert unter http://cms.uni-kassel.de/?id=37580#126886.

Susanne Beck

Vorratsdatenspeicherung und aktuelle Entwicklungen in der Inneren Sicherheit im Vereinigten Königreich – eine Analyse im Mai 2011

Abstract

Im Anschluss an eine von Sorge vor terroristischen Anschlägen und einem starken Sicherheitsbedürfnis geprägten Entwicklung eines differenzierten Datenschutzrechts auf der einen, eine die Überwachung der Bürger vorantreibende Ausbau der Staatsmacht auf der anderen Seite besteht im Vereinigten Königreich (VK) nun – nach jahrelangem Ausbau der staatlichen Überwachungsbefugnisse in verschiedensten Bereichen – seit 2007 (Neuregelung zu Internetdaten 2009) eine explizite gesetzliche Festschreibung der Vorratsdatenspeicherung. Diese beinhaltet eine Verpflichtung der öffentlichen Telekommunikationsanbieter, Daten zu Festnetz- und Mobiltelefonaten, Internetnutzung, Emailverkehr und Internettelefonaten für 12 Monate zu speichern. Diese Regelung ist in vielerlei Hinsicht Ausdruck einer spezifischen englischen Einstellung zur Privatsphäre, zum Staat als Sicherheitsgarant, zur Realität terroristischer Bedrohung. Das bedeutet keineswegs umfassende Akzeptanz der aktuellen Gesetzeslage oder der geplanten Weiterentwicklungen – etwa hin zu einer staatlichen „Big Brother"-Datenbank. Unter Anführung des Schutzes der Privatsphäre, aber auch mit Hinweis auf die Ineffizienz und technische Unzulänglichkeit wird das geltende Recht kritisiert. Die Ausbalancierung von Privatsphäre und Sicherheit in einem durch Terrorismus ernsthaft bedrohten Staat ist noch lange nicht abgeschlossen.

Die Vorratsdatenspeicherung wird, wie wir gerade gehört haben, in ganz Europa intensiv diskutiert (Schweda 2011). Das Ausbalancieren von Sicherheit und Freiheit, von wirksamer Verbrechensbekämpfung und Persönlichkeitsschutz, stellt sowohl die Europäische Union als auch die Nationalstaaten vor erhebliche Herausforderungen.[1] Die im Beitrag von Bukow und Schweda diskutierten, die europäischen Regulierungen und Umsetzungen erschwerenden Unterschiede im Umgang mit den persönlichen Daten sind Ausdruck der Identität der jeweiligen Staaten, insbesondere ihrer kulturbedingten Prioritätensetzung in Bezug auf innere Sicherheit und Persönlichkeitsschutz.

[1] Vgl. exemplarisch nur Bedner (2009: 372 ff.); Leutheusser-Schnarrenberger (2007: 9 ff.); Kindt (2009: 661 ff.); Roßnagel (2010: 1238 ff.) Die Richtlinie wird in ihrer aktuellen Form möglicherweise nicht mehr lange existieren (Bolzen 2011). Zur Bedeutung des Internets bei der Terrorismusbekämpfung und konkreten Überlegungen zu verhältnismäßiger Überwachung der Bürger eingehend Brown/Korff (2009: 119 ff.).

Die Regelungen und ihre Umsetzung im Vereinigten Königreich (VK)[2] weisen interessante Besonderheiten auf, die Ausdruck einer spezifischen Einstellung zum Datenschutz sind (Beck 2008: 195 ff.). Den Betrachtungen zur englischen Rechtslage möchte ich einige Überlegungen zu Zweck und Methode der Rechtsvergleichung voranstellen.[3] Die bloße Beschreibung oder gar unreflektierte Bewertung einer ausländischen Rechtslage birgt nur begrenzten Erkenntnisgewinn, solange keine Festlegung von Ziel und diesem dienlicher Methodik erfolgt. Allgemeiner Art, wenn auch keineswegs per se unspezifisch, ist das Ziel des besseren Verständnisses der fremden Rechtslage, der Gründe für die Unterschiede zur eigenen Situation und damit nicht zuletzt der Ursachen für die deutschen Regelungen. Basierend auf diesem Verständnis lassen sich gegebenenfalls im Ausland gefundene Lösungen übernehmen. Diese Übertragung stößt jedoch aufgrund der kulturellen Prägung der jeweiligen rechtlichen Lösungen auf Grenzen.

Gerade in Fällen wie der Vorratsdatenspeicherung, in der aufgrund der Grenzüberschreitung des Internets, des Verbrechens und der die Daten verwaltenden Unternehmen internationale und europäische Lösungen gesucht werden müssen, die nationalen Prägungen jedoch zu unterschiedlichen Rechtslagen führen, lohnt sich ein Blick auf die Gründe für diese Unterschiede. Nur in gegenseitigem Verständnis lassen sich nachhaltige transnationale Lösungen finden. Noch eine weitere Anmerkung: die Betrachtung fremden Rechts bedeutet, das ausländische Recht und die kulturellen Hintergründe aus externer Perspektive zu beschreiben, was jedenfalls zu einer anderen Beschreibung führt als die eines Juristen des fremden Rechtssystems.

[2] Die meisten der im Folgenden dargestellten Regelungen finden im gesamten Vereinigten Königreich Anwendung, teilweise verändern sich bezüglich der Durchsetzung einige Details für Schottland und Nord-Irland (z.B. die Zuständigkeit der Behörden). Soweit für Schottland oder Nordirland spezielle Gesetze gelten oder die Durchsetzung der Regelungen erheblich von der englischen Regelung abweicht, wird darauf in den Anmerkungen hingewiesen.

[3] Zur Methodik der Strafrechtsvergleichung vgl. die Beiträge in Beck/Burchard/Fateh-Moghadam (Hrsg.), Strafrechtsvergleichung als Problem und Lösung, Baden-Baden, 2011.

1. Historische Entwicklung der Gesetzeslage zur Vorratsdatenspeicherung

Ein tiefergehendes Verständnis der aktuellen englischen Rechtslage erfordert zunächst eine Betrachtung der Entwicklung der Gesetzgebung bis zum heutigen Zeitpunkt:

1998: Der „*Data Protection Act 1998*" (Beck 2008: 195 ff.) regelt das Recht jeder Person, auf Anfrage unverzüglich darüber informiert zu werden, ob und wie ihre Daten genutzt werden. Festgelegt werden u.a. Prinzipien über die zulässigen Zwecke oder die Angemessenheit der Datennutzung, die zulässige Speicherdauer und den erforderlichen Schutz der Daten, u.a. gegen unbefugte Nutzung. Für die Verhinderung und Aufdeckung von Verbrechen, die Verfolgung von Straftätern sowie die Ermöglichung der Besteuerung können Ausnahmen von den Vertraulichkeitsbestimmungen gemacht werden, ebenso im Bereich Gesundheit, Erziehung und Sozialarbeit sowie für zahlreiche Aktivitäten des Staates. Auf gerade diesen Ausnahmebestimmungen basieren die zahlreichen Überwachungsaktivitäten des VK (dazu sogleich), unter anderem im Zusammenhang mit der Vorratsdatenspeicherung. 2003 wurden die „*Privacy and Electronic Communications Regulations 2003 (No.2426)*" erlassen, die die Rechte von Individuen stärken. Unter anderem wird die Nutzung von Daten, die zur Kommunikationsübermittlung in einem elektronischen Kommunikationsnetzwerk oder zur Erstellung von Rechnungen für die Kommunikation verwendet werden sowie die Nutzung von Daten, die in einem elektronischen Kommunikationsnetzwerk verwendet werden, aus denen sich der Aufenthaltsort des Nutzers ergibt, beschränkt. Dies bedeutet, dass staatliche Regelungen und Handlungen in Bezug auf Vorratsdatenspeicherung das anerkannte Recht der Privatsphäre einschränken und deshalb minimalinvasiv zu gestalten sind. Es bedeutet auch, dass Firmen die Daten selbst nicht länger als notwendig speichern und nutzen oder ohne gesetzliche Grundlage weitergeben dürfen.

