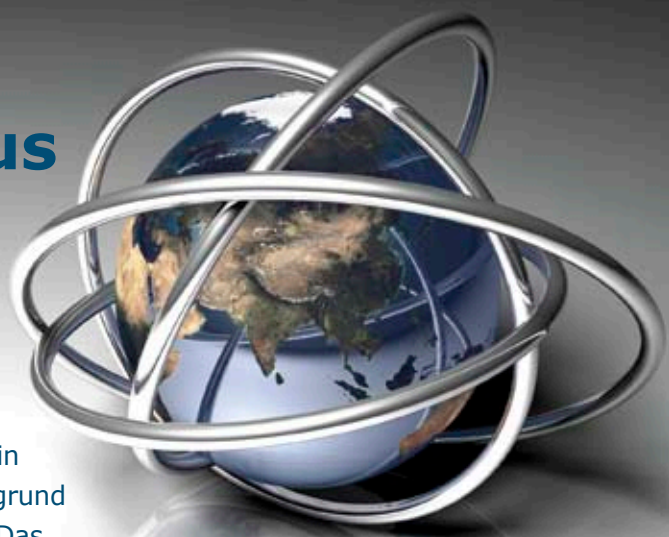
BIGS | Essenz

Brandenburgisches Institut für GESELLSCHAFT und SICHERHEIT

Sicherheitspolitik versus Datenschutz? –

Die Kontroverse um die Vorratsdatenspeicherung



Die Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung in deutsches Recht wird kontrovers diskutiert werden. Im Vordergrund stehen hierbei insbesondere datenschutzrechtliche Bedenken. Das Bundesverfassungsgericht stufte das Gesetz 2010 als verfassungswidrig ein. Eine Einigung der Bundesregierung auf einen neuen Gesetzentwurf steht bisher noch aus.

Constance P. Baban

Nummer 11 · November 2012

Einleitung

Mit der umfassenden Digitalisierung vieler gesellschaftlicher Bereiche und der Transformation der Gesellschaft hin zu einer Informationsgesellschaft haben sich nicht nur die Möglichkeiten der Vernetzung in einer Vielzahl von Lebensbereichen erhöht, sondern im gleichen Zug haben sich auch die sicherheitspolitisch relevanten Schutzräume erweitert. Zugleich hat damit auch eine Erweiterung der Zugriffsräume also der prinzipiellen Möglichkeiten zur Aufklärung und Verfolgung von Straftaten sowie zur Abwehr von Gefahren stattgefunden. Doch nicht alles, was durch diesen technischen Fortschritt im Bereich der Verbrechensbekämpfung und der Gefahrenabwehr möglich ist, fußt per se auf einer verfassungsrechtlichen Grundlage oder trifft auf eine breite gesellschaftspolitische Akzeptanz. Hierunter fällt auch die sogenannte Vorratsdatenspeicherung, die mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG am 9. November 2007 vom Deutschen Bundestag verabschiedet wurde. Die Massenklage des Arbeitskreises Vorratsdatenspeicherung vor dem Bundesverfassungsgericht gegen die Vorratsdatenspeicherung, an der sich rund 35.000 Bürger beteiligten, war in dieser Dimension bisher einmalig. Während das Bundesverfassungsgericht die Umsetzung der EG-Richtlinie in deutsches Recht im März 2010 für nicht mit dem Telekommunikationsgeheimnis (Artikel 10 GG) vereinbar und damit für verfassungswidrig erklärt hat, pochte die Europäische Kommission auf eine zügige Umsetzung der Richtlinie und reichte im Juli 2012 vor dem Europäischen Gerichtshof Klage gegen die Bundesregierung ein. Dabei ist die Kritik am Umgang mit technischen Fortentwicklungen im Politikfeld der Inneren Sicherheit nicht per se neu oder gar ausschließlich auf neue Bedrohungslagen wie den transnationalen Terrorismus zurückzuführen. So wurde zum Beispiel in den 1990er Jahren die Gesetzgebung zum sogenannten „Großen Lauschangriff", der akustischen Wohnraumüberwachung, kontrovers diskutiert.

In diesem BIGS Essenz Paper werden die Hintergründe der Vorratsdatenspeicherung skizziert und das Spektrum der mit der Umsetzung der europäischen Richtlinie verbundenen Positionen anhand des sicherheitspolitischen Diskurses ergründet. Dabei wird das Ziel verfolgt, die Facetten des Aspekts Datenschutz als Herausforderung für die Sicherheitspolitik Deutschlands anhand der Kontroverse um die Vorratsdatenspeicherung beispielhaft zu betrachten.

