An den Kanzler
des Europäischen Gerichtshofs für Menschenrechte
Europarat
F-67075 STRASBOURG CEDEX

Beschwerde

1. des Herrn Patrick Breyer, [*...anonymisiert...*],
2. des Herrn Wolfgang Wieland (MdB), Deutscher Bundestag, Platz der Republik 1, 11011 Berlin.

gegen

die Bundesrepublik Deutschland

Inhaltsübersicht

A. GEGENSTAND DER BESCHWERDE 4

B. BETROFFENHEIT 9

C. SUBSIDIARITÄT 10

D. BEGRÜNDETHEIT DER BESCHWERDE 11

I. Verletzung des Art. 8 EMRK 11

1. Schutzbereich 11
2. Grundrechtseingriff 12
3. Mangelnde Rechtfertigung 15
   a) Mangelnde Vorhersehbarkeit und Präzision 15
   b) Verletzung des Verhältnismäßigkeitsgebots 17
      aa) Legitimes Ziel 18
      bb) Verhältnismäßigkeit 18
         (1) Gewicht des Eingriffsinteresses 18
         (2) Gewicht des beeinträchtigten Freiheitsinteresses 19
            (a) Maßgebliche Kriterien 19
            (b) Tragweite des § 5 BSIG 21
            (c) Insbesondere: Aussagekraft von Verkehrs- und Nutzungsdaten 23
            (d) Sicherheitsrisiken und sonstige Nachteile für Internetnutzer 25
            (e) Diskriminierung 27
         (3) Zentralisierung nicht erforderlich 28
         (4) Unverhältnismäßigkeit einer Vorratsdatenspeicherung 30
            (a) Übertragbarkeit des Urteils des EGMR in Sachen S. und Marper 30
            (b) Vorratsdatenspeicherung verzichtbar für die Strafverfolgung 32
               (aa) Minimale Relevanz für die Strafverfolgung 33
               (bb) Fehlende Relevanz für die Aufklärungsquote 35
               (cc) Unverhältnismäßigkeit 36
            (c) Unzumutbar schwerer Grundrechtseingriff 37
               (aa) Staatliche Fehlurteile 38
               (bb) Risiko von Datenpannen und des Missbrauchs durch Private 39
               (cc) Abschreckungswirkung 41
               (dd) Meinungsumfragen belegen Abschreckungswirkung 44
               (ee) Bedeutung von Anonymität für unsere Gesellschaft 45
            (d) Verletzung der Unschuldsvermutung 46
            (e) Weitere Rechtsprechung 47
            (f) Drohender Dammbruch 51
         (5) Unverhältnismäßiges Erkennen und Beseitigen von Störungen und Fehlern (§ 5 Abs. 1 S. 1 Nr. 1 Var. 1 BSIG) 52
            (a) Kommunikationsverkehrsdaten 53

(b) Telemedien-Nutzungsdaten 55
(6) Unverhältnismäßiges Erkennen und Beseitigen von Angriffen (§ 5 Abs. 1 S. 1 Nr. 1 Var. 2 BSIG) 58
(a) Verkehrsdaten 62
(aa) Schadprogramme 62
(bb) Überflutung 63
(cc) Einbruchsversuche 64
(b) Telemedien-Nutzungsdaten 65
(aa) Überflutung 65
(bb) Einbruchsversuche 67
(7) Unverhältnismäßige Abwehr von Schadprogrammen (§ 5 Abs. 1 S. 1 Nr. 2 BSIG) 68
(8) Unverhältnismäßige Vorratsdatenspeicherung (§ 5 Abs. 2 BSIG) 69
(9) Ergebnis 71
II. Verletzung des Art. 10 EMRK 73
1. Schutzbereich 73
2. § 5 BSIG als Eingriff 76
3. Mangelnde Rechtfertigung 78

A. Gegenstand der Beschwerde

Wir wenden uns gegen § 5 BSI-Gesetz, weil die dort vorgesehene Sammlung von Informationen über unser Kommunikations- und Informationsverhalten unsere Menschenrechte verletzt.

§ 5 BSIG lautet:

§ 5 Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes

(1) [1]Das Bundesamt darf zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes

1. Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen, erheben und automatisiert auswerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist,

2. die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auswerten, soweit dies für die Erkennung und Abwehr von Schadprogrammen erforderlich ist.

[2]Sofern nicht die nachfolgenden Absätze eine weitere Verwendung gestatten, muss die automatisierte Auswertung dieser Daten unverzüglich erfolgen und müssen diese nach erfolgtem Abgleich sofort und spurenlos gelöscht werden. [3]Die Verwendungsbeschränkungen gelten nicht für Protokolldaten, sofern diese weder personenbezogene noch dem Fernmeldegeheimnis unterliegende Daten beinhalten. [4]Behördeninterne Protokolldaten dürfen nur im Einvernehmen mit der jeweils betroffenen Behörde erhoben werden.

(2) [1]Protokolldaten nach Absatz 1 Satz 1 Nummer 1 dürfen über den für die automatisierte Auswertung nach Absatz 1 Satz 1 Nummer 1 erforderlichen Zeitraum hinaus, längstens jedoch für drei Monate, gespeichert werden, soweit tatsächliche Anhaltspunkte bestehen, dass diese für den Fall der Bestätigung eines Verdachts nach Absatz 3 Satz 2 zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich sein können. [2]Durch organisatorische und technische Maßnahmen ist sicherzustellen, dass eine Auswertung der nach diesem Absatz gespeicherten Daten nur automatisiert erfolgt. [3]Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist. [4]Eine nicht automatisierte Auswertung oder eine personenbezogene Verwendung ist nur nach Maßgabe der nachfolgenden Absätze zulässig. [5]Soweit hierzu die Wiederherstellung des Personenbezugs pseudonymisierter Daten erforderlich ist, muss diese durch den Präsidenten des Bundesamts angeordnet werden. [6]Die Entscheidung ist zu protokollieren.

(3) [1]Eine über die Absätze 1 und 2 hinausgehende Verwendung personenbezogener Daten ist nur zulässig, wenn bestimmte Tatsachen den Verdacht begründen, dass

1. diese ein Schadprogramm enthalten,

2. diese durch ein Schadprogramm übermittelt wurden oder

3. sich aus ihnen Hinweise auf ein Schadprogramm ergeben können,

und soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen. [2]Im Falle der Bestätigung ist die weitere Verarbeitung personenbezogener Daten zulässig, soweit dies

1. zur Abwehr des Schadprogramms,

2. zur Abwehr von Gefahren, die von dem aufgefundenen Schadprogramm ausgehen oder

3. zur Erkennung und Abwehr anderer Schadprogramme erforderlich ist.

[3]Ein Schadprogramm kann beseitigt oder in seiner Funktionsweise gehindert werden. [4]Die nicht automatisierte Verwendung der Daten nach den Sätzen 1 und 2 darf nur durch einen Bediensteten des Bundesamtes mit der Befähigung zum Richteramt angeordnet werden.

(4) [1]Die Beteiligten des Kommunikationsvorgangs sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder von Gefahren, die von einem Schadprogramm ausgehen, zu benachrichtigen, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange Dritter entgegenstehen. [2]Die Unterrichtung kann unterbleiben, wenn die Person nur unerheblich betroffen wurde und anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat. [3]Das Bundesamt legt Fälle, in denen es von einer Benachrichtigung absieht, dem behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem weiteren Bediensteten des Bundesamtes, der die Befähigung zum Richteramt hat, zur Kontrolle vor. [4]Der behördliche Datenschutzbeauftragte ist bei Ausübung dieser Aufgabe weisungsfrei und darf deswegen nicht benachteiligt werden (§ 4f Absatz 3 Bundesdatenschutzgesetz). [5]Wenn der behördliche Datenschutzbeauftragte der Entscheidung des Bundesamtes widerspricht, ist die Benachrichtigung nachzuholen. [6]Die Entscheidung über die Nichtbenachrichtigung ist zu dokumentieren. [7]Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. [8]Sie ist nach zwölf Monaten zu löschen. [9]In den Fällen der Absätze 5 und 6 erfolgt die Benachrichtigung durch die dort genannten Behörden in entsprechender Anwendung der für diese Behörden geltenden Vorschriften. [10]Enthalten diese keine Bestimmungen zu Benachrichtigungspflichten, sind die Vorschriften der Strafprozessordnung entsprechend anzuwenden.

(5) [1]Das Bundesamt kann die nach Absatz 3 verwendeten personenbezogenen Daten an die Strafverfolgungsbehörden zur Verfolgung einer mittels eines Schadprogramms begangenen Straftat nach den §§ 202a, 202b, 303a oder 303b des Strafgesetzbuches übermitteln. [2]Es kann diese Daten ferner übermitteln

1. zur Abwehr einer Gefahr für die öffentliche Sicherheit, die unmittelbar von einem Schadprogramm ausgeht, an die Polizeien des Bundes und der Länder,

2. zur Unterrichtung über Tatsachen, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht erkennen lassen, an das Bundesamt für Verfassungsschutz.

(6) [1]Für sonstige Zwecke kann das Bundesamt die Daten übermitteln

1. an die Strafverfolgungsbehörden zur Verfolgung einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere einer in § 100a der Strafprozessordnung bezeichneten Straftat,

2. an die Polizeien des Bundes und der Länder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist,

3. an die Verfassungsschutzbehörden des Bundes und der Länder, wenn tatsächliche Anhaltspunkte für Bestrebungen in der Bundesrepublik Deutschland vorliegen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 3 Absatz 1 des Bundesverfassungsschutzgesetzes genannten Schutzgüter gerichtet sind.

[2]Die Übermittlung nach Satz 1 Nummer 1 bedarf der vorherigen gerichtlichen Zustimmung. [3]Für das Verfahren nach Satz 1 Nummer 1 gelten die Vorschriften des Gesetzes über die Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. [4]Zuständig ist das Amtsgericht, in dessen Bezirk das Bundesamt seinen Sitz hat. [5]Die Übermittlung nach Satz 1 Nummer 3 erfolgt nach Zustimmung des Bundesministeriums des Innern; die §§ 9 bis 16 des Artikel 10-Gesetzes gelten entsprechend.

*(7) [1]Eine über die vorstehenden Absätze hinausgehende inhaltliche Auswertung zu anderen Zwecken und die Weitergabe von personenbezogenen Daten an Dritte sind unzulässig. [2]Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. [3]Werden aufgrund der Maßnahmen der Absätze 1 bis 3 Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder Daten im Sinne des § 3 Absatz 9 des Bundesdatenschutzgesetzes erlangt, dürfen diese nicht verwendet werden. [4]Erkenntnisse aus dem Kernbereich privater Lebensgestaltung sind unverzüglich zu löschen. [5]Dies gilt auch in Zweifelsfällen. [6]Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. [7]Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. [8]Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt. [9]Werden im Rahmen der Absätze 4 oder 5 Inhalte oder Umstände der Kommunikation von in § 53 Absatz 1 Satz 1 der Strafprozessordnung genannten Personen übermittelt, auf die sich das Zeugnisverweigerungsrecht der genannten Personen erstreckt, ist die Verwertung dieser Daten zu Beweiszwecken in einem Strafver-

fahren nur insoweit zulässig, als Gegenstand dieses Strafverfahrens eine Straftat ist, die im Höchstmaß mit mindestens fünf Jahren Freiheitsstrafe bedroht ist.

(8) [1]Vor Aufnahme der Datenerhebung und –verwendung hat das Bundesamt ein Datenerhebungs- und –verwendungskonzept zu erstellen und für Kontrollen durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit bereitzuhalten. [2]Das Konzept hat dem besonderen Schutzbedürfnis der Regierungskommunikation Rechnung zu tragen. [3]Die für die automatisierte Auswertung verwendeten Kriterien sind zu dokumentieren. [4]Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit teilt das Ergebnis seiner Kontrollen nach § 24 des Bundesdatenschutzgesetzes auch dem Rat der IT-Beauftragten der Bundesregierung mit.