2000: „*Regulation of Investigatory Powers Act 2000*" (RIPA) (UK Government 2000 a/b, 2002): Dieses Gesetz regelt die Telekommunikationsüberwachung und ermächtigt spezifische staatliche Behörden (inzwischen fast 800), zu bestimmten Zwecken

(Nationale Sicherheit, Verbrechensbekämpfung, Erhalt der öffentlichen Sicherheit und Gesundheit, nationales wirtschaftliches Interesse), Überwachungsmaßnahmen zu ergreifen. Dies beinhaltet auch:

- von Internetdienstanbietern Zugang zur elektronischen Kommunikation eines Kunden zu verlangen, ohne dass dieser davon erfährt,
- von Internetdienstanbietern die Installation technischer Einrichtungen zur Kommunikationsüberwachung zu verlangen,
- von einer Person die Herausgabe von elektronischen Schlüsseln zu verlangen und bei Weigerung Haftstrafen zu verhängen,
- großflächige Überwachung mobiler Kommunikation,
- sowie die Überwachung der Internetaktivitäten bestimmter Personen.

Die „*Telecommunications Regulations 2000 No.2699*" erlauben unter bestimmten Bedingungen zusätzliche Abhörmaßnahmen.

2001: Als Reaktion auf die Anschläge des 11. September wurde der "*Anti-Terrorism, Crime and Security Act 2001*" erlassen. In Abschnitt 11 findet sich die Regelung zur freiwilligen Vorratsdatenspeicherung durch Service Provider (UK Government 2001). Daten in diesem Sinne liegen vor, wenn durch sie die Identifizierung des Nutzers, des von ihm genutzten Service und des Zeitpunkts der Nutzung möglich sind, sowie Informationen darüber, wen der Nutzer kontaktiert hat. Nicht eingeschlossen sind die Inhalte der Kommunikation. In den auf der Regelung basierenden Richtlinien werden Zeiträume für die Speicherung bestimmter Informationen empfohlen: Für Informationen über den Nutzer und über Telefonate ein Zeitraum von 12 Monaten, für Informationen über SMS, EMS, MMS sowie Emails 6 Monate und über die Internetaktivität 4 Tage. Der staatliche Zugang zu diesen Daten bestimmte sich nach dem RIPA. Diese Regelung wurde intensiv diskutiert. Kritisiert wurde etwa der freiwillige Charakter der Richtlinien, da die Befolgung durch private Kommunikationsfirmen die Privatsphäre verletzen könnte.[4] Zudem wurde die Problematik der Kostenübernahme durch den Staat debattiert. In der Kritik stand auch die Praxis vieler, durch den RIPA zu Überwachungsmaßnahmen ermächtigter Regionalbehörden, ihre Befugnisse zur Verfolgung von Bagatelldelikten

[4] Zu den Erfordernissen im Lichte des europäischen Datenschutzrechts, insbesondere den Urteilen des EGMR, detailliert Brown/Korff (2009: 128 ff.). Insbesondere erfordert jede Sammlung oder Speicherung von Daten eine spezifische gesetzliche Basis.

einzusetzen (Williams 2009 b). Überdies wurden Vorwürfe laut, viele Parlamentarier und Regierungsmitglieder hätten das Gesetz bei der Verabschiedung nicht ausreichend verstanden (OUT-LAW.COM 2006).

2006 wurde nach langer Diskussion und nicht zuletzt unter dem Eindruck der Londoner Terroranschläge die EU-Richtlinie erlassen, über die wir schon einiges gehört haben (Europäisches Parlament und Europäischer Rat 2006). Durch sie wurde erforderlich, die auf Freiwilligkeit basierende Regelung durch eine verpflichtende Normierung zu ersetzen. Auch wenn es in Erklärungen der Regierung des VK gelegentlich so klingt, wurde die Richtlinie jedoch nicht „von außen" an sie herangetragen: Das VK hatte zu dieser Zeit die Ratspräsidentschaft inne und war wesentlich mitverantwortlich für den Erlass (Walker 2009: 326).

2007: Ein Jahr später erfolgte deshalb der Erlass der „*Data Retention (EC Directive) Regulations 2007*"[5] (Home Office 2007), die die Telekommunikationsfirmen zur Speicherung von Daten über Festnetz- und Mobiltelefonate für 12 Monate verpflichteten (Jones 2008: 147 ff.; Nettleton/Watts 2007: 58 ff.).

2007/2008: Ab 2007/2008 wurde das „*Interception Modernisation Programme*" diskutiert (teilweise bezeichnet als „Big Brother" Datenbank (Grice, Andrew 2009)), das die Regierung als typisches Beispiel dafür anführte, wie der Staat modernste Technologien – hier einen möglichst schnellen und umfassenden Zugriff auf Kommunikationsdaten – zur Terrorismusbekämpfung einsetzen könnte (Home Office 2007 a). Die Regierung sollte durch „black boxes" einen live-Zugriff auf jede elektronische Kommunikation im VK erlangen und die Erkenntnisse in eine staatliche Datenbank überführen können (Verkaik 2008). Die Kosten dieses Programms wurden auf 12 Milliarden Pfund geschätzt (Williams 2008). Eine Zeitlang wurde diskutiert, das Programm gemeinsam mit der Vorratsdatenspeicherung in Form der „*Data Communications Bill*" zu regeln (Williams 2009 a). Dieser Vorschlag wurde in der Öffentlichkeit heftig kritisiert und auch im Parlament und House of Lords hinterfragt. Im September 2008 entschied sich die Regierung, nur die

[5] Vgl. Nettleton/Watts (2007: 58 ff.).

Verpflichtungen aus der Richtlinie zu erfüllen und auf die Errichtung einer zentralen Datenbank – vorerst – zu verzichten.

2009: Um der Verpflichtung, auch Internet-Kommunikationsdaten zu speichern, zu entsprechen, wurden „*The Data Retention (EC Directive) Regulations 2009*" erlassen. Hierzu erfolgte zunächst eine Konsultation mit Beteiligten (Home Office 2008), mit der sich die Regierung vor dem Gesetzeserlass intensiv auseinandersetzte (Home Office 2009). Die Normen erfassen nun, in Nachfolge der Regelungen von 2007 und in starker Anlehnung an die Richtlinie, alle relevanten Kommunikationsdaten. Verschiedene Details der Umsetzung werden noch zwischen dem Innenministerium, den Verfolgungs- und Verwaltungsbehörden und den Kommunikationsdienstleistern verhandelt (Walker 2009: 326).