BIGS
BRANDENBURGISCHES INSTITUT
für GESELLSCHAFT und SICHERHEIT

Hintergründe der Vorratsdatenspeicherung

Verfassungsrechtliche Grundlagen für den Datenschutz in Deutschland

Der Begriff des Datenschutzes selbst wird nicht explizit im Grundgesetz genannt, er manifestiert sich jedoch im allgemeinen Persönlichkeitsrecht, welches aus einer Verbindung von Artikel 2 Absatz 1 GG (Freie Entfaltung der Persönlichkeit) in Verbindung mit Artikel 1 Absatz 1 GG (Menschenwürde) hervorgeht.[1] Für den Rechtswissenschaftler Alexander Roßnagel ist „Datenschutz [...] ein irreführender Begriff, denn es sollen nicht die Daten (des Datenbesitzers) geschützt werden, sondern die informationelle Selbstbestimmung (des Betroffenen).“[2] Zudem ist eine wichtige Säule des Datenschutzes in Deutschland das grundrechtlich verankerte Telekommunikationsgeheimnis (Artikel 10 GG).

Ein bedeutender Schritt in der Entwicklung des Datenschutzes in Deutschland war das sogenannte Volkszählungsurteil des Bundesverfassungsgerichts von 1983, bei dem das Bundesverfassungsgericht aus dem allgemeinen Persönlichkeitsrecht das Recht auf informationelle Selbstbestimmung ableitete[3] und somit den Datenschutz grundrechtlich verankerte.[4] Das Urteil zur Volkszählung legte zudem die Grundlage für eine Neuausrichtung der bis zu diesem Zeitpunkt noch jungen Datenschutzgesetzgebungen auf Bundes- und Länderebene.

Ein wichtiger Schritt in der Entwicklung des Datenschutzes: das Volkszählungsurteil von 1983

Plenarsaal des Deutschen Bundestages
© Makrodepecher/pixelio.de

Was ist die Vorratsdatenspeicherung?

Grundsätzlich bezieht sich der Begriff der Vorratsdatenspeicherung auf den Vorgang der anlassunabhängigen Speicherung von Telekommunikationsdaten, wie Telefondaten (Festnetz, Mobilfunk, SMS und MMS) sowie Internet- und E-Mail-Daten, über einen definierten Zeitraum. Sie soll der Gefahrenabwehr sowie der Strafverfolgung dienen. Die mit der EU-Richtlinie verbundene Form der Vorratsdatenspeicherung zielt nicht auf die Speicherung von konkreten Kommunikationsinhalten. Auf der Webseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Peter Schaar, werden die wichtigsten Aspekte der Vorratsdatenspeicherung – so wie sie in Deutschland zunächst umgesetzt wurden – zusammengefasst:

„Das Gesetz verpflichtet die Anbieter von öffentlich zugänglichen Telekommunikations- und Internetdiensten, umfangreiche Verkehrsdaten auf Vorrat für die Strafverfolgungsbehörden zu speichern, ohne dass ein konkreter Verdacht vorliegen muss. Verkehrsdaten sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden, wie zum Beispiel Telefon-/Faxnummern, IP-Adressen, Datum, Uhrzeit, Dauer der Verbindung oder Datenmenge. Diese Verkehrsdaten inklusive der Standortdaten, die beim Telefonieren, Faxen, Mailen, Surfen oder Chatten anfallen, müssen ohne konkreten Anlass für sechs Monate vorgehalten werden.“[5]

Als zentrale (Kritik-)Punkte sind aus datenschutzrechtlicher Sicht zunächst die Aspekte der verdachtsunabhängigen Speicherung sämtlicher Kommunikationsdaten sowie die Speicherdauer von sechs Monaten hervorzuheben. Zwar wurden die Verkehrsdaten auch bisher von den Telekommunikationsanbietern erfasst, durften aber nur zu Abrechnungszwecken gespeichert werden und alle weiteren, nicht abrechnungsrelevanten Daten, waren umgehend zu löschen.[6] Vor diesem Hintergrund problematisiert Peter Schaar die mit dem Gesetz zur Vorratsdatenspeicherung verbundene Praxis, dass „das gesamte Telekommunikationsverhalten der Bevölkerung erfasst [wird], obwohl nur ein verschwindend kleiner Teil der gigantischen Datenmenge zur Aufklärung schwerer Straftaten beitragen kann.“[7]