(9) Das Bundesamt unterrichtet den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über

1. die Anzahl der Vorgänge, in denen Daten nach Absatz 5 Satz 1, Absatz 5 Satz 2 Nummer 1 oder Absatz 6 Nummer 1 übermittelt wurden, aufgegliedert nach den einzelnen Übermittlungsbefugnissen,

2. die Anzahl der personenbezogenen Auswertungen nach Absatz 3 Satz 1, in denen der Verdacht widerlegt wurde,

3. die Anzahl der Fälle, in denen das Bundesamt nach Absatz 4 Satz 2 oder 3 von einer Benachrichtigung der Betroffenen abgesehen hat.

(10) Das Bundesamt unterrichtet kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Innenausschuss des Deutschen Bundestages über die Anwendung dieser Vorschrift.

Zusammengefasst hat die Ermächtigung den folgenden Inhalt:

§ 5 Abs. 1 S. 1 Nr. 1 BSIG ermächtigt das BSI, die näheren Umstände der elektronischen Kommunikation mit Bundesbehörden (§ 2 Abs. 8 BSIG) aufzuzeichnen und automatisiert auszuwerten. Namentlich wird zur Erfassung und Aufzeichnung von Verkehrsdaten über jede computergestützte Kommunikation mit Bundesbehörden (z.B. per E-Mail, Internettelefonie oder Instant Messaging) sowie von Daten über jede Nutzung öffentlicher Telemedien von Bundesorganen (§ 2 Abs. 8 S. 2 BSIG) ermächtigt.

§ 5 Abs. 1 S. 1 Nr. 2 BSIG ermächtigt das BSI, die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auszuwerten. Dies betrifft nicht nur Verkehrsdaten über die computergestützte Kommunikation mit Bundesbehörden (z.B. E-Mail) sowie Daten über die Nutzung öffentlicher Telemedien von Bundesorganen (§ 2

Abs. 8 S. 2 BSIG). Vielmehr dürfen auch der Inhalt computergestützter Kommunikation mit Bundesbehörden (z.B. E-Mail) sowie die von öffentlichen Telemedien von Bundesorganen abgerufenen und dorthin übertragenen Inhalte erfasst und ausgewertet werden.

§ 5 Abs. 2 BSIG ermächtigt das Bundesamt für Sicherheit in der Informationstechnik, die näheren Umstände der elektronischen Kommunikation mit Bundesbehörden (§ 2 Abs. 8 BSIG) drei Monate lang auf Vorrat zu speichern. Auf Vorrat gespeichert werden dürfen namentlich Verkehrsdaten über die computergestützte Kommunikation mit Bundesbehörden (z.B. E-Mail) sowie Daten über die Nutzung öffentlicher Telemedien von Bundesorganen (§ 2 Abs. 8 S. 2 BSIG).

§ 5 BSIG ermächtigt eine Sicherheitsbehörde der Bundesrepublik mithin zu einer generellen und undifferenzierten Aufzeichnung, Auswertung und Vorratsspeicherung von Informationen über jede elektronische Kommunikation und Information mittels Bundesnetzen. Jede E-Mail und jeder Abruf einer Internetseite über Bundesnetze ist betroffen. Dies gilt für die 500.000 Bundesbediensteten ebenso wie für die 80 Mio. Menschen in Deutschland, wenn sie mit Bundesbediensteten oder -behörden kommunizieren oder sich bei ihnen informieren. § 5 BSIG macht insoweit eine anonyme Kommunikation und Information ohne das Risiko einer Rückverfolgung und daran anschließender Nachteile unmöglich. Im Unterschied zu der umstrittenen, von der EU 2006 beschlossenen Richtlinie zur Vorratsdatenspeicherung erfolgt die in § 5 BSIG vorgesehene Datenspeicherung unmittelbar durch eine staatliche Stelle und umfasst sogar Daten, die Aufschluss über den Inhalt der Kommunikation geben (z.B. URLs abgerufener Internetseiten).

§ 5 BSIG ist am Tag nach seiner Verkündung in Kraft getreten.[1]

[1] Art. 3 des Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes.

B. Betroffenheit

Der Beschwerdeführer ist selbst und gegenwärtig betroffen, wenn er darlegt, dass er mit einiger Wahrscheinlichkeit durch die auf den angegriffenen Vorschriften beruhenden Maßnahmen in seinen Rechten berührt wird.[2] Dies ist bei uns der Fall. § 5 Abs. 1 und 2 BSIG ermächtigt das Bundesamt für Sicherheit in der Informationstechnik, Informationen über unser Kommunikations- und Informationsverhalten mit Behörden des Bundes aufzuzeichnen und auszuwerten. Wir kommunizieren regelmäßig per E-Mail mit Bundesbehörden (z.B. Ministerien, Bundesdatenschutzbeauftragter) und informieren uns über das WWW auf den Internetportalen von Bundesbehörden. Dies dient zum Teil auch der journalistischen Recherche für Artikel und Beiträge, wie sie der Beschwerdeführer zu 1 verfasst.

Der Beschwerdeführer zu 2 ist daneben in seiner Eigenschaft als Mitglied des Deutschen Bundestags betroffen: Der Bundestag betreibt seine Informationstechnik nicht in eigener Verantwortung. Vielmehr sind die Abgeordnetenbüros über den Informationsverbund Berlin-Bonn (IVBB) mit dem Internet verbunden. Für den IVBB zeichnet das Bundesinnenministerium verantwortlich. Dementsprechend ermächtigt § 5 BSIG das BSI, die E-Mail-Kontakte und das Internet-Surfverhalten des Beschwerdeführers zu 2 an seinem Arbeitsplatz zu erfassen, auszuwerten und drei Monate lang auf Vorrat zu speichern.

[2] Vgl. BVerfGE 115, 118 (137) m.w.N.

C. Subsidiarität

Unmittelbare Betroffenheit ist gegeben, wenn die angegriffenen Bestimmungen, ohne eines weiteren Vollzugsakts zu bedürfen, die Rechtsstellung des Beschwerdeführers verändern.[3] Unmittelbare Betroffenheit ist aber auch dann anzunehmen, wenn der Beschwerdeführer gegen einen denkbaren Vollzugsakt nicht oder nicht in zumutbarer Weise vorgehen kann.[4] Ein Vorgehen gegen den Vollzug ist insbesondere dann unzumutbar, wenn der Beschwerdeführer keine Kenntnis von dem Vollzug erlangt.[5]

So liegt es hier. § 5 BSIG stellt die Anwendung der Maßnahmen, zu denen er in Absatz 1 und 2 ermächtigt, in das Ermessen des Bundesamts für Informationstechnik. Wir haben keine Möglichkeit, zu erfahren, ob und inwieweit solche Maßnahmen ergriffen werden und wir davon betroffen sind. Eine Benachrichtigung ist hinsichtlich der in den Absätzen 1 und 2 vorgesehenen Aufzeichnung und Auswertung von Informationen, die mit der vorliegenden Beschwerde angegriffen wird, nicht vorgesehen. Nach dem Willen des Gesetzgebers soll eine Benachrichtigung nur „hinsichtlich der auch nichtautomatisiert verwendeten Daten“ erfolgen.[6] Die systematische Stellung von Absatz 4, der sich auch auf die Absätze 1 und 2 beziehen könnte, führt insoweit in die Irre. Nach dem Gesetzentwurf der Bundesregierung sollte die Benachrichtigung ursprünglich in § 5 Absatz 3 BSIG geregelt werden. Nur „zur besseren Lesbarkeit“ wurde der ursprüngliche Absatz 3 „in zwei Absätze aufgeteilt“.[7] Selbst wenn man den Absatz 4 auf die Absätze 1 und 2 anwenden wollte, wäre eine Benachrichtigung damit nicht sichergestellt. Die Absätze 1 und 2 ermächtigen zu einer flächendeckenden und permanenten Erhebung und Auswertung sämtlicher Telekommunikation mit Bundesbehörden. Es liegt auf der Hand, dass eine Benachrichtigung sämtlicher Betroffenen schlichtweg nicht möglich ist, weil sonst weite Teile der Bevölkerung ständig benachrichtigt werden müssten. Dementsprechend kann nach § 5 Abs. 4 S. 2 BSIG eine Benachrichtigung unterbleiben, „wenn die Person nur unerheblich betroffen wurde und anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat.“ Insgesamt gewährleistet die angefochtene Norm nicht zuverlässig, dass wir von Maßnahmen nach § 5 Abs. 1 und 2 BSIG benachrichtigt werden. Auch ein Auskunftsanspruch gegen das Bundesamt gewährleistet eine Kenntnisnahme nicht. Insbesondere ermöglicht § 34 BDSG, der einen Anspruch auf Auskunft über zur eigenen Person „gespeicherte Daten“ vorsieht, keine Kenntnisnahme. Hinsichtlich der Maßnahme nach § 5 Abs. 1 BSIG wird der Anspruch regelmäßig schon daran scheitern, dass im Gesetz eine „unverzügliche Löschung“ der ver-

[3] Vgl. BVerfGE 115, 118 (137) m.w.N.

[4] Vgl. BVerfGE 115, 118 (137) m.w.N.

[5] Vgl. BVerfGE 109, 279 (306).

[6] Rechtsausschuss des Bundestages; BT-Drs. 16/13259, 6.

[7] Rechtsausschuss des Bundestages; BT-Drs. 16/13259, 6.

arbeiteten Informationen vorgesehen ist. Hinsichtlich der Maßnahme nach § 5 Abs. 2 BSIG wird eine Auskunft daran scheitern, dass die Daten in pseudonymisierter (verschlüsselter[8]) Form aufbewahrt werden und das Gesetz eine Aufdeckung der Pseudonyme (Entschlüsselung) zum Zwecke einer Auskunfterteilung nicht vorsieht. Ohne die Aufdeckung kann das Bundesamt nicht feststellen, ob es Daten über uns speichert.

Im Übrigen muss der Rechtsweg gegen den Gesetzesvollzug nicht in Anspruch genommen werden, wenn er offensichtlich aussichtslos wäre,[9] etwa weil die Gesetzesnorm von den Fachgerichten nicht grundrechtskonform ausgelegt werden kann. Im vorliegenden Fall ist eine grundrechtskonforme Auslegung des § 5 Abs. 1 und 2 BSIG nicht möglich. Die Norm ermächtigt eindeutig zu einer anlasslosen, dauerhaften und allgemeinen Aufzeichnung und Auswertung von Informationen über jede informationstechnische Kommunikation mit einer Bundesbehörde. Ein Auslegungsspielraum besteht insoweit nicht. Es ist nicht Aufgabe der Fachgerichte, die Anwendung einer verfassungswidrigen Norm gerade auf das noch grundrechtskonforme Maß zu beschränken. Selbst das Bundesverfassungsgericht verwirft eine Norm insgesamt, wenn der Gesetzgeber sie bewusst unbestimmt gehalten hat,[10] wie es hier erfolgt ist. Nach alledem würde eine Anrufung der Fachgerichte, selbst wenn wir von den Maßnahmen nach § 5 BSIG Kenntnis erhielten, keinen wirksamen Rechtsschutz gegen die Verletzung unserer Grundrechte eröffnen.

D. Begründetheit der Beschwerde

Die Beschwerde ist begründet, weil § 5 Abs. 1 und 2 BSIG mit den Rechten auf Achtung der Privatsphäre (Art. 8 EMRK) und auf freie Meinungsäußerung (Art. 10 EMRK) nicht zu vereinbaren ist.

I. Verletzung des Art. 8 EMRK

1. Schutzbereich

Art. 8 EMRK gewährleistet das Recht auf informationelle Selbstbestimmung und auf Schutz personenbezogener Daten.[11] Dieses Recht umfasst die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen seine persönliche Lebenssachverhalte erhoben, gespeichert, verwendet oder weiter gegeben werden. Unter Bezugnahme auf die Datenschutzkonvention erkennt der Gerichtshof an, dass die Sammlung und Speicherung personenbezogener Daten einen Eingriff in das Privatleben des Einzelnen darstellt,[12] ebenso wie die Verwendung solcher Daten und die Verweige-

[8] Rechtsausschuss des Bundestages; BT-Drs. 16/13259, 6.