2011: Eine auch für die Vorratsdatenspeicherung relevante Entwicklung ist die aktuelle Diskussion zur „*Protection of Freedoms Bill*". Die erste Anhörung hierzu fand am 11. Februar diesen Jahres statt, die zweite Lesung am 1. März. Am 17. Mai fand die sogenannte „Committee Debate" im House of Commons statt, inzwischen befindet sich die Bill in der „Report Stage" (UK Parliament 2011). Durch die Regelung soll u.a. der RIPA insofern ergänzt werden, als für bestimmte Investigationen ein richterlicher Beschluss[6] gefordert wird. Hierzu gehört der Zugang zu und die Offenlegung von Kommunikationsdaten. Die starke Ausweitung der staatlichen Eingriffsbefugnisse in die Privatsphäre der Bürger scheint also durch diese geplante Neuregelung eine gewisse Einschränkung zu erfahren.

2. Aktuelle Gesetzeslage: The Data Retention (EC Directive) Regulations 2009

Das aktuelle Gesetz verpflichtet die öffentlichen Telekommunikationsanbieter, Daten zu Festnetz- und Mobiltelefonaten, Internetnutzung, Emailverkehr und Internettelefonaten für die Dauer von 12 Monaten zu speichern (Regelung 4 und 5).

„Öffentlicher Kommunikationsanbieter" ist nach dem Gesetz ein Anbieter sowohl eines öffentlichen Kommunikationsnetzwerks als auch eines öffentlichen Kommunikationsdienstes. Da die Anbieter Zweifel an der Klarheit dieser Regelung

[6] Die Überwachung des Umgangs mit derartigen Daten sollte auch aus europarechtlichen Gesichtspunkten normalerweise durch einen Richter erfolgen, vgl. Brown/Korff (2009: 130).

äußerten, greift sie nur für Unternehmen, die von staatlicher Seite hiervon unterrichtet wurden. Diese Benachrichtigungen sollen durch Verhandlungen zwischen Regierung und Unternehmen über die erforderlichen Änderungen in dessen Speicherungspraxis, die beste Speichermethode, einen Zeitplan für die Umsetzung sowie die Kostenübernahme vorbereitet werden (Home Office 2009: 25).
Zu den zu speichernden Daten gehören u.a. die IP-Adresse und Zeitpunkte des Ein- und Ausloggens, Sender, Empfänger, Datum und Uhrzeit von Emails, Anrufer und Angerufener von Internettelefonaten, überdies Details aller Nutzungen von Festnetz- und Mobiltelefonaten einschließlich des Aufenthaltsorts des Anrufers. Dies gilt auch für erfolglose Anrufversuche, nicht jedoch für unverbundene Anrufe. Nicht erfasst werden soll der Inhalt der Kommunikation. Grundsätzlich sind nur Daten zu speichern, die von den Firmen ohnehin erhoben werden, d.h. es gibt keine Verpflichtung, Daten nur zur Verfolgung staatlicher Zwecke zu generieren (Walker 2009: 327). Kritik wurde insofern geäußert, als die Speicherung mancher Daten in betrieblichen Zusammenhängen sinnlos sei und eben doch zusätzliche Maßnahmen erforderlich mache (Stampfel/Gansterer/IIger 2007). Die Firmen müssen dem Gesetz nach auf Zugangsersuche von Ermittlungsbehörden oder anderen zuständigen Behörden unverzüglich reagieren. Der Zugang soll nur für spezifische Fälle und bei expliziter gesetzlicher Erlaubnis erfolgen.
Zudem wird geregelt, dass die Kosten der privaten Unternehmen für die Vorratsdatenspeicherung – nach Befolgung bestimmter Bedingungen – vom Staat getragen werden sollen. Trotz der insofern offenen gesetzlichen Formulierung („may“) hat die Regierung zugesichert, dass kein Unternehmen die Verpflichtungen aus den Regelungen umsetzen muss, bevor keine Vereinbarung über die Kostenübernahme getroffen wurde (Home Office 2009: 4).
Kommt ein Unternehmen seinen gesetzlichen Pflichten nicht nach, kann der Staat eine zivilrechtliche Leistungsklage oder ein spezifisches Verfahren einleiten. Zudem besteht das Risiko einer negativen PR, wenn sich ein Unternehmen weigert, bei Fragen der nationalen Sicherheit oder der Verfolgung schwerwiegender Verbrechen mitzuwirken (Walker 2009: 328).

2.1. Beschreibung der Ziele und Vorgehensweise aus Sicht der englischen Regierung:

Gerechtfertigt wird die aktuelle Regelung von der Regierung wie folgt: "This data is a vital tool to investigations and intelligence gathering in support of national security and crime". "Communications data allows investigators to identify suspects, examine their contacts, establish relationships between conspirators and place them in a specific location at a certain time". (Home Office 2009) Polizei, Sicherheitsbehörden und Geheimdienste sowie andere öffentliche Stellen seien für die Durchsetzung des Rechts und der öffentlichen Sicherheit in hohem Maß von der Nutzung der Kommunikationsdaten abhängig. Gerade bei längeren Investigationen besteht die Gefahr, dass diese Daten nicht mehr zur Verfügung stehen. Die Veränderung des UK-Rechts von freiwilliger zu verpflichtender Speicherung soll insbesondere die Investigationen in Mordfällen, Sexualverbrechen und im Terrorismusbereich erleichtern. Hierfür wurde die Option gewählt, nur durch die erforderliche Benachrichtigung ausgewählte Provider zur Speicherung von Daten zu verpflichten, um so die Anzahl an Firmen, die durch diese Regelung belastet werden, zu minimieren.

Die Regierung rechnete zum Zeitpunkt des Erlasses damit, dass die Kosten für die Finanzierung der Speichermöglichkeiten ca. 50 Mio. Pfund betragen würden. Diesbezüglich wird diskutiert, ob diese Ausgaben tatsächlich gerechtfertigt sind, der Steuerzahler also eine Gegenleistung erhält. Problematisch ist insofern insbesondere die dünne statistische Datenlage zur Effizienz der Vorratsdatenspeicherung (Walker 2009: 330).[7]

2.2. Vorkehrungen gegen Missbrauch

Verschiedene gesetzliche und verfahrensbezogene Vorkehrungen sollen vor Missbrauch der Regelungen schützen:

- Die beteiligten Unternehmen müssen verschiedene Prinzipien des Datenschutzes beachten, insbesondere was die Sicherheit der Daten vor

[7] Zu den Schwierigkeiten der Vorratsdatenspeicherung aufgrund moderner Technologien vgl. Custers (2008: 94 ff.).

Veröffentlichung oder Zugriff von außen, aber auch vor Verlust oder Zerstörung betrifft. Die Daten müssen grundsätzlich nach der gesetzlich bestimmten Frist gelöscht werden.

- Die Regelungen legen explizit fest, dass Zugriff auf die Daten nur für spezifische Fälle und nur soweit durch ein anderes Gesetz vorgesehen, möglich ist. Die Voraussetzungen für einen Zugriff sind im ersten Abschnitt des RIPA geregelt.
- Dort ist u.a. reguliert, dass der Zugriff notwendig und verhältnismäßig sein muss. Die Notwendigkeit bestimmt sich danach, ob einer der folgenden Zwecke verfolgt wird: nationale Sicherheit, Verhütung oder Verfolgung von Verbrechen, öffentliche Sicherheit, wirtschaftliche Interessen des VK, Schutz der öffentlichen Gesundheit, Steuereintreibung u.ä., Vermeidung eines Todes oder einer Verletzung einer Person.

Der Zugriff auf die Daten ist einer Vielzahl öffentlicher Institutionen möglich, die der ursprünglich kurzen Liste im RIPA nachträglich hinzugefügt wurden. Obwohl einige von ihnen nur Zugang zu einem Teil der Daten haben, ist dieser Aspekt umstritten (Walker 2009: 329).