Anlass und Ziele der Vorratsdatenspeicherung

Der Anlass für die Initiative zu einer EU-weiten Vorratsdatenspeicherung waren primär die Terror-Anschläge in Madrid am 11. März 2004 sowie die in London am 7. Juli 2005. In der abschließenden Beratung des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG am 9. November 2007 erläuterte die damalige Justizministerin Brigitte Zypries die Entstehung der EU-Richtlinie:

„Das Gesetz zur Vorratsdatenspeicherung dient der Umsetzung einer europäischen Richtlinie. Wie kam es zu dieser europäischen Richtlinie? Nach den Attentaten von Madrid wurde anhand von Handys, die man gefunden hatte, festgestellt, mit wem die Attentäter zuvor telefoniert hatten. Auf diese Weise konnte man andere aus dem terroristischen Umfeld fangen, die an den Attentaten beteiligt waren. Das war der Anlass für England, Schweden, Frankreich und Irland, eine Initiative im Rat zu starten mit dem Ziel, dass künftig in ganz Europa Verbindungsdaten gespeichert werden."[8]

Als maßgebliche Ziele der EU-Richtlinie zur Vorratsdatenspeicherung können deshalb eine verbesserte Strafverfolgung und Gefahrenabwehr zur Bekämpfung von Terrorismus sowie von Organisierter Kriminalität gesehen werden und zugleich eine Harmonisierung der betreffenden Regelungen auf europäischer Ebene.

Europafahne © Stephanie Hofschlaeger/pixelio.de

Gesetzgebungsprozess und aktueller Stand

Den Ausgangspunkt für das Gesetz zur Vorratsdatenspeicherung in Deutschland bildete die EU-Richtlinie 2006/24/EG vom 15. März 2006 mit der die Vorratsdatenspeicherung EU-weit eingeführt werden sollte. Mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG wurde diese in deutsches Recht transformiert. Das Gesetz wurde vom Bundestag in der abschließenden Beratung am 9. November 2007 mit der Mehrheit der Stimmen der Großen Koalition (CDU/SPD) und den Gegenstimmen der FDP, der Grünen sowie von DIE LINKE verabschiedet und trat im Januar 2008 in Kraft. Nachdem mehrere Klagen gegen die Vorratsdatenspeicherung eingereicht wurden (Arbeitskreis Vorratsdatenspeicherung, eine Klage von Mitgliedern der FDP um Burkhard Hirsch und Gerhard Baum sowie einer Organklage der Bundestagsfraktion der Grünen) stellte das Bundesverfassungsgericht im März 2010 für die Ausgestaltung der Vorratsdatenspeicherung durch den deutschen Gesetzgeber Verfassungswidrigkeit fest.[9] Mit dieser Feststellung der Verfassungswidrigkeit wurde die Vorratsdatenspeicherung in Deutschland wieder ausgesetzt. Innerhalb der Regierungskoalition konnte zwischen den beteiligten Ministerien, dem Justizministerium (BMJ) sowie dem Bundesministerium des Innern (BMI), keine Einigung über eine neue gesetzliche Regelung zur Vorratsdatenspeicherung erzielt werden. Im Sommer 2011 leitete die Europäische Kommission ein Vertragsverletzungsverfahren gegen Deutschland ein und setzte dann zum 22. März 2012 noch einmal eine einmonatige Frist bis zum 26. April. Nachdem auch diese Frist verstrichen und es zu keiner Einigung zwischen den beiden Ministerien gekommen war, reichte die Europäische Kommission schlussendlich eine Klage gegen Deutschland vor dem Europäischen Gerichtshof (EuGH) ein. Nun prüft der EuGH nicht nur die Klage gegen Deutschland, sondern auch die Klage, die der oberste Gerichtshof in Dublin gegen die Vorratsdatenspeicherung eingereicht hatte. Auch auf EU-Ebene steht die Richtlinie auf dem Prüfstand und wird überarbeitet. Eine Vorstellung der überarbeiteten Richtlinie war seitens der EU zunächst für Sommer 2012 geplant, dies wird nun aber möglicherweise erst nach den Wahlen zum Europaparlament 2014 umgesetzt. Bis zur Vorstellung der neuen EU-Richtlinie bleibt die ursprüngliche Fassung weiterhin gültig.