[9] BVerfGE 102, 197 (208).

[10] BVerfG, 1 BvR 2074/05 vom 11.3.2008, Absatz-Nr. 155.

[11] EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 66 ff.

[12] Frowein/Peukert-Frowein, Art. 8, Rn. 5 m.w.N.

rung ihrer Löschung.[13] Ein persönlicher Lebenssachverhalt liegt bereits dann vor, wenn die Verknüpfung des Lebenssachverhalts mit der zugehörigen Person möglich ist.[14]

2. Grundrechtseingriff

§ 5 Abs. 1 und 2 BSIG greift in unser Recht aus Art. 8 EMRK ein, indem das Bundesamt für Sicherheit in der Informationstechnik ermächtigt wird, Informationen über unsere informationstechnisch gestützte Kommunikation (z.B. E-Mail, Nutzung von Internetportalen) mit Bundesorganen und ihren Bediensteten, im Fall der Beschwerdeführers zu 2 auch mit beliebigen Dritten, aufzuzeichnen und auszuwerten.

Am deutlichsten wird dies bei privater Kommunikation von und mit Bundesbediensteten. Der Beschwerdeführer zu 1 kann private Nachrichten an Bundesbedienstete versenden. Dem Beschwerdeführer zu 2 ist seinerseits die private Nutzung des vom Bundestag bereitgestellten Internetzugangs erlaubt. Wenn nun das BSI ermächtigt wird, sich in solche private Kommunikationsbeziehungen einzuschalten und Informationen darüber zu sammeln und auszuwerten, greift der Gesetzgeber in das Recht auf Achtung der Privatsphäre ein. Denn dieses Recht gewährleistet, dass die Kommunizierenden selbst bestimmen können, wer von ihrer Kommunikation Kenntnis erlangt. § 5 BSIG schränkt dieses Selbstbestimmungsrecht ein. Der Gesetzgeber hat durch sein Zitat des Grundrechts auf Wahrung des Fernmeldegeheimnisses (Art. 10 GG) auch anerkannt, dass er in dieses Grundrecht eingreift (§ 11 BSIG). Eine Aussonderung privater Kommunikationsvorgänge ist dem BSI technisch nicht möglich.

Aber auch bei dienstlicher Telekommunikation zwischen dem Bürger und einem Bundesbediensteten oder Bundestagsabgeordneten greift die Einschaltung einer anderen Behörde (BSI) in die Vertraulichkeit des Fernmeldevorgangs ein. Kommuniziert der Bürger mit einer Behörde, so muss er sich grundsätzlich darauf verlassen können, dass sich nicht andere Stellen in den Kommunikationsvorgang einschalten („informationelle Gewaltenteilung“).[15] Auch die Bundesbehörde muss sich auf die Vertraulichkeit und Unbefangenheit der Telekommunikation mit dem Bürger verlassen können, um ihre Aufgaben ordnungsgemäß erfüllen zu können. Ein besonderes Interesse des Bürgers daran, dass eine Kenntnisnahme anderer Behörden unterbleibt, besteht etwa bei vertraulichen Meldungen des Verdachts von Subventionsbetrug, von Steuerhinterziehung, von Arzneimittelgesetzesverstößen, von Gesundheitsgefährdungen und ähnlichen Verstößen an die zuständige Aufsichtsbehörde, wenn der Informant bei Bekanntwerden seiner Identität Nachteile zu befürchten hat. Mitunter bieten Behörden dem Bürger sogar besondere Kanäle zur anony-

---

[13] EGMR, Leander-S (1987), Publications A116, Abs. 48; EGMR, Rotaru-ROM (2000), Decisions and Reports 2000-V, Abs. 46.

[14] Vgl. BVerfGE 65, 1 (42 und 49); BVerfGE 67, 100 (143); BVerfGE 77, 1 (46); BVerfGE 103, 21 (33); zu Art. 10: BVerfGE 100, 313 (366).

[15] Vgl. BVerfG, 1 BvR 962/87 vom 18.12.1987, NJW 1988, 959.

men Meldung etwa von Straftaten oder auch zur anonymen Beratung an. Unter Geltung des § 5 BSIG ist die Zusicherung absoluter Vertraulichkeit hinsichtlich elektronischer Kommunikation mit Bundesorganen nicht mehr möglich. Der Bund steht dem Bürger nicht als „Informationseinheit" gegenüber.[16] Werden die einer Behörde vorliegenden Informationen einer anderen Behörde zugänglich gemacht, so wird damit in die Rechte des Betroffenen eingegriffen.[17] Art. 8 EMRK schützt mithin auch die dienstliche Telekommunikation mit Bundesbehörden und –organen vor einer Einschaltung anderer Bundesbehörden in den Kommunikationsvorgang.

Dem Menschenrechtseingriff steht in diesen Fällen nicht etwa ein Einverständnis der Beteiligten entgegen. Weder hat der Kommunikationspartner des Bürgers dem BSI die Einschaltung „freiwillig ermöglicht"[18] (diese erfolgt hoheitlich aufgrund eines Gesetzes). Noch liegt ein bloßes Mithören am Endgerät vor. Während der Bürger mit einer Weiterleitung etwa von E-Mails durch den Empfänger rechnen muss und sich darauf einstellen kann, muss er nicht hinnehmen, dass eine Zentralbehörde ohne das Wissen seines Kommunikationspartners die Umstände seiner sämtlichen Telekommunikation mit Bundesbehörden aufzeichnet, rastert und den Inhalt seiner Telekommunikation durchsucht.

Dem Eingriff durch § 5 Abs. 1 BSIG steht auch nicht entgegen, dass die automatisierte Auswertung der erhobenen Daten grundsätzlich „unverzüglich" zu erfolgen hat und die Daten nach erfolgtem Abgleich sofort und spurenlos zu löschen sind. Nach allgemeinen Rechtsgrundsätzen schützt das Recht auf Datenschutz vor jeglicher Erhebung, Speicherung, Verwendung und Weitergabe persönlicher Lebenssachverhalte.[19] Die Erhebung von Protokoll- und Inhaltsdaten und sowie ihre automatisierte Auswertung stellt zweifellos eine Erhebung und Verwendung personenbeziehbarer Lebenssachverhalte dar. Schon in der Erfassung personenbezogener Daten liegt ein Grundrechtseingriff, weil die Datenerhebung eine nachfolgenden Datenverarbeitung ermöglicht. An einem Eingriff fehlt es allenfalls, soweit Daten ungezielt und allein technikbedingt miterfasst, unmittelbar nach der Erfassung aber technisch wieder spurenlos, anonym und ohne die Möglichkeit, einen Personenbezug herzustellen, ausgesondert werden.[20] In einem solchen Fall des bloßen „Durchflusses" kann der Tatbestand der Datenerhebung verneint werden.

Im Fall des § 5 Abs. 1 BSIG werden die erhobenen Daten indes nicht ungezielt und allein technikbedingt miterfasst, um unmittelbar nach der Erfassung wieder ausgesondert zu

---

[16] Heußner, RDV 1988, 9; Simitis, BDSG, Einl., Rn. 36 m.w.N.

[17] BVerwG, NJW 2005, 2330.

[18] BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. 291.

[19] Art. 2 Buchst. c DSK; Art. 2 Buchst. b RiL 95/46/EG; Art. 8 Abs. 2 S. 1 Grundrechtscharta; BVerfGE 65, 1 (46).

[20] Vgl. BVerfGE 100, 313 (366); BVerfGE 107, 299 (328); BVerfGE 115, 320 (343); BVerfG, NJW 2008, 1505 (1506 f.).

werden. Ziel der Erfassung ist es vielmehr, die Daten für die staatlichen Datenverarbeitungssysteme verfügbar zu machen, um sie „auswerten“ zu können. Die Löschung der Daten erfolgt nicht unmittelbar nach ihrer Erfassung, sondern erst nach ihrer Auswertung. Eine spätere Löschung kann die voran gegangenen Grundrechtseingriffe nicht ungeschehen machen.

Nach der Gesetzesbegründung sollen Logfiles von Servern, Firewalls usw. erhoben und automatisiert ausgewertet werden.[21] Das bedeutet, dass nach § 5 Abs. 1 S. 1 Nr. 1 BSIG beispielsweise jede E-Mail von und an Bundesangehörige, jeder Zugriff auf das Internetportal einer Bundesbehörde und jeder Klick eines Bundesangehörigen im Internet aufgezeichnet und protokolliert werden soll. Der damalige BSI-Präsident führte aus, auf der Grundlage des § 5 Abs. 1 BSIG sollten „Detektionstools“ eingesetzt werden.[22] Damit dürften sog. „Einbruchserkennungsvorrichtungen“ („Intrusion Detection Systems“) gemeint sein. Es handelt sich dabei um eine Art Alarmanlage, die verdächtige oder außergewöhnliche Kommunikationsmuster automatisiert feststellen und melden soll. Aus einer einzelnen Verbindung kann man Kommunikationsmuster nicht feststellen. Um Kommunikationsmuster feststellen zu können, ist eine Speicherung und Vorhaltung der Kommunikationsdaten für eine gewisse Dauer erforderlich, um dann die Gesamtheit der Verbindungen in dem maßgeblichen Zeitraum analysieren zu können. Die erforderliche Speicherdauer ist gesetzlich nicht definiert. Während der Dauer der Datenspeicherung können die Informationen über die Telekommunikation kopiert, ausgelesen, zur Kenntnis genommen und zu verschiedensten Zwecken verwendet werden, was eine konkrete Gefährdung der Vertraulichkeit begründet. Das Gebot der „unverzüglichen Auswertung“ gewährleistet nicht, dass die erhobenen Daten unmittelbar nach der Erfassung wieder gelöscht werden. Werden erfasste Daten aber im Speicher festgehalten und können sie gegebenenfalls Grundlage weiterer Maßnahmen werden, so liegt in jedem Fall ein Grundrechtseingriff vor.[23]

Die in § 5 Abs. 2 BSIG vorgesehene Pseudonymisierung steht dem Grundrechtseingriff nicht entgegen. Ein Eingriff in Art. 8 EMRK liegt bereits dann vor, wenn die Verknüpfung des Lebenssachverhalts mit der zugehörigen Person möglich ist.[24] Dies ist auch nach einer Pseudonymisierung der Internetnutzungs- und -verkehrsdaten der Fall. Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen (§ 3 Abs. 6a BDSG). Da das BSI über die Zuordnungsfunktion verfügt, können Namen und Identifikationsmerkmale anhand des Pseudonyms jederzeit wieder ermittelt werden (§ 5 Abs. 2 S. 5 BSIG). Im Übrigen sind Internetnutzungs- und -verkehrsdaten regelmäßig bereits pseudonymisiert. IP-Adressen und E-Mail-Adressen stellen meist Pseudonyme dar.

---

[21] Bundesregierung, BT-Drs. 16/11967, 14.

[22] Helmbrecht, INA-Drs. 16(4)570 A, 6.

[23] Vgl. BVerfGE 120, 378 (399).

[24] Vgl. BVerfGE 100, 313 (366).

Die Identität des Nutzers einer IP-Adresse oder E-Mail-Adresse kann das BSI „zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung“ über § 113 TKG in Erfahrung bringen. Mitunter sind Internetnutzungs- und -verkehrsdaten allerdings auch unmittelbar personenbezogen, etwa wenn neben einer E-Mail-Adresse auch der Klarname des Absenders oder Empfängers angegeben ist oder wenn die E-Mail-Adresse den Klarnamen enthält.