2.3. Umsetzung der Regelungen in der Praxis

Wie der Berichterstatter für Kommunikationsüberwachung meldete, wurden 2007 von öffentlichen Behörden über 500.000 Anfragen bezüglich Kommunikationsdaten an Provider gestellt. Jede Vermutung, dass ein niedrigrangiger Gemeindebeamter uneingeschränkten Zugang zu den Telefondaten der Bürger hätte, entbehre einer realen Grundlage, da immer ein Verfahren durchlaufen werden müsse, in dem Notwendigkeit und Verhältnismäßigkeit der Anfrage durch einen höherrangigen Beamten überprüft würden. Nach dem Bericht hat das Parlament das Recht auf Zugang zu Kommunikationsdaten für fast 500 Ortsbehörden gebilligt. Diese haben jedoch keinen Zugang zu Verkehrsdaten, so dass sie nicht den Ort identifizieren können, von dem oder zu dem die Kommunikation vermittelt wurde. Tatsächlich haben nur etwa 150 kommunale Behörden von dem Recht Gebrauch gemacht. In der Regel nutzen die Behörden dieses Recht vor allem zur Strafverfolgung, etwa von Trickbetrügern.

Die konkrete Umsetzung ist in einem „Code of Practice“ geregelt, der detaillierte Vorgaben für die Behörden enthält, unter anderem über die Notwendigkeit und

Verhältnismäßigkeit des Zugriffs auf Daten: der jeweils Zuständige muss im konkreten Fall den spezifischen Vorteil für die Investigation oder die spezifische Maßnahme, die von der Behörde im öffentlichen Interesse durchgeführt wird, gegen das Ausmaß des Eingriffs in das individuelle Recht auf Schutz der Privatsphäre abwägen (Home Office 2007: 10).

Eine unabhängige Überwachung des Umgangs mit den gespeicherten Daten soll durch den Interception of Communications Commissioner gewährleistet werden (Section 57 RIPA). Dieser untersucht die Rechtmäßigkeit des Handelns der zuständigen Behörden sowie die Effektivität der Nutzung der Daten und erstattet dem Parlament jährlich über seine Erkenntnisse Bericht (Kennedy 2007). Zusätzlicher Datenschutz wird durch das Investigatory Powers Tribunal gewährleistet, das individuellen Beschwerden bezüglich der nach dem RIPA vorgenommenen Maßnahmen nachgeht (Section 65 RIPA). Wie effektiv diese Maßnahmen bezüglich des Zugriffs auf Daten, die durch die Kommunikationsfirmen gespeichert wurden, sind, wird sich erst im Laufe der nächsten Jahre zeigen.

3. Kritik an der bestehenden Regelung

Wie in allen europäischen Ländern wird die Vorratsdatenspeicherung auch in England kritisiert. Überdies gibt es Kritikpunkte an der konkreten Umsetzung.

3.1. Kritik an der Vorratsdatenspeicherung unter Berücksichtigung der englischen Besonderheiten

Sowohl über die Verhältnismäßigkeit der Vorratsdatenspeicherung als solcher als auch über die vom UK gewählte Dauer von 12 Monaten wurde vor Gesetzeserlass intensiv diskutiert (Walker 2009: 330).[8] Nach Angaben der Regierung wurde in 95 % aller Ermittlungen in Fällen schwerwiegender Verbrechen und in fast allen Maßnahmen des Sicherheitsdiensts der letzten Jahre Kommunikationsdaten als wichtiges Beweismittel verwendet. Insbesondere Investigationen in den Bereichen

[8] Sehr deutlich die Kritik bezüglich der generellen Entwicklung von Brown/Korff (2009: 131): "We are giving up freedom without gaining security. In the process, all of us are increasingly placed under general, precautionary mass surveillance, with comprehensive data being captured on our activities. The European surveillance society is developing in a profoundly undemocratic way".

Kinderpornographie, bewaffnete Raubüberfälle, Entführungen aber auch Selbstmordversuche werden als von Kommunikationsdaten abhängig dargestellt. Doch gibt es hierzu nur wenige statistische Daten; die einzige Quelle ist der jährliche Parlamentsbericht des Interception of Communications Commissioner. So gibt es Zahlen aus dem Jahr 2007, wobei sich jedoch der Commissioner weigert, die Gesamtanzahl an Zugriffen einzelnen Bereichen zuzuordnen. Es findet sich lediglich ein allgemeiner Kommentar:

> *"…it is evident that the acquisition of the data was justified and that it is being used as a powerful investigative tool,* primarily *to prevent crime and disorder. Communications data plays a crucial role in the successful outcome of prosecutions and often it is the primary reason why offenders plead guilty".* (Smith 2008)

Bezüglich der Entführungs- und Vermisstenfälle führt er an, dass der Zugriff auf Kommunikationsdaten Leben retten könne. Generell schlussfolgert der Commissioner, dass Eingriffe in die Privatsphäre soweit möglich vermieden oder zumindest gering gehalten werden und er feststellen könne, dass sich die Behörden an das Gesetz und den „Code of Practice" hielten.

Dennoch werden an der Vorratsdatenspeicherung auch in England generelle Zweifel geäußert,[9] weil sie einen erheblichen Eingriff in die Privatsphäre darstellt, ihre Effektivität jedoch nicht bewiesen ist, einige Fakten sogar dagegen sprechen. So merkt Davies, der Vorsitzende von „Privacy International" an, dass die deutlich weniger eingriffsintensive Speicherung von Daten konkreter Verdächtiger dieselben Ziele erreichen würde (Espiner 2009). Überdies wird befürchtet, dass die Behörden die Daten auch für weit weniger wichtige Zwecke als die angegebenen nutzen könnten. Hierfür fehlt es nach Ansicht einiger Kritiker noch an hinreichenden Abwehrmechanismen im geltenden Recht (Walker 2009: 332). Insbesondere besteht die Sorge, dass der Zugang jeder Behörde eröffnet werde, die die Gerichte von ihrer Berechtigung überzeugen könne (Taylor 2007). Nach Angaben der Regierung arbeiten Innen- und Justizministerium sowie der Commissioner an Richtlinien für den Umgang der Gerichte mit solchen Fällen (Home Office 2009: Abs. 15 f.).

[9] Zur Diskussion allgemein vgl. u.a.: Breyer (2005: 365 ff.); Brown/Korff (2009: 119 ff.); Mitrou (2008: 409 ff.); Mitrou (2010: 127 ff.).

Allerdings ist es für ein Verständnis der spezifischen englischen Debatte nicht ausreichend, die allgemeinen, etwa in Deutschland ausgetauschten Argumente, direkt zu übertragen. Denn in England besteht im Bereich des Datenschutzes, aber auch bei der öffentlichen Wahrnehmung staatlichen Handelns eine Sondersituation.

Auf der einen Seite sind die Erfahrungen mit der Sicherheitsgesetzgebung und staatlichen Reaktion auf neue Bedrohungen wie den Terrorismus, etwa mit dem RIPA, alles andere als positiv.[10] Die kommunalen Behörden haben die gewährten Befugnisse zu intensiver Überwachung der Bürger genutzt und unbedeutende Gesetzesverstöße mittels dieser Maßnahmen verfolgt. Aus diesem Grund wird befürchtet, dass die Daten, sobald sie einmal gespeichert sind, für unterschiedliche, den Behörden jeweils dienliche Zwecke genutzt werden und das Vertrauen in die Regierung weiter geschwächt würde (Espiner 2009).