Der sicherheitspolitische Diskurs zur Vorratsdatenspeicherung

Das Urteil des Bundesverfassungsgerichts

Wie vorausgehend angeführt, hat das Bundesverfassungsgericht die Umsetzung der EU-Richtlinie durch den deutschen Gesetzgeber mit seinem Urteil vom 2. März 2010 für verfassungswidrig erklärt. Als zentrale Gründe für die Verfassungsbeschwerde wurden insbesondere die Verletzung des Telekommunikationsgeheimnisses sowie des Rechts auf informationelle Selbstbestimmung angeführt.[10] In der Pressemitteilung des Bundeverfassungsgerichts wird die Entscheidung wie folgt begründet:

„Der Erste Senat des Bundesverfassungsgerichts hat entschieden, dass die Regelungen des TKG und der StPO über die Vorratsdatenspeicherung mit Art. 10 Abs. 1 GG nicht vereinbar sind. Zwar ist eine Speicherungspflicht in dem vorgesehenen Umfang nicht von vornherein schlechthin verfassungswidrig. Es fehlt aber an einer dem Verhältnismäßigkeitsgrundsatz entsprechenden Ausgestaltung. Die angegriffenen Vorschriften gewährleisten weder eine hinreichende Datensicherheit, noch eine hinreichende Begrenzung der Verwendungszwecke der Daten. Auch genügen sie nicht in jeder Hinsicht den verfassungsrechtlichen Transparenz und Rechtsschutzanforderungen. Die Regelung ist damit insgesamt verfassungswidrig und nichtig."[11]

Gerichtsurteil © Thorben Wengert/pixelio.de

Als problematisch wurde insbesondere erachtet, dass „es sich bei einer solchen Speicherung um einen besonders schweren Eingriff mit einer Streubreite [handelt], wie sie die Rechtsordnung bisher nicht kennt."[12] Die Folgen dieser Form der Vorratsdatenspeicherung wäre so unter anderem, dass „sich aus diesen Daten bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse ziehen [lassen]. 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."[13] Mit seinem Urteil hat das Bundesverfassungsgericht allerdings nicht die EU-Richtlinie selbst als verfassungswidrig eingestuft, sondern die „konkrete Ausgestaltung".[14] Entsprechend kam es nicht zu einer Vorlage der EU-Richtlinie beim Europäischen Gerichtshof (EuGH). Deutlich hat das Bundesverfassungsgericht aufgezeigt, wie sich eine verfassungskonforme Vorratsdatenspeicherung gestalten müsste:

„Die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten setzt voraus, dass diese eine Ausnahme bleibt. Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss".[15]

Hiermit setzte das Bundesverfassungsgericht auch wichtige Signale für den deutschen Gesetzgeber im Hinblick auf die Aufgabe der Bundesrepublik bei Gesetzgebungen im europäischen Gefüge. Denn so wird in der Urteilsbegründung hervorgehoben, dass „[d]er Inhalt der Richtlinie [...] der Bundesrepublik Deutschland einen weiten Entscheidungsspielraum [belässt]. [...] Mit diesem Inhalt kann die Richtlinie ohne Verstoß gegen die Grundrechte des Grundgesetzes umgesetzt werden."[16] Zugleich räumte das Bundesverfassungsgericht jedoch auch ein, welche Bedeutung der Telekommunikation heutzutage in der Gesellschaft und damit für die Gefahrenabwehr und Strafverfolgung zukommt. So stellt sich „[e]ine Speicherung der Telekommunikationsverkehrsdaten für sechs Monate [...] auch nicht als eine Maßnahme dar, die auf eine Totalerfassung der Kommunikation oder Aktivitäten der Bürger insgesamt angelegt wäre. Sie 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."[17]

Die Positionen des Bundesjustizministeriums sowie des Bundesinnenministeriums

Seit der Verkündung des Urteils ist es zwischen dem Bundesjustizministerium und dem Bundesinnenministerium zu keiner Einigung auf eine neue Regelung gekommen. Während sich das Bundesinnenministerium unter Minister Friedrich weiterhin für eine Umsetzung der Regelung in Form einer anlasslosen Speicherung für die Dauer von sechs Monaten ausspricht, plädiert das Bundesjustizministerium unter Ministerin Leutheusser-Schnarrenberger für eine Datenspeicherung bei Vorliegen eines konkreten Verdachtsfalles – ein sogenanntes Quick-Freeze-Verfahren. Dieses Verfahren sieht insofern eine anlassbezogene Sicherung der Daten vor, die generell von den Telekommunikationsunternehmen gespeichert werden und deren Verfügbarkeit für die Strafverfolgungsbehörden dann an einen richterlichen Beschluss gekoppelt ist.[18] Auf das Quick-Freeze-Verfahren konnten sich die beiden Ministerien bisher nicht einigen und auch von der EU wird dieses als nicht ausreichend erachtet. Trotz der möglichen drohenden Strafzahlungen für Deutschland, ist eine Einigung auf eine neue Auflage der Vorratsdatenspeicherung in dieser Legislaturperiode nicht mehr realistisch.