Art. 8 EMRK ist auch nach seinem Schutzzweck einschlägig. Das Recht auf Achtung des Privatlebens soll dem Individuum eine Sphäre sichern, in der es die Entwicklung und Erfüllung seiner Persönlichkeit anstreben kann. Zu diesem Zweck muss es unter anderem auch die Möglichkeit haben, Beziehungen zu anderen Menschen aufzunehmen.[25] Im Fall der Erhebung von Protokoll- und Inhaltsdaten der Telekommunikation durch das BSI ist für den Betroffenen nicht vorhersehbar, ob und inwieweit seine Daten weiter verarbeitet werden. Er kann nicht wissen, nach welchen Kriterien die Auswertung der Daten erfolgt, ob seine Daten nach der Auswertung wieder gelöscht werden oder ob nachteilige Meldungen oder Registrierungen erfolgen, ob die Daten vielleicht sogar missbraucht, verkauft oder verloren werden. Schon von diesen Risiken möglicher Nachteile geht eine abschreckende Wirkung auf die unbefangene elektronische Kommunikation zwischen Menschen aus. Wo zwischenmenschliche Kommunikation wegen § 5 BSIG verändert verläuft oder unterbleibt, kann sich dies nachteilig auf die zwischenmenschliche Beziehung auswirken.

3. Mangelnde Rechtfertigung

Gerechtfertigt ist dieser Grundrechtseingriff nur, wenn er gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer (Art. 8 EMRK).

Dies ist bei § 5 BSIG nicht der Fall. Die Vorschrift ist in Tragweite wie Auswirkungen nicht hinreichend vorhersehbar und schränkt das Recht auf Achtung der Privatsphäre unverhältnismäßig weit ein.

a) Mangelnde Vorhersehbarkeit und Präzision

Staatliche Stellen dürfen in die Privatsphäre von Menschen nur eingreifen, soweit der Eingriff gesetzlich vorgesehen ist (Art. 8 Abs. 2 EMRK). Aus dem Erfordernis einer gesetzlichen Grundlage in Verbindung mit dem in der Präambel der EMRK erwähnten Rechtsstaatsprinzip leitet der Gerichtshof ab, dass das eingreifende innerstaatliche Recht hinreichend bestimmt und für den Bürger zugänglich sein muss.[26] Dem Einzelnen muss es mög-

---

[25] KOM, Brüggemann mid Scheuten ./. D, DR 10,100,115 = EuGRZ 1978,199.

[26] EGMR, Sunday Times-GB (1979), EuGRZ 1979, 386 (387), Abs. 49; EGMR, Silver u.a.-GB (1983), EuGRZ 1984, 147 (150), Abs. 87 und 88; EGMR, Lambert-F (1998), Decisions and Reports 1998-V, Abs. 23.

lich sein, sein Verhalten den Vorschriften entsprechend einzurichten, was ein – gemessen an der Schwere des Eingriffs[27] – hinreichendes Maß an Vorhersehbarkeit voraussetzt.[28]

Räumt das nationale Recht der Exekutive ein Ermessen bei der Anordnung von Maßnahmen ein, dann verlangt das Bestimmtheitserfordernis – auch und gerade bei geheimen Maßnahmen –, dass der zulässige Zweck der Maßnahme, die Reichweite und Grenzen des Ermessens und die Kriterien, nach denen es auszuüben ist, hinreichend erkennbar sind, insbesondere, dass vorhersehbar ist, unter welchen Umständen und Bedingungen Eingriffe zulässig sind[29]. Die Anforderungen an die Vorhersehbarkeit im Einzelnen hängen von der Eingriffstiefe der jeweiligen Maßnahme ab, so dass schwerwiegende Eingriffe eine besonders präzise gesetzliche Regelung erforderlich machen[30].

Für den Fall einer Informationssammlung und -speicherung durch einen Geheimdienst hat der Gerichtshof entschieden, dass das nationale Recht detailliert festlegen muss, welche Arten von Informationen gespeichert werden dürfen, gegenüber welchen Personengruppen Überwachungsmaßnahmen ergriffen werden dürfen, unter welchen Umständen Informationen gesammelt werden dürfen, welches Verfahren dabei einzuhalten ist, nach welcher Zeitdauer erlangte Informationen zu löschen sind, welche Personen auf den Datenbestand zugreifen dürfen, die Art und Weise der Speicherung, das Verfahren des Informationsabrufs sowie die zulässigen Verwendungszwecke für die abgerufenen Informationen[31].

Hieran gemessen, wird insbesondere § 5 Abs. 1 S. 2 BSIG dem Erfordernis einer vorhersehbaren und präzisen Regelung nicht gerecht.

Nach § 5 Abs. 1 S. 2 BSIG soll die in Satz 1 vorgesehene automatisierte Auswertung des Kommunikationsverkehrs „unverzüglich“, also ohne schuldhaftes Zögern (§ 121 BGB) erfolgen. Nach dem Willen des Gesetzgebers soll es also zulässig sein, die Auswertung erst mit Verzögerung vorzunehmen und die Daten bis zu diesem Zeitpunkt offenbar – im Fall des § 5 Abs. 1 S. 1 Nr. 2 BSIG unausgesprochen – zu speichern, solange die Verzögerung nicht schuldhaft erfolgt, also unter Beachtung der „im Verkehr erforderlichen Sorgfalt“ (§ 276 BGB). Im Rahmen des § 121 BGB wird von der Rechtsprechung als „unverzüglich“ noch ein Handeln innerhalb von zwei Wochen angesehen.[32] Der Bundesdatenschutzbe-

---

27 EGMR, Kruslin-F (1990), Publications A176-A, Abs. 33.

28 EGMR, Silver u.a.-GB (1983), EuGRZ 1984, 147 (150), Abs. 88; EGMR, Malone-GB (1984), EuGRZ 1985, 17 (20), Abs. 66; EGMR, Amann-CH (2000), Decisions and Reports 2000-II, Abs. 56.

29 EGMR, Silver u.a.-GB (1983), EuGRZ 1984, 147 (150), Abs. 88; EGMR, Malone-GB (1984), EuGRZ 1985, 17 (20 f.), Abs. 67 und 68; EGMR, Leander-S (1987), Publications A116, Abs. 51; EGMR, Valenzuela Contreras-ES (1998), Decisions and Reports 1998-V, Abs. 60; EGMR, Khan-GB (2000), Decisions and Reports 2000-V, Abs. 26.

30 EGMR, Kopp-CH (1998), StV 1998, 683 (684), Abs. 72.

31 EGMR, Rotaru-ROM (2000), Decisions and Reports 2000-V, Abs. 57.

32 BAGE 32, 237.

auftragte hat es als „unverzügliche“ Löschung im Sinne des § 96 Abs. 2 TKG angesehen, wenn Verkehrsdaten erst nach siebentägiger Aufbewahrung gelöscht werden.[33]

Die Bedeutung der Frage nach der zulässigen Speicherdauer ist sehr groß, weil § 5 Abs. 1 S. 1 BSIG zu einer Speicherung und Auswertung der gesamten Internetkommunikation mit und von Bundesbehörden und ihren Mitarbeitern ermächtigt. Bis zur Löschung der Daten besteht die Gefahr ihrer legalen oder illegalen Nutzung durch Mitarbeiter des BSI. Außerdem besteht die Gefahr unbefugter Zugriffe und das Risiko einer versehentlichen oder fahrlässigen Weiterleitung oder Veröffentlichung (Datenpannen).

§ 5 Abs. 1 S. 1 BSIG ermächtigt zu einer automatisierten Auswertung. Ein Computer kann nicht „zögern“ im Sinne von „unverzüglich“, sondern nur Befehle abarbeiten. Der Begriff „unverzüglich“ passt auf eine automatisierte Verarbeitung nicht. Automatisierte Prozesse laufen entweder „sofort“ oder in programmierten Zeitabständen ab. Der Gesetzgeber hat nicht festgelegt, ob er zu einer automatisierten Auswertung in Echtzeit oder zu einer automatisierten Auswertung in bestimmten, festzulegenden Zeitabständen ermächtigen will.

Dies genügt dem Gebot der Vorhersehbarkeit in Anbetracht der Eingriffsintensität des § 5 BSIG nicht. Vor dem Hintergrund der hohen Eingriffsintensität der Ermächtigung zu flächendeckenden und pauschalen Eingriffen in die Privatsphäre hätte der Gesetzgeber festlegen müssen, ob und wie lange die auszuwertenden Daten gespeichert werden dürfen und wann ihre Löschung erfolgen muss. Der Begriff „unverzüglich“ ist zu unbestimmt.

Hinreichend bestimmt wäre etwa die Vorgabe „sofort“ oder „so bald wie nach dem Stand der Technik möglich, spätestens aber nach einer Stunde“ gewesen. Auf eine solch präzise Regelung der Frage hat der Gesetzgeber indes verzichtet, obwohl er auf dieses Erfordernis schon im Gesetzgebungsverfahren hingewiesen worden war. Der Begriff „unverzüglich“ ist im Zusammenhang mit der Regelung des § 5 BSIG nach alledem zu unbestimmt.

b) Verletzung des Verhältnismäßigkeitsgebots

Nach Art. 8 Abs. 2 EMRK müssen Eingriffe in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohl des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer erforderlich sein. In einer demokratischen Gesellschaft erforderlich ist eine Maßnahme nur, wenn ein in Anbetracht des Stellenwerts des garantierten Freiheitsrechts hinreichend dringendes soziales Bedürfnis nach ihr besteht, sie einen legitimen Zweck verfolgt und ihre Belastungsintensität nicht außer Verhältnis zu dem Gewicht des damit verfolgten Zwecks

[33] Schaar, Antwort vom 16.03.2007, http://www.vorratsdatenspeicherung.de/content/view/89/79/.

steht.[34] Der Gerichtshof hat entschieden, dass das Interesse des Staates gegenüber den Interessen des Einzelnen an der Achtung seiner Privatsphäre abgewogen werden muss.[35] Eingriffe sind zwar nicht auf das unerlässliche Maß beschränkt, aber ein bloßes Nützlich- oder Wünschenswertsein genügt zu ihrer Rechtfertigung nicht.[36] Die nachteiligen Auswirkungen des Eingriffs dürfen nicht schwerer wiegen als die zur Rechtfertigung des Eingriffs angeführten Gründe.[37]

§ 5 BSIG genügt diesen Anforderungen nicht. Das grundrechtlich geschützte Interesse unbescholtener Bürger daran, Informationen über Bundesnetze ohne Furcht vor Aufdekkung des Informationsverhaltens abrufen und darüber kommunizieren zu können, überwiegt das Interesse des Bundes daran, seine Informationstechnik in seltenen Ausnahmefällen besser schützen zu wollen.

aa) Legitimes Ziel

Das mit § 5 BSIG verfolgte gesetzgeberische Anliegen, Störungen und Fehlern der Kommunikationstechnik des Bundes, Angriffen auf die Informationstechnik des Bundes sowie Schadprogrammen zu begegnen, ist im Ausgangspunkt legitim. Die Funktionsfähigkeit der öffentlichen Informationstechnik ist für Bürger und Staat von erheblicher und zunehmender Bedeutung, gerade im Bereich „kritischer Infrastrukturen“. Auch die Vertraulichkeit der öffentlichen Informationstechnik und der darauf gespeicherten personenbezogenen Daten ist ein wichtiges Gut. Legitim ist zudem die Verfolgung von Straftaten, die Abwehr von Gefahren und der Staatsschutz (§ 5 Abs. 6 BSIG).

bb) Verhältnismäßigkeit

Das zur Erreichung dieser Ziele gewählte Mittel des § 5 BSIG greift aber unverhältnismäßig tief in die Rechte von Personen ein, die zu dem Eingriff keinen Anlass gegeben haben.