Dies ist jedoch nur eine Facette der gesellschaftlichen Hintergründe der englischen Debatte.[11] Ein weiterer Aspekt ist, dass die Toleranzgrenze gegenüber staatlichen Eingriffen in England eher hoch zu sein scheint – zumindest bisher.[12] Hierfür gibt es eine Vielzahl von Gründen, von denen an dieser Stelle zur Veranschaulichung einige wenige expliziert werden:

Ein historisch-kultureller Grund ist, dass die aktuell die Politik mitbestimmenden Bürger keine Erfahrungen mit militärischer Besetzung oder Diktaturen haben, während in den meisten kontinentaleuropäischen Ländern die Konsequenzen tyrannischer Herrschaftsformen noch deutlich im historischen Gedächtnis eingeprägt sind (Pounder/Kosten 1993: 1).

Überdies ist die Angst vor Verbrechen hoch, nicht zuletzt aufgrund einer in Deutschland in diesem Maß unüblichen Presseberichterstattung, in der ein erheblicher Schwerpunkt auf Kriminalität liegt (Reiner 2007: 302 ff.). Die Kriminalität wird bewusst als Sonderbereich der Gesellschaft dargestellt, der Kriminelle als

[10] Zur wachsenden Kritik an der Entwicklung der englischen Innenpolitik vgl. auch Neumann (2008)

[11] Zur britischen Rechtskultur etwa Legrand (1996: 232 ff.).

[12] Erstaunlich hoch bedeutet keineswegs grenzenlos, wie die heftige Kritik an der Big-Brother-Datenbank gezeigt hat. Es ist jedoch zumindest wahrscheinlich, dass ein derartiger Vorschlag beispielsweise in Deutschland erheblich stärkere Reaktionen hervorgerufen hätte. Dass die Regierung eine derartige Datenbank überhaupt in Erwägung zieht, weist durchaus auf gewisse kulturelle Unterschiede hin.

psychologisch auffällig, als „anders“ wahrgenommen. Der Staat wird aufgefordert, mit Härte und Kontrolle gegen diese extra-gesellschaftlichen Bedrohung vorzugehen. Typisch ist etwa der bekannte Wahlspruch von Tony Blair: „tough on crime and the causes of crime“. Auch die historische Erfahrung mit terroristischer Bedrohung hat hierauf Einfluss: Die vielen Anschläge der IRA, der Terroranschlag auf die Londoner U-Bahn 2005 und einige knapp vereitelte Anschläge haben die Furcht vor Terroristen steigen lassen.[13]

Als letzte Erklärung soll eine linguistische Überlegung angeführt werden: Die Bedeutung des „Heims“ in England (vgl. den berühmten Ausspruch „A man’s home is his castle“). Während etwa in Deutschland jegliche Sammlung von persönlichen Daten kritisch bewertet wird, spielt in England vor allem der „private Raum“ eine Rolle, der weder gegenüber Fremden noch gegenüber dem Staat ohne Weiteres geöffnet wird. Dies zeigt sich unter anderem an der linguistischen Signifikanz[14] und in einigen Präzedenzfällen.[15] Daten, die in einem anderen Kontext freiwillig bekannt gegeben werden, erscheinen für Engländer weniger schutzwürdig. Bezüglich der hier in Frage stehenden Daten zu Internet- und Telefonnutzung gilt dies sicherlich nicht im selben Ausmaß wie für den Aufenthalt auf öffentlichen Straßen und Plätzen, denn die Kommunikation über Email oder Telefon ist auch in englischem Verständnis Teil der Privatsphäre, das Internet andererseits durchaus ein öffentlicher Raum.

---

[13] Gerade diese Entwicklungen führten u.a. zum „Anti-terrorism, Crime and Security Act 2001“, „Prevention of Terrorism Act 2005“, „Terrorism Act 2006“. Die Wahrnehmung terroristischer Bedrohung in England ist aus deutscher Sicht schwer nachvollziehbar, da aktuelle Betroffenheit durch Anschläge die gesellschaftliche Realität erheblich beeinflusst. Es ist auch nicht zu bestreiten, dass gerade das Internet für die Ermittlung und Prävention in diesem Bereich eine zentrale Rolle spielt, vgl. detailliert hierzu Brown/Korff (2009: 121 ff.). Die Kritik zielt weniger auf die Nutzung auch des Internets im Bereich Verbrechensbekämpfung und -prävention als auf die Frage, ob gerade die langfristige, unselektierte Speicherung der Daten aller Bürger hierfür ein angemessenes und effektives Mittel ist.

[14] Alles, was in Deutschland unter „Heimat“, „Wohnort“, „Wohnung“, aber auch „Geburtsort“ oder „Geburtsland“ usw. fällt, ist von „home“ umfasst. Es finden sich zahlreiche Sprichwörter und Redewendungen wie „make yourself at home“, „home made“, „home sick“, „until the cows come home“, etc.

[15] Semayne's Case, 5 Co. Rep. 91a, 91b, 77 Eng. Rep. 194, 195 (1603); Curtis' Case, Fost. 135, 168 Eng. Rep. 67, entschieden 1756.

Die englische Gesetzgebung zur Vorratsdatenspeicherung ist nur im Spannungsfeld zwischen Wichtigkeit des eigenen Heims, geringer Bedeutung des Datenschutzes im öffentlichen Raum, Angst vor Verbrechen und terroristischen Anschlägen und geringem Misstrauen gegenüber einem übermächtigen Staat verständlich. Diese Skizzen zu den Hintergründen sind bewusst kursorisch und überspitzt, sollen sie doch nur eine gewisse Sensibilität für die Unterschiede der Rechtskulturen und die Gründe des englischen Umgangs mit der Problematik schaffen.

3.2. Kritik an der konkreten Umsetzung

Ein Ansatzpunkt für Kritik an der konkreten Gesetzesfassung ist bereits die Erklärung, mit der die Regierung den aktuellen Gesetzeserlass rechtfertigt. In diesem ist etwa von einer „breiten Unterstützung" durch die Telekommunikationsfirmen die Rede (Home Office 2009: 7). Dies wird jedoch bezweifelt: Tatsächlich gibt es zwar eine enge Zusammenarbeit zwischen den Firmen und der Regierung, jedoch waren nicht wenige der Firmen der Meinung, dass der Gesetzesentwurf eine Vielzahl von Problemen beinhalte (Milford 2008).

Die Regelung wird auch dafür kritisiert, dass sie nicht genug technische Details klarstelle. Begriffe wie „Internet-Email" oder „Internettelefonate" wären zu vage, um bestimmen zu können, welche Daten konkret gespeichert werden sollten. Die Regierung hat hiergegen eingewandt, eine weitergehende Konkretisierung sei nicht hilfreich, weil damit bestimmte Kontexte und bestimmte technische Vorgehensweisen ausgeschlossen werden könnten (WTWU 2009). Dies ist problematisch, weil sich die Regierung damit ihrer Verantwortung einer möglichst genauen Beschreibung des zulässigen Eingriffs in die Privatsphäre entzieht. Gerade aufgrund dieser Vagheit ist eine genaue Bestimmung der Nachteile der Regelung nicht möglich. Diese Schwierigkeiten sind die Folge sowohl einer eiligen, vielleicht sogar übereilten Umsetzung der Richtlinie, als auch der generellen Probleme bei der Regulierung moderner Technologien.