Zentrale Argumentationen für und wider die Vorratsdatenspeicherung

Die zentralen argumentativen Wendungen für und wider die Vorratsdatenspeicherung können analog zu denjenigen Argumentationen abgeleitet werden, die sich allgemein über die Betrachtung des sicherheitspolitischen Diskurses seit 9/11 identifizieren lassen und sich generell auf den Aspekt der Kollision von sicherheitspolitischen Maßnahmen, wie der Datenspeicherung sowie des Datenaustauschs, mit dem Grundrecht des Telekommunikationsgeheimnisses sowie dem Recht auf informationelle Selbstbestimmung beziehen. Neben der Kontroverse um die Vorratsdatenspeicherung kann hier auf die Diskussion um die sogenannte Online-Durchsuchung als prominentes Beispiel verwiesen werden. Wesentliche Aspekte des Für und Wider sind der technologische Fortschritt und die damit einhergehende Erweiterung der Möglichkeiten zur präventiven Gefahrenabwehr sowie allgemein zur Strafverfolgung. Die tatsächliche Nutzung dieser Möglichkeiten steht jedoch in der Kritik, oft zu Lasten des allgemeinen Datenschutzes zu gehen: Sicherheit versus Freiheit.

Darüber hinaus steht die Vorratsdatenspeicherung auch deshalb in der Kritik, weil eine Einführung der Speicherpflicht in Deutschland bis zum Erlass der EU-Richtlinie in Deutschland gescheitert war, wohingegen die EU-Richtlinie Deutschland zur Umsetzung der Vorratsdatenspeicherung binnen 18 Monaten verpflichtete. Entsprechend stand auch der Vorwurf im Raum, dass die EU als Hintertür für nationale Vorhaben genutzt wurde, denn die EU-Vorgabe erweiterte den politischen Möglichkeitsraum der Befürworter der Vorratsdatenspeicherung in Deutschland.

Zugespitzt kollidiert der mit der Kritik an der Vorratsdatenspeicherung verbundene Anspruch auf die Achtung der individuellen Privatsphäre mit der beinahe unumstößlichen Argumentation „Wer nichts zu verbergen hat, hat auch nichts zu befürchten." beziehungsweise „Ich habe nichts zu verbergen."

Der Rechtswissenschaftler Daniel J. Solove von der George Washington Universität in Washington, D.C. nennt diese Form der Argumentation das „Nothing to Hide"-Argument, für das er konstatiert: „This argument permeates the popular discourse about privacy and security issues."[19] Das Problem dieses Arguments sieht Solove darin, dass hiermit ein Missverständnis des Konzepts von Privatheit verbunden ist: „Many commentators who respond to the argument attempt a direct refutation by trying to point to things that people would want to hide. But the problem with the nothing to hide argument is the underlying assumption that privacy is about hiding bad things."[20]

> Datenschutz in Deutschland als elementarer Grundpfeiler einer freiheitlichen Demokratie

Wie der Bundesbeauftragte für Datenschutz hervorhebt, ist allerdings die Privatsphäre nicht nur „Raum des individuellen Rückzugs"[21] sondern „zugleich unverzichtbare Voraussetzung einer freien Meinungsbildung."[22] Diese wiederum ist Voraussetzung für eine freie Öffentlichkeit[23] und damit elementarer Bestandteil jeder funktionierenden Demokratie.

Ausblick: Datenschutz als sicherheitspolitische Herausforderung für die Bundesrepublik Deutschland