(1) Gewicht des Eingriffsinteresses

Es besteht – wie bereits erwähnt – ein berechtigtes Interesse an der Gewährleistung der Funktionsfähigkeit und Vertraulichkeit der Informationstechnik des Bundes. Allerdings ist nicht zu verkennen, dass das Gewicht dieses Interesses weit hinter dem Interesse etwa am Schutz von Leib, Leben oder Freiheit von Menschen zurückbleibt. Dementsprechend werden Angriffe auf die Sicherheit von Informationstechnik nach dem deutschen Strafgesetzbuch in der Regel mit Freiheitsstrafe von nur bis zu zwei oder drei Jahren oder mit

---

[34] EGMR, Sunday Times-GB (1979), EuGRZ 1979, 386 (389), Abs. 62; EGMR, Silver u.a.-GB (1983), EuGRZ 1984, 147 (152), Abs. 97; EGMR, Foxley-GB (2000), hudoc.echr.coe.int/Hudoc1doc2/HEJUD/200107/foxley%20-%2033274jv.chb3%20200 62000e.doc, Abs. 43.

[35] EGMR, Sunday Times-GB (1979), EuGRZ 1979, 386 (390 und 391), Abs. 65 und 67; EGMR, Leander-S (1987), Publications A116, Abs. 59.

[36] EGMR, Silver u.a.-GB (1983), EuGRZ 1984, 147 (151), Abs. 97.

[37] EGMR, Dudgeon-GB (1981), Publications A45, Abs. 60.

Geldstrafe bestraft (§§ 202a, 202b, 303a, 303b StGB). Diese Strafrahmen gehören zu den geringsten, die das Strafgesetzbuch kennt.

Die Bestimmung des Gewichts der Rechtsgüter, deren Schutz der Grundrechtseingriff dient, darf überdies nicht abstrakt und unabhängig von dem Maß an Eignung des jeweiligen Grundrechtseingriffs zum Schutz dieser Rechtsgüter erfolgen. Vielmehr erfordert eine konkrete Abwägung, den einzelnen Grundrechtseingriff und dessen Maß an Eignung zur Erreichung der verfolgten Ziele zu bestimmen. Eine kaum taugliche Maßnahme vermag nur leichte Grundrechtseingriffe zu rechtfertigen, während eine zur Abwehr schwerer Gefahren unabdingbare Maßnahme tiefere Grundrechtseingriffe rechtfertigen kann. Die Tauglichkeit der einzelnen in § 5 BSIG vorgesehenen Maßnahmen wird noch im Einzelnen zu untersuchen sein.

Ein besonderes Interesse an § 5 BSIG lässt sich nicht mit der Begründung annehmen, hinsichtlich Computerdaten gebe es mangels öffentlicher Wahrnehmbarkeit kein gesellschaftliches Gedächtnis, das es wie in anderen Bereichen erlaubte, zurückliegende Vorgänge auf der Grundlage zufälliger Erinnerung zu rekonstruieren. Denn auch außerhalb der Kommunikationsnetze gibt es kein gesellschaftliches Gedächtnis, das es erlaubte, zurückliegende Vorgänge systematisch zu rekonstruieren. Soweit § 5 BSIG zur Erfassung und Auswertung von Internet-Nutzungsdaten ermächtigt, ist die Nutzung der Telemedien von Bundesorganen mit der Abholung ausliegender Formulare und Informationsschriften aus einer Behörde vergleichbar. Angriffe auf Internetserver können mit Beschädigungen öffentlicher Einrichtungen verglichen werden. Dass jemand – etwa der Pförtner einer Filiale der Arbeitsagentur – frühere Besucher der Behörde erinnerte oder gar identifizieren könnte, ist unwahrscheinlich. Erst recht gilt dies für Angriffe von außen. Soweit § 5 BSIG zur Erfassung und Auswertung von Telekommunikationsinhalten und -umständen ermächtigt, ist die E-Mail-Kommunikation mit Behördenmitarbeitern dem postalischen Schriftverkehr mit Behörden vergleichbar. Schadprogrammen sind vielleicht Giftstoffe, Briefbomben und Wanzen vergleichbar, die per Post versandt werden können. Es ist nun offensichtlich, dass es im Bereich des postalischen Massenschriftverkehrs mit Behörden niemanden gibt, der zurückliegende Briefsendungen oder gar deren Absender erinnerte – mit Ausnahme des Empfängers, dem aber auch im Fall einer E-Mail alle Inhalte und Verkehrsdaten vorliegen. § 5 BSIG begründet danach ein Maß an Überwachung und Nachvollziehbarkeit menschlichen Kommunikations- und Informationsverhaltens wie es in vergleichbaren Situationen sonst nicht existiert.

(2) Gewicht des beeinträchtigten Freiheitsinteresses

(a) Maßgebliche Kriterien

Das Gewicht eines Grundrechtseingriffs bemisst sich danach, unter welchen Voraussetzungen Eingriffe zulässig sind, welche und wie viele Grundrechtsträger von ihnen betroffen

sind und wie intensiv die Grundrechtsträger beeinträchtigt werden.[38] Zu berücksichtigen ist auch, ob und in welcher Zahl Personen mitbetroffen werden, die für den Eingriff keinen Anlass gegeben haben.[39] Die Eingriffsintensität hängt bei Informationseingriffen unter anderem von Art, Umfang und denkbarer Verwendungen der erhobenen Daten sowie von der Gefahr ihres Missbrauchs ab.[40] Bei der Feststellung der Möglichkeiten zur Verwendung erlangter Daten ist zu berücksichtigen, ob die Betroffenen anonym bleiben und welche Nachteile ihnen aufgrund der Maßnahmen drohen oder von ihnen nicht ohne Grund befürchtet werden.[41] Bei der Gewichtung möglicher Nachteile ist die Nutzbarkeit und Verwendungsmöglichkeit der Daten maßgeblich, und zwar unter besonderer Berücksichtigung der Möglichkeit, dass die Daten mit anderen Daten kombiniert und dadurch weitergehende Kenntnisse gewonnen werden können.[42]

Für die Beurteilung der Verhältnismäßigkeit sind primär die rechtlich zulässigen Verwendungsmöglichkeiten maßgeblich. Einzubeziehen sind aber auch die sonstigen, tatsächlich und technisch vorhandenen Verwendungsmöglichkeiten. Dies ist einerseits vor dem Hintergrund erforderlich, dass sich die rechtlichen Grenzen des staatlichen Zugriffs vergleichsweise leicht erweitern lassen, nachdem die grundsätzliche Zugriffsmöglichkeit erst einmal eingeführt und die erforderliche Überwachungsstruktur aufgebaut worden ist. Nicht nur die wiederholt vorgenommene Ausweitung des Straftatenkatalogs in § 100a StPO zeigt, dass eine solche Entwicklung auch in anderen Bereichen möglich und nicht unwahrscheinlich ist. Zum anderen ist auch an die Gefahr eines rechtswidrigen Missbrauchs zu denken, gerade dort, wo dieser nur schwer zu bemerken ist. Zwar ist, was den Staat selbst angeht, die bloß abstrakte Möglichkeit eines Missbrauches, das heißt unbegründete Befürchtungen dahin gehend, nicht zu berücksichtigen, weil grundsätzlich davon auszugehen ist, dass eine Norm „in einer freiheitlich-rechtsstaatlichen Demokratie korrekt und fair angewendet wird“.[43] Eine reale Missbrauchsgefahr ist im Rahmen der Abwägung demgegenüber durchaus zu berücksichtigen.[44] Die Menschenrechte schützen den Einzelnen nämlich auch „vor fehlerhafter, missbräuchlicher oder exzessiver Verwertung von Kommunikationsdaten durch [...] staatliche Stellen“.[45] Die „in der Gesprächsbeobachtung liegende Gefahr einer Menschenrechtsverletzung der [...] Gesprächsteilnehmer wie auch die Gefahr der Sammlung, Verwertung und Weitergabe der Informationen zu anderen Zwecken“ als

[38] Vgl. BVerfGE 109, 279 (353).

[39] Vgl. BVerfGE 109, 279 (353).

[40] Vgl. BVerfGE 65, 1 (46).

[41] Vgl. BVerfGE 100, 313 (376).

[42] Vgl. BVerfGE 65, 1 (45).

[43] Vgl. BVerfGE 30, 1 (27).

[44] Vgl. BVerfGE 65, 1 (45 f.).

[45] Vgl. BVerfGE 85, 386 (397).

den gesetzlich vorgesehenen darf daher nicht aus den Augen verloren werden.[46] Wenn die EMRK das unbefangene Gebrauchmachen von Freiheiten in einer Demokratie schützen soll, dann darf außerdem nicht unberücksichtigt bleiben, dass sich Bürger bei ihren Entscheidungen weniger durch die Gesetzesformulierungen leiten lassen als vielmehr durch Eindrücke, Emotionen und Befürchtungen. Dementsprechend kommt es im Rahmen der Abwägung auch nicht nur darauf an, welche Nachteile den Betroffenen konkret aufgrund der Überwachungsmaßnahmen drohen. Ebenso zu berücksichtigen sind entferntere Risiken, deren Eintritt von den Bürgern nicht ohne Grund befürchtet wird.[47] Das Gewicht drohender oder befürchteter Nachteile in der Abwägung hängt dabei unter anderem von der Wahrscheinlichkeit des Eintritts eines Schadens und von dessen potenziellem Ausmaß ab.

Auf die Frage, inwieweit von einer gesetzlichen Eingriffsermächtigung tatsächlich Gebrauch gemacht wird, kann es bei der Beurteilung der Eingriffsintensität richtigerweise nicht ankommen,[48] weil eine Vollzugspraxis jederzeit geändert werden kann[49] und weil der Gesetzgeber verpflichtet ist, die wesentlichen Eingriffsgrenzen selbst zu regeln. Eine Verwaltungspraxis ist für die Betroffenen regelmäßig nicht vorhersehbar und daher bei der Verhältnismäßigkeitsprüfung ohne Bedeutung.[50] Zwar entspricht es der Eigenart von Rechtsnormen, dass diese bis zu einem gewissen Grad allgemein gehalten sind. Nichtsdestotrotz muss der Gesetzgeber eine Norm jedenfalls dann eingrenzen, wenn sie ansonsten in abstrakt umschreibbaren Fallgruppen zu Eingriffen ermächtigen würde, in denen der Verhältnismäßigkeitsgrundsatz durchweg verletzt würde.[51]

(b) Tragweite des § 5 BSIG

Die Anwendung dieser Grundsätze auf § 5 BSIG ergibt: Zur Aufzeichnung des Informations- und Kommunikationsverhaltens wird frei von jeder Voraussetzung und Eingriffsschwelle dauerhaft und allgemein – mithin global und pauschal[52] – ermächtigt. Es erfolgt eine flächendeckende Massenerfassung[53] des computergestützten Kommunikations- und Informationsverhaltens im Verhältnis unbescholtener und ungefährlicher Bürger zum Bund. Beeinträchtigt sind sämtliche Grundrechtsträger, die mit dem Bund kommunizieren oder sich auf seinen Internetportalen informieren, und damit potenziell alle Bürger. Eine größere Zahl betroffener Grundrechtsträger infolge einer Grundrechtsbeschränkung ist kaum denkbar. Es gibt praktisch keine unbeeinträchtigte computergestützte Kommunikation mit Be-

[46] Vgl. BVerfGE 85, 386 (400).

[47] Vgl. BVerfGE 100, 313 (376).

[48] MVVerfG, LKV 2000, 149 (154); AK-GG-Bizer, Art. 10, Rn. 86; a.A. wohl BVerfGE 100, 313 (376 ff.).

[49] Vgl. BVerfGE 100, 313 (380).

[50] EGMR, Khan-GB (2000), Decisions and Reports 2000-V, Abs. 27.

[51] Vgl. BVerfGE 100, 313 (384 f.).

[52] Vgl. BVerfGE 313, 100 (376 und 383).

[53] Vgl. dazu BVerfGE 313, 100 (377).

hörden, Mitarbeitern und Abgeordneten des Bundes und keine unbeeinträchtigte Nutzung seiner Internetportale mehr.