Einige Details, die durch die Vagheit der Regelung ungeklärt bleiben, sind (Walker 2009: 330):

- Nicht alle Internetzugänge generieren die erforderliche „ID“ (etwa freie WLAN-Hotspots) und nicht immer sind alle erforderlichen Informationen, wie Log-In- und Log-Out-Zeitpunkt verfügbar, da viele Zugänge permanent eingeloggt sind.
- Vorhandene Informationen über den Email-Versand werden je nach Protokoll und Szenario stark divergieren. Überdies ist unklar, ob auch Daten zu Spam-Emails gespeichert werden sollen (die über 60% des Emailverkehrs ausmachen).
- Das Konzept „erfolgloser Anrufversuch“ macht im Zusammenhang mit Internetdaten keinen Sinn und wurde wohl unreflektiert aus der Richtlinie kopiert.
- Im Zusammenhang mit bestimmten Emailanbietern sind die Daten zu Zeitpunkt und Ort der Versendung eng mit dem Inhalt der Kommunikation verknüpft, die jedoch nach den Regelungen nicht gespeichert werden dürfen.

Die gesetzlichen Mängel bezüglich der technischen Details haben auch zur Folge, dass Personen mit nur geringen technischen Kenntnissen sich ohne Weiteres größtenteils unentdeckten Zugang zum Internet verschaffen können, etwa über webbasierte Emailanbieter, kostenlose WLAN-Hotspots und Dienste außerhalb der EU. Dass die Gesetzgebung ihr technisches Ziel verfehlen könnte, ist neben den möglichen Menschenrechtsverletzungen und finanziellen Kosten durch die Vorratsdatenspeicherung ein gewichtiges Argument gegen die Maßnahme (Walker 2009: 332; Milford: 2008).

Bezüglich der Auswirkungen der Regelungen auf die Kommunikationsfirmen ist zwischen Firmen, die Telefondienste zur Verfügung stellen, und Internetanbietern zu unterscheiden (Walker 2009: 330). Für erstere sind die Auswirkungen gering, da sie die jeweiligen Daten ihrer Kunden ohnehin speichern. Letztere dagegen stehen durch die Regelungen vor erheblichen Herausforderungen, da sie die Daten typischerweise nicht speichern. Insofern ist auch problematisch, dass die Kostenerstattung im Gesetz eben nicht gesichert ist (Walker 2009: 330). Zwar wird die Regierung ihre zahlreichen öffentlichen Zusicherungen (Home Office 2009: 10) wohl einhalten müssen, aber die Rechtssicherheit würde sich durch eine gesetzliche Regelung deutlich erhöhen. Auch werden die Aussagen der Regierung zur Höhe der zu erwartende Kosten bezweifelt (Stampfel/Gansterer/IIger 2007).

Wenn auch scheinbar von den meisten Beteiligten unhinterfragt akzeptiert, sollte auch die vom VK festgesetzte Dauer der Speicherung kritisch betrachtet werden (Walker 2009: 330). Die Regierung vertritt die Ansicht, 12 Monate seien der beste Kompromiss zwischen der Verletzung der Privatsphäre und den Bedürfnissen der Behörden. Entgegnet wird hierauf, dass in der Praxis die wenigsten (ca. 2 %) angeforderten Daten älter als zwei Monate seien.[16]

3.3. Ausblick

Schon kurz nach dem Inkrafttreten der Neuregelung hat die Regierung erkannt, dass sie den Bedürfnissen der Rechtsdurchsetzung nicht umfassend gerecht wird. Bereits im April 2009 wurden Vorschläge zu weitreichenden Reformen vorgelegt (Walker 2009). So sollen die Regelungen an den technologischen Fortschritt angepasst werden. Als Probleme der Regelung wurden identifiziert: Die Diversifikation der Arten von Kommunikation, insbesondere die Bewegung des IP-Protokolls, das schwindende Bedürfnis der Serviceprovider, die Daten zum Unternehmensgebrauch zu speichern, die steigende Anonymisierung des Service, die Fragmentierung der Daten über verschiedene Kommunikationsnetzwerke hinweg und der Umzug von Serviceprovidern aus der englischen Jurisdiktion. Doch statt einer zentralisierten Datenbank will die Regierung das aktuelle dezentralisierte System ausbauen. Die Serviceprovider sollen jedoch sehr viel mehr Daten als derzeit speichern, sie organisieren und mit denen anderer Provider verbinden. Zudem soll die jetzige 12-Monats-Frist in bestimmten Fällen ausgeweitet werden können. Statt einer stärkeren Berücksichtigung der Bürgerrechte ist also eher von einer Ausweitung der staatlichen Befugnisse auszugehen.

4. Aktuelle Entwicklungen in der Inneren Sicherheit

Die tatsächliche sowie die wahrgenommene Bedrohung für die Innere Sicherheit im VK sind nach wie vor hoch (Neumann 2008). So gab der Direktor des MI5 im Jahr

[16] Milford (2008): "practical experience indicates that most requests are for data of relatively recent origin, typically one to two months old".

2007 an, dass der Geheimdienst von 2000 gewaltbereiten islamistischen Terroristen im VK wüsste, dass jedoch zusätzlich von etwa weiteren 2000 Personen auszugehen sei, von denen seine Behörde keine Kenntnis habe (Evans 2007). Es verwundert daher nicht, dass die Debatte um eine Effizienzsteigerung bei der Bekämpfung von Terrorismus und Schwerstkriminalität immer noch anhält (Home Office 2011). So wurde im Mai 2010 das National Security Council gegründet, dessen Aufgabe es ist, die Koordination und Entwicklung des Vorgehens in Fragen der Inneren Sicherheit zu übernehmen.

Bereits Ende 2010 wurde eine „National Security Strategy" veröffentlicht (UK Gorvernment 2010). Sie beginnt mit den bezeichnenden Worten: "The security of our nation is the first duty of government. It is the foundation of our freedom and our prosperity". Der Bericht besagt weiterhin: "The United Kingdom faces a complex array of threats from a myriad of sources. [...] Our national interest requires our continued full and active engagement in world affairs, promoting our security, our prosperity and our values".

In dem Strategieplan werden als Prioritäten der Inneren Sicherheit festgelegt: Terrorismusbekämpfung, Sicherheit im Cyberspace, Sicherheit bei internationalen militärischen Krisen und nationalen Katastrophen wie etwa Hochwasser oder Pandemien (auf große Gebiete eines Landes übergreifende Epidemien). Hierbei handelt es sich um ganz unterschiedliche Bedrohungen, teilweise durch Bürger oder externe „Feinde" des VK, teilweise durch Naturkatastrophen. Eine derart weitreichende Zielrichtung erfordert auch eine breit angelegte Bekämpfung. Zur Eindämmung dieser Risiken sollen deshalb dem Strategieplan nach auch alle Instrumente der Staatsmacht herangezogen werden, einschließlich Militär, Diplomaten, Geheimdienste, Polizei, der private Sektor sowie das britische Volk.