Der Blick auf den sicherheitspolitischen Diskurs zur Vorratsdatenspeicherung verdeutlicht die Dreh- und Angelpunkte der Kontroverse. Zugleich wird deutlich, dass der Datenschutz sich als eine wesentliche sicherheitspolitische Herausforderung für die Gegenwart und Zukunft erweist. Der Sicherheitspolitik in Deutschland muss es gelingen, den Spagat zwischen zeitgemäßen sicherheitspolitischen Maßnahmen und datenschutzrechtlichen Anforderungen zu schaffen. Zwar ist Sicherheitspolitik auch immer mit einer Abwägung von Gütern wie Sicherheit und Freiheit verbunden, dennoch muss in einer vernetzten Welt, in der mit Informationen allgemein nicht nur ein sicherheitspolitischer, sondern auch ein ökonomischer und sozialer Wert verbunden ist, der Schutz des Rechts auf informationelle Selbstbestimmung sowie der Telekommunikationsfreiheit generell verfolgt werden – auch damit sich Sicherheitspolitik und Datenschutz nicht als Gegenspieler manifestieren. Hiermit verbunden sind die Verfolgung zentraler datenschutzrechtlicher Prinzipien wie das der Datensparsamkeit sowie das der Datenvermeidung. Im Fall der Vorratsdatenspeicherung agiert die Politik zudem nicht allein, sondern letztlich auch im Zusammenwirken mit den Telekommunikationsunternehmen, an welche die Sammlung und Bereitstellung der Daten vonseiten des Staates übertragen wird. Dies ist für die Unternehmen nicht nur mit der Übernahme einer datenschutzrechtlichen Verantwortung, sondern auch mit Kosten verbunden, die im Gesetzgebungsprozess berücksichtigt werden müssen. So beliefen sich zum Beispiel laut Verband der deutschen Internetwirtschaft die mit der Umsetzung der Vorratsdatenspeicherung verbundenen Kosten für die Internetprovider auf rund 330 Millionen Euro.[24] Datensparsamkeit und Datenvermeidung erweisen sich sodann auch mit Blick auf die an die Wirtschaft herangetragenen Aufgaben und die damit verbundenen volkswirtschaftlichen Belastungen als wesentlich. In einer langfristigen Perspektivierung besteht im Hinblick auf diese Verquickung von Politik, Unternehmen und Datensammlung zudem die Gefahr einer Normalisierungstendenz dahingehend, dass Unternehmen unter dem Vorwand der Sicherheit vermehrt Daten über Kunden und Mitarbeiter sammeln.

Der Fokus auf den Datenschutz wird, wie sich anhand der EU-Richtlinie verdeutlichen lässt, zudem auch deshalb zentral sein, weil datenfokussierte Sicherheitspolitik bereits heute und auch in Zukunft nicht mehr nur eine nationale Angelegenheit sein kann. Hier wird auch die EU als Impulsgeber für Gesetze zukünftig noch stärker aktiv werden. Dies bedeutet für die Bundesrepublik, dass der Datenschutz umso mehr eine Aufgabe für nationale Politik in europäisierten Politikprozessen sein muss. Nicht umsonst hat das Bundesverfassungsgericht in seinem Urteil auf die „verfassungsrechtliche Identität Deutschlands“[25] verwiesen „für deren Wahrung sich die Bundesrepublik in europäischen und internationalen Zusammenhängen einsetzen muss.“[26]