Betroffen ist der dem Bund gegenüber tretende Bürger selbst dann, wenn er keinerlei Anlass zur Aufzeichnung seiner Kommunikation oder seines Informationsabrufs gegeben hat. Fast durchgängig betrifft der Eingriff Personen und Computersysteme, von denen keine Störung und kein Angriff auf die Informationstechnik des Bundes ausgeht. Zu schätzungsweise über 99,9% sind daher unschuldige und ungefährliche Bürger betroffen und ist eine Aufzeichnung deren Kommunikations- und Informationsverhaltens von vornherein überflüssig. Die Ermächtigung setzt keine Verantwortlichkeit oder wenigstens Gefahrennähe der Betroffenen voraus. Der bloße informationstechnische Kontakt oder Informationsabruf soll zur Aufzeichnung führen.

Die Aufzeichnungen sind auch nicht sofort, sondern nur „unverzüglich“ auszuwerten und zu löschen, was eine Vorhaltung auf unbestimmte Dauer impliziert. § 5 Abs. 2 BSIG sieht sogar eine Aufbewahrung „auf Vorrat“ für bis zu drei Monate vor.

Ein weiteres Kriterium für die Bestimmung der Eingriffsintensität ist die Identifizierbarkeit der Betroffenen. Diese ist über Informationen, die bei dem vom Bürger genutzten Anbieter des Internetzugangs oder des Kommunikationsdienstes (z.B. E-Mail) vorhanden sind, in der Regel gegeben. Über § 113 TKG kann unter anderem das BSI von Diensteanbietern eine Identifizierung elektronischer Kennungen (z.B. IP-Adressen, E-Mail-Adressen) zur Verfolgung von Straftaten oder Ordnungswidrigkeiten oder zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung verlangen. § 5 BSIG ermächtigt nicht nur zur Erfassung anonymer Daten. Zwar gibt es vielfältige Möglichkeiten einer anonymen Internetnutzung, welche die Herstellung eines Personenbezugs verhindern können und deren Einsatz sich für Kriminelle lohnen mag. Dem Normalbürger ist die ausschließliche Nutzung anonymer Formen von Telekommunikation zur Kommunikation mit dem Bund aber wegen des damit verbundenen Aufwands auf Dauer nicht möglich oder jedenfalls unzumutbar. Die Möglichkeiten anonymer Telekommunikation bewirken daher nur eine geringfügige Minderung der Eingriffsintensität.

Nach § 5 Abs. 4 BSIG erfolgt die etwaige Erfassung und Auswertung der Daten bis zum Erkennen eines etwaigen Schadprogramms oder einer anderen Gefahr heimlich. Dies führt zu einer weiteren Erhöhung des Gewichts der gesetzgeberischen Freiheitsbeeinträchtigung. Dem Betroffenen wird durch die Heimlichkeit des Eingriffs vorheriger Rechtsschutz faktisch verwehrt und nachträglicher Rechtsschutz kann zumindest erschwert werden.[54] Dem Bürger wird nicht mitgeteilt, ob und inwieweit das Bundesamt von seinen Befugnissen nach § 5 Abs. 1 BSIG Gebrauch macht.

[54] Bundesrat, BT-Drs. 16/12225, 3.

Die verdachtslose Totalregistrierung des Kommunikationsverhaltens zwischen Bürger und Staat oder dessen Mitarbeitern ist ein tiefgreifender Grundrechtseingriff. Während die (verfassungswidrige) Regelung zur Vorratsspeicherung von Verkehrsdaten dies noch im Einklang mit zwingendem Verfassungsrecht[55] ausschloss (§ 113a Abs. 8 TKG), ermächtigt § 5 BSIG nun erstmals auch zur Protokollierung des Abrufs von Inhalten des Bundes im Internet. Anhand dieser Totalerfassung des Informationsverhaltens lässt sich jederzeit rekonstruieren, wer wann welche Internetseite einer Bundesbehörde betrachtet oder Veröffentlichungen darauf vorgenommen hat (z.B. Kommentare, Gästebucheinträge), wonach er solche Internetseiten durchsucht (Suchworte als Bestandteil der URL) und welche externen Internetseiten er vor und nach dem Zugriff betrachtet hat („Referrer" einschließlich der in eine Suchmaschine eingegebenen Suchbegriffe, Links).

§ 5 BSIG legt nicht fest, aus welchem Anlass das BSI Informations- und Kommunikationsprotokolle erstellen darf. Er ermächtigt das BSI, das gesamte Surf- und Kommunikationsverhalten jedes mit einer Bundesbehörde in Kontakt tretenden Bürgers ohne Anlass aufzuzeichnen. Es ist nämlich nie auszuschließen, dass diese Daten einmal zum „Erkennen" denkbarer zukünftiger „Störungen" oder „Angriffe" erforderlich sein könnten. Damit wird das BSI zur Speicherung jeder Eingabe und jedes Mausklicks beim Lesen, Schreiben und Diskutieren in öffentlichen Internetangeboten des Bundes ermächtigt, zur Vorratsdatenspeicherung im Internet. Die Vorschrift macht insoweit den vom Bundesverfassungsgericht hervor gehobenen[56] Grundsatz der §§ 13, 15 TMG, demzufolge Nutzungsdaten nicht über die Dauer des Nutzungsvorgangs hinaus aufbewahrt werden dürfen, bedeutungslos. § 5 BSIG ist nicht auf eine Erfassung „im Einzelfall" bei Vorliegen einer konkreten Störung beschränkt, sondern erlaubt eine anlasslose, globale und pauschale Aufzeichnung unserer Internetnutzung über Bundesnetze.

(c) Insbesondere: Aussagekraft von Verkehrs- und Nutzungsdaten

Nach der Rechtsprechung des Bundesverfassungsgerichts bemisst sich die Intensität des Grundrechtseingriffs insbesondere nach der Aussagekraft der Daten, die erhoben werden können, wobei ihre Nutzbarkeit und ihre Verwendungsmöglichkeiten zu berücksichtigen sind.

Die Individualkommunikation mit Bundesorganen kann in hohem Maße Aufschluss auf das Privatleben von Personen, aber auch über Geschäftsgeheimnisse von Unternehmern geben. Dies gilt etwa für die private Kommunikation der etwa 500.000 Bundesbediensteten,[57] die mit dienstlicher Erlaubnis über ihren dienstlichen Internetanschluss privat – zum Beispiel mit Journalisten, Fachärzten, Psychologen, Beratungsstellen (z.B. Eheberatung, Schwangerschaftsberatung), Gewerkschaften oder Presseangehörigen – kommunizieren können. Auch dienstliche Kommunikation kann besonders vertraulich sein, etwa die Anzei-

[55] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 218.

[56] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 270.

[57] Statistisches Bundesamt, Pressemitteilung Nr.417 vom 30.09.2005, http://www.destatis.de..

ge von Straftaten, Steuerdelikten oder sonstigen Vergehen, aber auch die gesetzlich vorgeschriebene Übermittlung personenbezogener Daten etwa durch Arbeitgeber oder Steuerpflichtige. An Bundesbehörden wie das Bundeskriminalamt werden beispielsweise auch die hochsensiblen Ergebnisse aus Telekommunikationsüberwachungsmaßnahmen per E-Mail übermittelt. Auch Bundestagsabgeordneten in ihrer Eigenschaft als Volksvertreter und in ihrer Funktion als Organ zur Regierungskontrolle vertrauen Bürger regelmäßig hochsensible Sachverhalte an.

Im Vergleich zur Aufzeichnung des Kommunikationsverhaltens greift die Aufzeichnung des Informationsverhaltens noch tiefer in die Grundrechte der Betroffenen ein. Während Kommunikationsdaten unmittelbar nur Aufschluss über die näheren Umstände eines Kontakts geben, reflektieren Informationsdaten sogar den Inhalt der empfangenen oder gesendeten Information. Anhand der protokollierten Internetadressen (URLs) kann der Inhalt der Informationen, die der Nutzer abgerufen oder veröffentlicht hat, rekonstruiert werden. In der protokollierten URL sind regelmäßig auch vom Nutzer eingegebene Suchwörter enthalten. In quantitativer Hinsicht kommt hinzu, dass sich die Individualkommunikation eines Bürgers mit Bundesbehörden typischerweise auf einzelne Kontakte pro Jahr beschränken wird, während bei der Internetnutzung jeder Klick protokolliert wird und das Verhalten der Bürger dadurch sehr viel ausführlicher erfasst wird. Schon aus einem einzigen Internet-Nutzungsvorgang kann sich ein aussagekräftiges Persönlichkeitsprofil erstellen lassen.

Wenn wir Zeitungen, Magazine oder Bücher lesen, wenn wir im Radio Musik hören oder fernsehen, brauchen wir nicht zu befürchten, dass uns jemand über die Schulter schauen oder mitschreiben könnte. Lesen wir hingegen Zeitungen, Magazine oder Bücher im Internet, hören wir dort Musik oder betrachten wir Videos im Internet (z.B. eine Ministerrede auf der Ministeriumsseite), muss der Anbieter für die Dauer der Übertragung aus technischen Gründen unsere IP-Adresse kennen. Anhand dieser Adresse oder anderer Nutzerkennungen kann jede Eingabe und jeder Mausklick beim Lesen, Schreiben und Diskutieren im Internet erfasst, aufgezeichnet, ausgewertet, weiter gemeldet und offen gelegt werden. Eine Erfassung unseres Internet-Nutzungsverhaltens ist nicht nur einer Filmaufzeichnung unseres Zeitungslesens oder Fernsehens vergleichbar. Vielmehr können Internet-Nutzungsdaten – anders als Videoaufzeichnungen – maschinell zugeordnet und ausgewertet werden und weisen daher eine besonders „hohe Sensitivität“ auf.[58] Was wir im Internet lesen, suchen und schreiben, spiegelt unsere Persönlichkeit, unsere Vorlieben und Schwächen in einmaliger Deutlichkeit wider. Der Gesetzgeber hat unsere Mediennutzung daher im Telemediengesetz zurecht in besonderem Maße vor einer Erfassung geschützt. § 5 BSIG durchbricht und entwertet diesen Schutz im Bereich des Bundes.

Die nach § 5 BSIG gespeicherten Nutzungsprotokolle machen in Verbindung mit der Kenntnis der Identität eines Internetnutzers potenziell dessen gesamte über das Bundes-

[58] Bundesregierung, Begründung zum TDDSG, BT-Drs. 13/7385, 25.

netz abgewickelte Internetnutzung nachvollziehbar, also die Inhalte, für die er sich im Netz interessiert (gelesene Internetseiten, eingegebene Suchbegriffe), die er veröffentlicht oder per E-Mail versandt hat. Eine Vorratsspeicherung von Internetkennungen hebt damit die Anonymität der Internetnutzung auf,[59] die in vielen Situationen Voraussetzung für die Kommunikationsbereitschaft der Beteiligten ist (z.B. anonyme Information von Journalisten per E-Mail, anonyme Meinungsäußerung im Internet, vertraulicher Austausch von Geschäftsgeheimnissen, vertrauliche Koordinierung politischer Proteste, psychologische, medizinische und juristische Beratung oder Selbsthilfegruppen von Menschen in besonderen Situationen wie Notlagen und Krankheiten). Ist Anonymität in diesen Situationen nicht vorhanden, kann Kommunikation anders verlaufen oder ganz unterbleiben, was schwerwiegende Nachteile für Grundrechtsträger und die Gesellschaft insgesamt nach sich ziehen kann.

Aus der Internetkennung (IP-Adresse) lässt sich überdies der ungefähre Aufenthaltsort eines Nutzers ableiten, nach neuen Forschungsergebnissen sogar mit hoher Treffsicherheit, ob sich der Nutzer zu Hause, in der Arbeit oder unterwegs aufgehalten hat.[60] Die nach § 5 BSIG gespeicherten Daten können also auch die Erstellung von Bewegungsprofilen ermöglichen.