Der Strategieplan legt folgende acht Aufgaben für die Innere Sicherheit fest:

1) Identifikation und Überwachung von Risiken und Chancen für die Innere Sicherheit,
2) Beseitigung der Wurzeln von Instabilitäten,
3) Ausübung von Einfluss, um die Chancen zu nutzen und die Risiken zu managen,

4) Durchsetzung nationalen Rechts und Stärkung internationaler Regelungen, um dabei zu helfen, diejenigen zu bekämpfen, die das VK und seine Interessen bedrohen,
5) Schutz des VK und seiner Interessen im Staatsgebiet, an den Grenzen und international, um physische und elektronische Bedrohungen durch staatliche und nicht-staatliche Akteure zu bekämpfen,
6) Hilfe für die Lösung von Konflikten und für die Bildung von Stabilität. Interventionen in anderen Ländern, soweit notwendig, einschließlich der rechtmäßigen Ausübung von Zwang um die vitalen Interessen des VK zu sichern und die sich außerhalb des Staatsgebiets befindlichen Territorien und Bürger des VK zu schützen,
7) Aufbau von Widerstandsfähigkeit für das VK durch Vorbereitungen für alle Arten von Notfällen, so dass es möglich ist, sich von Schocks zu erholen und lebensnotwendige Dienste aufrechtzuerhalten,
8) Zusammenarbeit in Allianzen und Partnerschaften, wo immer möglich, um nachhaltigere Ergebnisse zu erzielen.

Dieser eher allgemeine Strategieplan zeigt vor allem, dass die Innere Sicherheit weiterhin höchste Priorität im VK hat. Die geplanten Strategien setzen auf Zusammenarbeit verschiedenster staatlicher Behörden und eine Verstärkung der Staatsmacht und gesetzlichen Regelungen. Da zu den wichtigsten Zielen die Sicherheit des Cyberspace gehört, wird auch die Vorratsdatenspeicherung weiterhin eine zentrale Rolle spielen.

5. Zusammenfassung

Die Regelungen zur Vorratsdatenspeicherung im VK setzen die EU-Richtlinie umfassend um und verpflichten Kommunikationsdienstanbieter zu einer 12-monatigen Speicherung von Daten über Identität, Zeitpunkt, und Ort der Nutzung des Dienstes. Hierfür werden von der Regierung die Bekämpfung von Terrorismus und Schwerstkriminalität und die Bedeutung dieser Maßnahmen für die Innere Sicherheit angeführt, während Bedenken hinsichtlich der Verhältnismäßigkeit, Effektivität oder technische Umsetzbarkeit kaum berücksichtigt werden. Dies entspricht der generellen Entwicklung des Umgangs mit Sicherheitsfragen im VK. Die Bedrohung durch Terrorismus und Verbrechen wird besonders stark empfunden und führt, neben anderen kulturellen Hintergründen, zu einer starken Fokussierung auf den Staat als Verantwortlichen für die Innere Sicherheit. Zwar mehren sich die

kritischen Stimmen, dennoch ist zumindest davon auszugehen, dass die Gesetze zur Vorratsdatenspeicherung dauerhaft verstärkt und auch die staatlichen Zugriffsmöglichkeiten auf Daten ausgeweitet werden. Auch wenn die EU-Richtlinie derzeit wieder in der Diskussion steht und ihre Zukunft ungewiss ist, ist zumindest nicht mit einer gravierenden Änderung der politischen Linie zu rechnen.

Data Retention and actual developments in Inner Security in the UK – an analysis from May 2011

Abstract: Following a development of a sophisticated Privacy Law and an extension of state powers, which has been caused by concerns about terrorism and a strong need for safety, since 2007 the UK has regulated obligatory data retention (since 2009 including internet data). These laws oblige public service provider to retain data about phone calls (location of the caller, person he has called, etc.), internet usage and other connected data for a duration of 12 months. In many ways, these laws express specific English perceptions and approaches of privacy, of the role of the State, of the reality of terrorism as thread for everyday life. This does not lead to general acceptance of the actual legal situation or the plans of the legislator (such as the discussed "big brother" databank). On the contrary, the legal situation is widely criticised, because of its thread for privacy as well as because of possible inefficiencies and technical inadequateness. The balancing between privacy and security in a state which faces realistic threads by terroristic organisations has not been finalised until today.

Key Words: Data Retention, Privacy, Inner Security, Anti-Terrorism-Laws, Internet Law

Literatur

Beck, Susanne/Burchard, Christoph/Fateh-Moghadam, Bijan (Hrsg.) 2011: Strafrechtsvergleichung als Problem und Lösung, Baden-Baden: Nomos.

Beck, Susanne 2008: Leben im Überwachungsstaat? Ein einführender Überblick über das englische Datenschutzrecht, in: Hilgendorf, Eric (Hrsg.): Neue Dimensionen des Informationsrechts, Berlin: 195-222.

Bolsen, Stefanie 2011: Brüssel will neue Regeln für Vorratsdaten erlassen. In: Die Welt, 15.4.2011. http://www.welt.de/print/die_welt/politik/article13179292/Bruessel-will-neue-Regeln-fuer-Vorratsdaten-erlassen.html. (Abrufdatum 16.9.2011)

Bukow, Sebastian: Verortung der Diskussion um Vorratsdatenspeicherung im Politikfeld Innere Sicherheit (in diesem Band).

Bedner, Mark 2009: Vorratsdatenspeicherung, in: Datenschutz und Datensicherheit (6/2009) 372 ff.

Breyer, Patrick 2005: Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal 11: 365-375.

Brown, Ian/Korff, Douwe 2009: Terrorism and the Proportionality of Internet Surveillance, European Journal of Criminology 6, 119-134.

Custers, Bart 2008: Tapping and Data Retention in Ultrafast Communication Networks, Journal of International Commercial Law and Technology 3, 94-100.

Espiner, Tom 2009: Internet data-retention law comes into force, ZDNet.co.uk, 06.04.2009; http://www.zdnet.co.uk/news/networking/2009/04/06/internet-data-retention-law-comes-into-force-39637592/ (Abrufdatum: 16.09.2011)

Europäisches Parlament und Europäischer Rat 2006: Richtlinie *2006*/24/EG vom 15. März 2006 über die Vorratsspeicherung von Daten; Amtsblatt der EU 13.04.2006, L 105/55, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:DE:PDF. (Abrufdatum: 16.09.2011)

Evans, Jonathan 2007: Full text of MI5 Director General's speech, Daily Telegraph, 07.11.2007; http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/11/05/nevans205.xml. (Abrufdatum: 16.09.2011)

Grice, Andrew 2009: Straw Forced into Retreat over Big Brother Data Sharing Plan; The Independent, 24.2.2009.

Home Office 2007 b: Acquisition and Disclosure of Communications Data – Code of Practice, 1.10.2007, 10.

Home Office 2007 a: The United Kingdom Security & Counter-Terrorism Science & Innovation Strategy, Juni 2007.

Home Office 2007 c: EXPLANATORY MEMORANDUM TO THE DATA RETENTION (EC DIRECTIVE) REGULATIONS, http://www.opsi.gov.uk/si/em2007/uksiem_20072199_en.pdf. (Abrufdatum 20.09.2011)

Home Office 2008: A consultation paper – Transposition of Directive 2006/24/EC, August 2008.

Home Office 2009 a: Impact Assessment of the Final Transposition of the EU Data Retention Directive, 10.02.2009.

Home Office 2009 b: Government Response to the Public Consultation of the Transposition of Directive 2006/24/EC – Final Impact Assessment, 11.2.2009.

Home Office 2011: Counter-terrorism strategy, http://www.homeoffice.gov.uk/counter-terrorism/uk-counter-terrorism-strat/. (Abrufdatum: 10.9.2011)

Jones, Richard 2008: UK data retention regulations, Computer Law and Security Report 24, 147-150.