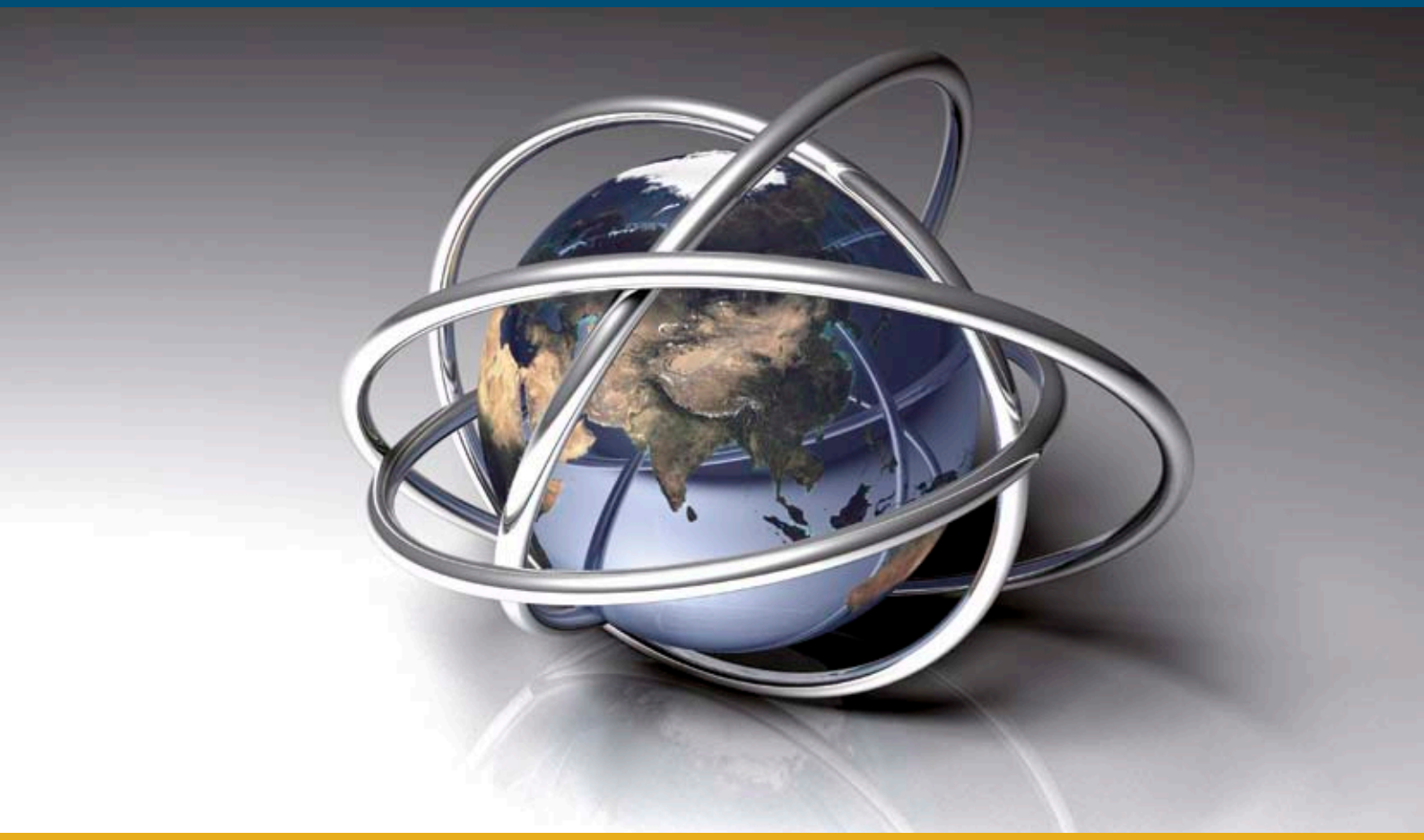
„Gläserne Menschen“ © Helmut J. Salzer/pixelio.de

Fußnoten

1. Vgl. Tinnefeld, Marie-Theres/Buchner, Benedikt/Petri, Thomas (2012): Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht. 5. Auflage. München: Oldenbourg Wissenschaftsverlag GmbH. Hier: S. 91.
2. Roßnagel, Alexander (2006): Datenschutz im 21. Jahrhundert. In: APuZ 5-6/2006. S. 9-15. Hier: S. 10.
3. Vgl. Tinnefeld et. al (2012), insbesondere S. 102ff.
4. Vgl. Garstka, Hans-Jürgen (2003): Informationelle Selbstbestimmung und Datenschutz. Das Recht auf Privatsphäre. In: Schulzki-Haddouti, Christiane (Hrsg.): Bürgerrechte im Netz. Schriftenreihe (Bd. 382) Bundeszentrale für Politische Bildung. Opladen: Leske + Budrich. S. 48-70. Hier: S. 48.
5. „Vorratsdatenspeicherung" In: Webseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (ohne Jahr). Verfügbar unter: http://www.bfdi.bund.de/DE/Schwerpunkte/Vorratsdaten/Artikel/Vorratsdatenspeicherung.html?nn=408922 [28.11.2012].
6. Vgl. Schaar, Peter (2008): Der Rüstungswettlauf in der Informationstechnologie. In: Huster, Stefan/Rudolph, Karsten (Hrsg.): Vom Rechtsstaat zum Präventionsstaat. Frankfurt am Main: Suhrkamp. S. 45-63. Hier: S. 55.
7. Ebd.
8. Brigitte Zypries, Bundesministerin der Justiz Zweite und Dritte Beratung des Gesetzes zur Vorratsdatenspeicherung 2007. Siehe Plenarprotokoll 16/124. S. 12993-13011. Hier: S. 12994.
9. Siehe BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. (1-345). Verfügbar unter: http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html [28.11.2012].
10. Vgl. Bundesverfassungsgericht – Pressestelle (02.03.2010): „Konkrete Ausgestaltung der Vor-ratsdatenspeicherung nicht verfassungsgemäß". Pressemitteilung Nr. 11/2010. Verfügbar unter: http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011 [28.11.2012].
11. Ebd.
12. Ebd.
13. Ebd.
14. Ebd.
15. Ebd.
16. Ebd.
17. Ebd.
18. Vgl. „Quick Freeze/Datensicherung" In: Webseite des Bundesministeriums der Justiz (ohne Jahr). Verfügbar unter: http://www.bmj.de/DE/Buerger/digitaleWelt/QuickFreeze/quickfreeze_node.html [28.11.2012].
19. Solove, Daniel J. (2007): I've Got Nothing to Hide' and Other Misunderstandings of Privacy. San Diego Law Review, Vol. 44, 2007; GWU Law School Public Law Research Paper No. 289. S. 745-772. Hier: S. 748. Verfügbar unter: http://ssrn.com/abstract=998565 [28.11.2012].
20. Ebd., S. 764.
21. Schaar, Peter (2007): Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft. München: C. Bertelsmann Verlag. Hier: S. 15.
22. Ebd.
23. Vgl. ebd.
24. Vgl. eco Verband der deutschen Internetwirtschaft e.V. (26.04.2012): „eco: Einführung der Vorratsdatenspeicherung verursacht mehr wirtschaftlichen Schaden als Brüsseler Strafzahlungen". eco Pressemeldungen. Verfügbar unter: http://www.eco.de/2012/pressemeldungen/eco-einfuehrung-der-vorratsdatenspeicherung-verursacht-mehr-wirtschaftlichen-schaden-als-bruesseler-strafzahlungen.html [28.11.2012].
25. Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung: BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. (1 - 345), Hier: Absatz 218. Verfügbar unter: http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html [28.11.2012].
26. Ebd.