(d) Sicherheitsrisiken und sonstige Nachteile für Internetnutzer

In der letzten Zeit häufen sich in Deutschland die Fälle versehentlicher und absichtlicher Veröffentlichung und Zweckentfremdung von Informationen über unsere Internetnutzung. Im Jahr 2008 wurden mehrere Fälle bekannt, in denen persönliche Daten von Internetnutzern offen gelegt und dem Risiko eines Missbrauchs ausgesetzt wurden. 18.000 Personen, die im Internet bei der Anzeigenblatt-Tochter WBV Wochenblatt des Axel Springer Verlages – zum Teil unter Chiffre – Anzeigen aufgegeben hatten, mussten ihre Privatanschrift, E-Mail-Adresse, Handynummer und Kontodaten im Internet wieder finden.[61] Das mit Diskretion werbende Erotikunternehmen Beate Uhse veröffentlichte die E-Mail-Adressen Tausender von Personen, die sich Sexfilme im Internet angesehen hatten.[62] In einem Forum des ZDF-Kinderkanals konnten sich beliebige Personen Klarnamen, Adresse, Telefonnummer und Geburtsdatum aller 1.000 registrierten Kinder verschaffen.[63]

---

[59] Vgl. BVerfG MMR 2010, 356.

[60] Pitsillidis/Xie/Yu/Abadi/Voelker/Savage, How to Tell an Airport from a Home, 2010, http://research.microsoft.com/pubs/139079/hotnets10.pdf.

[61] Spiegel 43/2008 vom 20.10.2008, Seite 70.

[62] Die Welt vom 04.09.2008: Beate Uhse verschlampt E-Mail-Adressen im Web, http://www.welt.de/welt_print/article2398543/Beate-Uhse-verschlampt-E-Mail-Adressen-im-Web.html.

[63] Spiegel Online vom 16.10.2008: Kika stellt Daten von Kindern ungeschützt ins Web, http://www.spiegel.de/netzwelt/web/0,1518,584525,00.html.

Die oben genannten Vorfälle zeigen eindeutig, dass nur nicht gespeicherte Daten sichere Daten sind. Sie bestätigen, dass der bisherige deutsche Ansatz einer strengen Beschränkung der Aufzeichnung von Kommunikationsspuren (§§ 96 TKG, 13, 15 TMG) richtig ist. Die bisherigen gesetzlichen Beschränkungen der Aufzeichnung von Verkehrs- und Nutzungsdaten minimieren den Schaden aus Datenlecks und gewährleistet Sicherheit vor einer missbräuchlichen Aufdeckung und Auswertung unserer Internetnutzung.

Wegen der vielen Fälle von Datenmissbrauch sind inzwischen 80% der Bundesbürger „sehr besorgt" um die Sicherheit ihrer Daten.[64] Eine deutliche Mehrheit der Bevölkerung fordert eine gesetzliche Stärkung des Datenschutzes.[65] Einer Umfrage aus dem Jahr 2007[66] zufolge befürchten 54% der Internetnutzer, dass ihre persönlichen Daten im Internet ungeschützt sind. 31% der Befragten haben schon häufiger auf eine Bestellung im Internet verzichtet, weil sie ihre Daten nicht preisgeben wollten. Einer Umfrage aus dem Jahr 2008 zufolge sind 57% der Deutschen „sehr besorgt" darüber, dass einige Internetanbieter ihr Nutzungsverhalten in personenbeziehbarer Form protokollieren und dass solche Daten mitunter versehentlich veröffentlicht werden.[67] 60% sorgen sich, dass ihre Daten in die Hände Dritter gelangen könnten.[68] Jeder vierte Internet-Nutzer ist zum Schutz seiner Daten inzwischen immer oder vorwiegend unter Fantasienamen im Netz unterwegs.[69] Auf diese Weise wollen die Bürger einen Missbrauch ihrer Daten verhindern, Internetangebote anonym nutzen und sich dagegen wehren, dass unangemessen viele Daten abgefragt werden.[70] Dieser Selbstschutz wird durch die Aufzeichnung von Protokolldaten unterlaufen, weil diese unbemerkt erfolgt und nicht verhindert werden kann. Internetnutzer informieren sich in vermeintlicher Anonymität über private politische oder gesundheitliche Belange und verkennen, dass ihre IP-Adresse aufgezeichnet wird und über § 113 TKG jederzeit auf ihre Person zurückgeführt werden kann.

Wo die nach § 5 BSIG gespeicherten Daten zur Strafverfolgung verwendet werden, kann das Informations- und Kommunikationsverhalten staatliche Ermittlungs- und Überwachungsmaßnahmen, Hausdurchsuchungen, Beschlagnahmen bis hin zur Festnahme nach sich ziehen. Dies geschieht nicht selten auch zu Lasten Unschuldiger auf Grund eines falschen Verdachts. Strafrechtliche Ermittlungsverfahren richten sich schon allgemein zu ei-

---

[64] Unisys-Umfrage vom 01.10.2008, http://www.unisyssecurityindex.com/resources/reports/-Germany%20security%20index%20Oct%201-08.pdf.

[65] Emnid-Umfrage vom 02.06.2008, http://www.presseportal.de/pm/13399/1204206/n24/rss.

[66] Institut Allensbach, Sicher im Netz?, http://www.ifd-allensbach.de/news/prd_0717.html.

[67] Microsoft, Umfrage vom Februar 2008, http://www.daten-speicherung.de/?p=267.

[68] Microsoft, Umfrage vom Februar 2008, http://www.daten-speicherung.de/?p=267.

[69] Fittkau und Maaß, Umfrage unter 121.233 deutschsprachigen Internet-Nutzern im Frühjahr 2009, http://www.w3b.org/nutzerverhalten/furcht-vor-datenmissbrauch-beeinflusst-nutzerverhalten.html.

[70] Fittkau und Maaß, Umfrage unter 121.233 deutschsprachigen Internet-Nutzern im Frühjahr 2009, http://www.w3b.org/nutzerverhalten/furcht-vor-datenmissbrauch-beeinflusst-nutzerverhalten.html.

nem großen Teil gegen Unschuldige, wie die hohe Einstellungsquote nahe legt. Telekommunikationsdaten wohnt darüber hinaus eine im Vergleich zu anderen Spuren besonders hohe Gefahr inne, den Verdacht auf Unschuldige zu lenken, weil sie sich nur auf den Inhaber des genutzten Anschlusses beziehen und keinen Aufschluss über den konkreten Nutzer geben. Nicht nur in Familie und Betrieb werden Internetanschlüsse gemeinsam genutzt.[71] Über offene WLAN-Funknetze oder Dienste wie TOR kann jeder Internetnutzer zum Internetanbieter für die Öffentlichkeit werden, ohne dass dies aus der genutzten Internetkennung hervor ginge und vor unbegründeten Ermittlungen schützte. Auch in anderer Hinsicht ist die Zuordnung dynamisch vergebener Internetkennungen besonders fehleranfällig (z.B. Zahlendreher, Zeitstempel).[72]

Müssen Internetnutzer nicht ohne Grund befürchten, durch bloße Inanspruchnahme ihrer grundrechtlich geschützten Freiheiten Nachteile zu erleiden, so werden sie sich nur noch eingeschränkt über das Internet informieren und darüber kommunizieren. Dies kann nicht nur Gefahren für Gesundheit, Leib und Leben einzelner Internetnutzer und ihres Umfeldes nach sich ziehen, etwa wenn mutmaßlich HIV-Infizierte sich nicht über Testmöglichkeiten zu informieren trauen oder wenn gewalttätige Ehemänner vor einer Kontaktaufnahme zu Internet-Beratungsstellen zurückschrecken. Letztlich leidet unser freiheitliches demokratisches Gemeinwesen insgesamt, wenn etwa Informanten die Presse oder auch staatliche Stellen nicht mehr ohne Furcht vor Rückverfolgung über Missstände in Kenntnis setzen können.

(e) Diskriminierung

Das Gewicht des Grundrechtseingriffs erhöht sich weiter durch die mit § 5 BSIG verbundene Schlechterstellung von Personen, welche die Informationstechnik des Bundes nutzen (müssen).

§ 5 BSIG sieht eine unterschiedliche Behandlung des Informationsaustausches mit Bundesorganen und deren Angehörigen einerseits und des Informationsaustauschs mit sonstigen Personen andererseits vor. Während § 5 Abs. 1 S. 1 Nr. 1 und Abs. 2 BSIG den Bund dazu ermächtigt, Informationen über das Telekommunikations- und Mediennutzungsverhalten der Bürger global und pauschal aufzuzeichnen, sind private Betreiber vergleichbarer Systeme zu einer solchen Maßnahme nicht berechtigt (§§ 28 BDSG, 15 TMG). Der Bürger muss bei der Kommunikation mit Bundesbehörden eine Verhaltenserfassung hinnehmen, vor der er sonst geschützt ist.

Die von § 5 BSIG Betroffenen haben in vielen Fällen keine zumutbare Ausweichmöglichkeit, was das Gewicht des Eingriffs erhöht. Wer dienstlich mit Bundesbehörden in Kontakt tritt, ist regelmäßig dazu gezwungen, etwa um gesetzlichen Verpflichtungen nachzukom-

[71] Näher Breyer, NJOZ 2010, 1085.

[72] Arbeitskreis Vorratsdatenspeicherung, http://wiki.vorratsdatenspeicherung.de/images/Bericht_Sicherheit-vor-Sammelwut.pdf, 7.

men. Dass in der heutigen Informationsgesellschaft Kommunikation ohne Telekommunikationsnetze kaum noch denkbar ist, liegt auf der Hand. Der Gesetzgeber beginnt sogar, elektronische Datenübermittlungen vorzuschreiben (z.B. Umsatzsteueranmeldungen). Auch bestimmte Berufsgruppen, etwa Journalisten, sind in hohem Maße auf die Kontaktaufnahme zu Bundesorganen angewiesen. Erst recht gilt dies für persönliche Kontakte zu Angehörigen von Bundesorganen, die während der Arbeitszeit oft nicht anders erreichbar sein werden.

Fraglich ist, ob ein sachlicher Grund von solcher Art und solchem Gewicht besteht, dass er es rechtfertigte, den Bund zu einer anlasslosen und flächendeckenden Erfassung, Rasterung und Vorratsspeicherung der näheren Umstände der Kommunikation über seine Netze zu ermächtigen, Privatpersonen dagegen nicht. Als Rechtfertigungsgrund könnte einzig angeführt werden, dass die Funktionsfähigkeit der Informationstechnik des Bundes schutzwürdiger sei als die Informationstechnik Privater. Dagegen spricht jedoch, dass eine erhöhte Schutzwürdigkeit der Informationstechnik von Bundesorganen im Vergleich zur Informationstechnik von Energieversorgern, Gefahrguttransportunternehmen, Banken, Börsen, Krankenhäusern, Medien usw. nicht gegeben ist. Auch das Bundesinnenministerium stellt die Bedeutung der Informationstechnik in diesen Bereichen auf eine Stufe mit der Bedeutung der Informationstechnik in Behörden, Verwaltung und Justiz.[73] Im Übrigen kennen auch die Bundesländer keine § 5 BSIG vergleichbaren Normen für deren Behörden.

Festzuhalten ist somit, dass keine Rechtfertigung dafür erkennbar ist, dass der Gesetzgeber dem BSI Maßnahmen zum Schutz der Informationstechnik des Bundes erlaubt, die er bei Trägern anderer kritischer Infrastrukturen nicht für erforderlich und verhältnismäßig hält.

(3) Zentralisierung nicht erforderlich

§ 5 BSIG ist bereits deshalb nicht erforderlich, weil Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit der Informationstechnik des Bundes ebenso gut oder besser bei derjenigen Behörde getroffen werden können, welche die jeweils zu schützende Anlage betreibt. Der Gesetzgeber kann durch materielle Anforderungen und durch Verfahren (z.B. vorgeschriebene Sicherheitszertifizierung durch das BSI) sicher stellen, dass bei jedem Bundesorgan ein ebenso hoher oder höherer Sicherheitsstandard vorhanden ist wie bei dem BSI selbst. Die Konzentration der Verarbeitung personenbezogener Daten auf eine Zentralbehörde – das BSI – ist danach nicht erforderlich.