Kennedy, Paul 2007: Report of the Interception of Communications Commissioner for 2007. https://www.mi5.gov.uk/output/uk-interception-of-comm-report-2007.pdf. (Abrufdatum 10.9.2011)

Kindt, Anne 2009: Die grundrechtliche Überprüfung der Vorratsdatenspeicherung: EuGH oder BVerfG – wer traut sich?, MMR, 661 ff.

Legrand, Pierre 1996: How to compare now, Legal Studies 1996, 232 ff.

Leutheusser-Schnarrenberger, Sabine 2007: Vorratsdatenspeicherung – ein vorprogrammierter Verfassungskonflikt, ZRP, 9-13.

Milford, Peter 2008: The retention of communications data: a view from industry, Practical Law Company IP& IT; http://www.petermilford.com/downloads/Data_Retention_PMilford.pdf. (Abrufdatum 16.04.2011)

Mitrou, Lilian 2010: The impact of communications data retention on fundamental rights and democracy – the case of the EU Data Retention Directive, in: Haggerty, *Kevin/Samatas, Minas* (Hrsg.): Surveillance and Democracy, Oxon, 127-147.

Mitrou, Lilian 2008: Retention: A Pandora's Box for Rights and Liberties?, in: Acquisti Allesandro et al (Hrsg.): Digital Privacy: Theory, Technologies, and Practices, New York, 409-433.

Nettleton, Ewan/Watts, Mark 2007: Assessing the costs of data retention in the UK, Journal of Database Marketing & Customer Strategy Management, 56-59.
Neumann, Peter 2008: Innere Sicherheit in Großbritannien, Internationale Politikanalyse der Friedrich Ebert Stiftung, http://library.fes.de/pdf-files/id/ipa/05226.pdf
OUT -LAW.COM 2006: Redbus and Demon founder denied RIPA appeal. In: The Register, 03.02.2006; http://www.theregister.co.uk/2006/02/03/redbus_founder_denied_ripa_appeal/. (Abrufdatum: 16.09.2011)*Pounder, Chris/Kosten, Freddy* 1993: Managing Data Protection, Oxford.
Reiner, Robert 2007: Media Made Criminality: The Representation of Crime in the Mass Media, in: Maguire, Mike/Morgan, Rod/Reiner, Robert (Hrsg.): The Oxford Handbook of Criminology, Oxford, 302-337.
Roßnagel, Alexander 2010: Die „Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung, NJW, S. 1238-1242.
Schweda, Sebastian: Richtline 2006/24/EG: Umsetzungsunterschiede in der EU, in: Bug, Mathias/Schmid, Viola/ Münch, Ursula 2011: Innere Sicherheit – auf Vorrat gespeichert? Tagungsband 2. SIRA Conference Series. S. 56-86.
Smith, Jacqui (Home Secretary) 2008: Speech to the Institute for Public Policy Research Commission on National Security, 15.10.2008. http://press.homeoffice.gov.uk/Speeches/speechto-ippr. /(Abrufdatum 16.09.2011)
Stampfel, G. et al 2007: Implications of the EU Data Retention Directive 2006/24/EC, Wien, http://eprints.cs.univie.ac.at/331/1/ImplicationsEUDR.pdf.
Taylor, Richard: Data Retention: a balancing act for telcos, TimesOnline, 10.5.2007.
UK Government 2000 a: Regulation of Investigatory Powers Act 2000 http://www.legislation.gov.uk/ukpga/2000/23/contents. (Abrufdatum: 16.09.2011)
UK Government 2000 b: Regulation of Investigatory Powers (Scotland) Act 2000 http://www.legislation.gov.uk/asp/2000/11/contents (Abrufdatum 16.09.2011)
UK Government 2001: Anti-terrorism, Crime and Securiy Act 2001; http://www.legislation.gov.uk/ukpga/2001/24/contents. (Abrufdatum: 16.09.2011)
UK Government 2002: Regulation of Investigatory Powers Act 2000 Amendment Order Northern Ireland 2002 http://www.legislation.gov.uk/nisr/2002/183/contents/made
UK Government 2011: Protection of Freedoms Bill 2010-11; http://services.parliament.uk/bills/2010-11/protectionoffreedoms.html. (Abrufdatum: 16.09.2011)
UK Government 2010: A Strong Britain in an Age of Uncertainty: The National Security Strategy, Presented to Parliament by the Prime Minister by Command of Her Majesty, October 2010 http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf?CID=PDF&PLA=furl&CRE=nationalsecuritystrategy (Abrufdatum: 16.09.2011)
UK Parliament 2011: Protection of Freedom Bill 2010-2011, http://services.parliament.uk/bills/2010-11/protectionoffreedoms.html. (Abrufdatum 10.6.2011)
Verkaik, Robert 2008: Government black boxes will collect every email, The Independent, 5.11.2008; http://www.independent.co.uk/news/uk/home-news/government-black-boxeswill-collect-every-email-992268.html. (Abrufdatum: 01.05.2011)
Walker, Claire 2009: Data retention in the UK: Pragmatic and proportionate or a step too far? Computer Law & Security Report, 325-334.
Williams, Chris 2008: Spy chiefs plot £12bn IT spree for comms uberdatabase'', The Register, 7.10.2008; http://www.theregister.co.uk/2008/10/07/detica_interception_modernisation/. (Abrufdatum: 16.09.2011)
Williams, Chris 2009 a: Confusion reigns ahead of comms uberdatabase'', The Register, 09.01.2009; http://www.theregister.co.uk/2009/01/09/imp_eudrd/. (Abrufdatum: 16.09.2011)
Williams, Chris 2009 b: Two convicted for refusal to decrypt data, The Register, 11.08.2009; http://www.theregister.co.uk/2009/08/11/ripa_iii_figures/. (Abrufdatum: 16.09.2011)
WTWU 2009: „*The Data Retention* (EC Directive) Regulations 2009 come into force on 6th April 2009" http://p10.hostingprod.com/@spyblog.org.uk/blog/2009/03/the-data-retention-ec-directive-regulations-2009-come-into-force-on-6th-april-20.html. (Abrufdatum: 16.09.2011)

Rechtsprechung

Semayne's Case, 5 Co. Rep. 91a, 91b, 77 Eng. Rep. 194, 195 (1603); Curtis' Case, Fost. 135, 168 Eng. Rep. 67, entschieden 1756.

Dr. Susanne Beck, LL.M. (LSE) ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Strafrecht u.a. (Prof. Dr. Dr. Eric Hilgendorf), Universität Würzburg. E-Mail: s.beck@jura.uni-wuerzburg.de

SIRA
Sicherheit im öffentlichen Raum

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Herausgebende Stelle:
SIRA-Konsortium

der Bundeswehr
Universität München

der Bundeswehr
Universität München

Fraunhofer ISI
Fraunhofer IOSB

TECHNISCHE UNIVERSITÄT DARMSTADT

European Business School
International University · Schloss Reichartshausen

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Die Herausgabe der SIRA-Working Paper Series erfolgt im Rahmen des Forschungsprojektes *Sicherheit im öffentlichen Raum*. Das Projekt wird im Zuge der Bekanntmachung *Gesellschaftliche Dimensionen der Sicherheitsforschung* im Rahmen des Programms *Forschung für zivile Sicherheit* der Bundesregierung vom Bundesministerium für Bildung und Forschung (BMBF) gefördert. Die Aufnahme eines Textes in diese Reihe soll die Veröffentlichung an anderer Stelle nicht einschränken. Das Copyright verbleibt bei den Autorinnen und Autoren. Der Autor/die Autorin des Arbeitspapiers ist für den Inhalt des Textes verantwortlich.

www.sira-security.de