Autorin

Constance P. Baban ist Senior Research Fellow am BIGS und Non-Resident Fellow im Programmbereich Außen- und Innenpolitik des American Institute for Contemporary German Studies (AICGS) an der Johns Hopkins Universität in Washington, D.C., an dem sie 2010 zur Europäisierung von Deutschlands innerer Sicherheitspolitik forschte. Sie studierte Angewandte Deutsche Sprachwissenschaft, Politische Wissenschaft sowie Medien- und Kommunikationswissenschaft an der Leibniz Universität Hannover und promovierte im Anschluss über den sicherheitspolitischen Wandel seit 9/11 in der Bundesrepublik Deutschland. Ihre Dissertation „Der innenpolitische Sicherheitsdiskurs in Deutschland" wird im Frühjahr 2013 bei Springer VS veröffentlicht. Neben dem Fokus auf Kommunikationsprozesse im Politikfeld der inneren Sicherheit umfasst ihre Expertise die deutsche Sicherheitspolitik mit einem europäischen und transatlantischen Fokus sowie die Analyse von sicherheitspolitischen Strukturen und deren Veränderungen unter Einbezug der Analyse von sicherheitspolitischen Diskursen.



IMPRESSUM

Die Brandenburgische Institut für Gesellschaft und Sicherheit (BIGS) gGmbH ist ein unabhängiges, überparteiliches und nicht-gewinnorientiertes wissenschaftliches Institut, das zu gesellschaftswissenschaftlichen Fragen ziviler Sicherheit forscht. Das BIGS publiziert seine Forschungsergebnisse und vermittelt diese in Veranstaltungen an eine interessierte Öffentlichkeit. Es entstand im Frühjahr 2010 in Potsdam unter der Beteiligung der Universität Potsdam und ihrer UP Transfer GmbH sowie der Unternehmen EADS, IABG und Rolls-Royce. Es wird vom Land Brandenburg gefördert. Alle Aussagen und Meinungsäußerungen in diesem Papier liegen in der alleinigen Verantwortung des Autors bzw. der Autoren.

Autor:

Constance P. Baban

Titel:

Sicherheitspolitik versus Datenschutz? –
Die Kontroverse um die EU-Richtlinie zur Vorratsdatenspeicherung

Herausgeber:

Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH
Dr. Tim H. Stuchtey (V.i.S.d.P.)

ISSN 2191-6756

Weitere Informationen über die Veröffentlichungen des BIGS befinden sich auf der Webseite des Instituts:

www.bigs-potsdam.org

BIGS
BRANDENBURGISCHES INSTITUT für GESELLSCHAFT und SICHERHEIT

Geschäftsführender Direktor: Dr. Tim H. Stuchtey
Rudolf-Breitscheid-Straße 178 · 14482 Potsdam
Tel.: +49-331-704406-0 · Fax: +49-331-704406-19 · info@bigs-potsdam.org · www.bigs-potsdam.org