Unter Fachleuten ist vielmehr anerkannt, dass eine zentrale Sicherheitsarchitektur Systeme angriffs- und fehleranfälliger macht als die dezentrale Anwendung verschiedener Sicherheitssysteme. Wenn künftig ein Angreifer die BSI-Schutzmaßnahmen überwindet, wird

---

[73] BMI: Nationaler Plan zum Schutz der Informationsinfrastrukturen, http://www.bmi.bund.de/cae/servlet/contentblob/121734/publicationFile/13577/Nationaler_Plan_Schutz_Informationsinfrastrukturen.pdf, 21.

er Zugang zur gesamten Informationstechnik aller Bundesbehörden und zu allen Verkehrs- und Nutzungsdaten des Bundes haben. Dezentrale Sicherheitslösungen sind daher schon aus Sicherheitsgründen vorzuziehen.

Es bedeutet auch für den Bürger einen Unterschied, ob nur die von ihm angeschriebene Behörde von seinem Kontakt Kenntnis hat oder ob eine zentrale Bundesbehörde Kenntnis von sämtlichen seiner Kontakte mit Bundesbehörden hat oder gar den Inhalt seiner sämtlichen Kommunikation mit Bundesbehörden zentral durchsucht (§ 5 Abs. 1 S. 1 Nr. 2 BSIG). Der zentralen Speicherung und Verarbeitung wohnt ein Missbrauchspotenzial inne, welches von der elektronischen Kontaktaufnahme zu Bundesbehörden abschrecken kann. Eine zentrale Sicherheitsarchitektur ist anfälliger für internen Missbrauch und weckt Begehrlichkeiten für ihre Nutzung zu weiteren Zwecken, zumal § 5 BSIG eine – ebenso wie Bundeskriminalamt und Nachrichtendienste – dem Bundesinnenminister unterstehende Behörde zu der Informationsverarbeitung ermächtigt. Schließlich erhöhen zentrale Datensammlungen auch die Gefahr von Datenpannen und das Ausmaß der dadurch drohenden Schäden. Wenngleich dem Staat im Grundsatz eine Zentralisierung von Verwaltungsaufgaben unbenommen ist, so überschreitet der Bund doch sein diesbezügliches Ermessen, wenn er an die Stelle von Sicherungsmaßnahmen der Kommunikationspartner die Einschaltung einer unbeteiligten Behörde und damit einen Eingriff in die Vertraulichkeit der Telekommunikation setzt. Es schreckt unzumutbar von der Kommunikation mit Bundesbehörden und ihren Angehörigen sowie von der Nutzung ihrer Telemedien ab, wenn Informationen über das gesamte Informations- und Kommunikationsverhalten bei einer Zentralbehörde zusammenlaufen und dort festgehalten und ausgewertet werden.

Auch ohne § 5 BSIG haben Bundesbehörden im Übrigen die Möglichkeit, das BSI mit einer Verarbeitung personenbezogener Daten in ihrem Auftrag zu betrauen. Von dieser Möglichkeit wurde auch Gebrauch gemacht.[74] Es ist nicht zu erkennen, warum die bisherigen Möglichkeiten nicht ausreichen und stattdessen ein derart erheblicher Grundrechtseingriff notwendig sein soll wie er in § 5 BSIG vorgesehen ist. Im Fall der Auftragsdatenverarbeitung behält die jeweilige Behörde, mit welcher der Bürger kommuniziert, die Kontrolle und auch die rechtliche Verantwortung für die auf das BSI ausgelagerten Aufgaben. Dies ist sowohl für den betroffenen Bürger wie auch für die betroffenen Behördenmitarbeiter – rund 500.000 Menschen sind bei Bundesorganen beschäftigt – wichtig und sicherte etwa die Anwendung der Mitbestimmungsregelungen, die § 5 BSIG aushebelt.

Ist die Ermächtigung einer Zentralbehörde somit nicht aus Sicherheitsgründen erforderlich, so mag sie zwar geeignet sein, den mit dezentralen Lösungen verbundenen finanziellen und personellen Aufwand zu reduzieren. Dieses wirtschaftliche Interesse könnte eventuell geringfügige Menschenrechtseingriffe rechtfertigen, nicht aber derart schwerwiegende Eingriffe in Fernmeldegeheimnis und Informationsfreiheit wie sie hier zur Diskussion ste-

[74] Helmbrecht, INA-Protokoll Nr. 16/94, 23.

hen. Das Interesse der Bürger an der Vertraulichkeit ihrer Kommunikation mit Bundesorganen und ihren Angehörigen überwiegt ein finanzielles Interesse des Bundes. Dabei ist auch zu berücksichtigen, dass die Mehrkosten dezentraler Sicherheitslösungen schon deswegen gering ausfallen, weil die meisten Bundesorgane entsprechende Vorkehrungen im eigenen Interesse bereits angeschafft und in Betrieb haben.

(4) Unverhältnismäßigkeit einer Vorratsdatenspeicherung

§ 5 BSIG ist vor dem Hintergrund einer allgemeinen Aufweichung des strikten Verbots der Sammlung personenbezogener Daten auf Vorrat durch den Gesetzgeber zu sehen. Der Grundgedanke, dass sich eine Aufzeichnung des Verhaltens beliebiger Bürger ins Blaue hinein mit der bloßen Möglichkeit einer Rechtsgutsgefährdung rechtfertigen lasse, stellt einen Dammbruch dar, der eine Flut anlassloser Erfassungen unseres täglichen Lebens nach sich ziehen wird, wenn ihm nicht am Beispiel des § 5 BSIG Einhalt geboten wird. Die Zulässigkeit einer globalen und pauschalen Erfassung allein im Hinblick auf eine mögliche künftige staatliche Verwendung von Informationen droht allmählich alle Lebensbereiche zu erfassen, weil eine Globalspeicherung für den Staat stets und in allen Bereichen nützlich ist.

Wir machen den Gerichtshof darauf aufmerksam, dass die Maßstäbe, die er in der vorliegenden Entscheidung entwickelt, auch in anderen Bereiche angewandt werden werden. § 5 BSIG stellt einen Präzedenzfall für eine immer weiter reichende vorsorgliche staatliche Aufzeichnung und Auswertung menschlichen Verhaltens dar. Diese Entwicklung droht schrittweise zu einem gläsernen Bürger zu führen, wenn nicht strenge Anforderungen zum Schutz der Privatsphäre der Bürger aufgestellt werden.

(a) Übertragbarkeit des Urteils des EGMR in Sachen S. und Marper

Dass § 5 BSIG das Grundrecht auf Achtung der Privatsphäre (Art. 8 EMRK) verletzt, ergibt sich aus dem Urteil der Großen Kammer des Europäischen Gerichtshofs für Menschenrechte vom 04.12.2008.[75] In diesem Urteil hat der Gerichtshof ausgeführt:[76]

> „*In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society.*"

[75] EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 66 ff.

[76] EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 125.

Der Gerichtshof hat also die „flächendeckende und unterschiedslose Natur der Befugnisse zur Vorratsspeicherung der Fingerabdrücke, Zellproben und DNA-Profile“ Verdächtiger als „unverhältnismäßigen Eingriff in das Recht des Beschwerdeführers auf Achtung seiner Privatsphäre“ bezeichnet und die entsprechende Eingriffsbefugnis des englischen Rechts als grundrechtswidrig verworfen. Er hat dabei wohlgemerkt nicht auf die Dauer der Speicherung abgestellt, sondern auf die „flächendeckende und unterschiedslose Natur der Befugnisse“, wie sie auch bei § 5 BSIG gegeben ist.

Im Vergleich zu der vom Gerichtshof verworfenen Vorratsspeicherung von Fingerabdrükken greift § 5 BSIG sogar noch weit tiefer in unser Recht auf Achtung der Privatleben ein.

Erstens ist § 5 BSIG quantitativ weit eingriffsintensiver:

a) Während die englische Befugnis nur Personen betraf, die einer Straftat verdächtig waren, betrifft § 5 BSIG quasi jeden Menschen, der für den Bund tätig ist oder mit ihm elektronisch kommuniziert. In Großbritannien waren einige Millionen von Personen von einer Speicherung ihrer biometrischen Daten betroffen. Von § 5 BSIG sind demgegenüber praktisch alle 50 Mio. Internetnutzer in Deutschland betroffen.

b) In der englischen Datensammlung waren von jedem Verdächtigen bis zu drei Angaben gespeichert: Fingerabdruck, Gewebeprobe und DNA-Profil. Aufgrund § 5 BSIG wird demgegenüber alltägliches Telekommunikations- und Informationsverhalten über Bundesnetze erfasst. Es handelt sich um eine weitaus größere Menge an Informationen.

Zweitens ist die Vorratsdatenspeicherung auch qualitativ weit eingriffsintensiver:

a) Die in England gesammelten biometrischen Informationen konnten zur Identifizierung Verdächtiger verwendet werden; im Fall von Gewebeproben und DNA-Profilen auch zur Gewinnung von Informationen über Herkunft und Krankheiten. Die unter § 5 BSIG gesammelten und ausgewerteten Informationen erlauben demgegenüber nicht nur eine Identifizierung von Bürgern, sondern reflektieren deren alltägliches Kommunikations-, Informations- und Bewegungsverhalten. Diese Informationen können Rückschlüsse auf unsere sozialen Kontakte, auf unseren Tagesablauf, auf unsere Interessen und – anhand der Kommunikationspartner – teilweise auch auf sensible Informationen wie unsere Krankheiten (Information bei der Bundeszentrale für gesundheitliche Aufklärung), unsere Herkunft, unser Sexualleben oder politische Einstellungen zulassen. Die über Monate aufbewahrten Telekommunikations- und Internetnutzungsdaten können einen erheblichen Teil der Persönlichkeit und des privaten und beruflichen Lebens von Menschen offen legen. Sie weisen damit einen unvergleichlich höheren Aussagegehalt auf als biometrische Merkmale zur Identifizierung von Personen, wie sie in England erfasst worden waren.

b) Während in England nur Personen, die einer Straftat verdächtig waren, biometrische Merkmale abgenommen wurden, trifft § 5 BSIG sogar Menschen, die nie auch nur im Verdacht einer Straftat gestanden haben. Selbst der rechtstreueste Bürger kann die

Erfassung seines Kommunikations- und Bewegungsverhaltens infolge § 5 BSIG nicht vermeiden.

Verletzt nach der Entscheidung des Europäischen Gerichtshofs für Menschenrechte die Sammlung biometrischer Daten aller Verdächtiger das Verhältnismäßigkeitsverbot, so tut es die weitgehende Sammlung des Kommunikations-, Informations- und Bewegungsverhaltens der gesamten (auch unverdächtigen) Bevölkerung erst Recht.

Soweit der Gerichtshof in einer Kammerentscheidung Finnland verurteilt hat, weil dessen Gesetze im Jahr 1999 die Aufklärung einer im Internet begangenen Straftat nicht zuließen,[77] steht dies der Unverhältnismäßigkeit einer Vorratsdatenspeicherung nicht entgegen, weil diese Entscheidung eine andere Fallgestaltung betraf: In jenem Fall verfügte der finnische Internetanbieter über Daten, die eine Identifizierung des mutmaßlichen Täters ermöglicht hätten;[78] das finnische Recht erlaubte die Herausgabe dieser Daten aber nicht.[79] Der Gerichtshof hat mit seiner Entscheidung beanstandet, dass das finnische Recht einen Zugriff auf ohnehin vorhandene Daten selbst zur Aufklärung einer vom Gerichtshof als schwer angesehenen Straftat (sexuelle Verleumdung eines Kindes in der Öffentlichkeit, welche das Kind der Gefahr sexueller Übergriffe aussetzte) nicht zuließ. Dass der Staat zur Aufklärung schwerer Straftaten auf ohnehin zu betrieblichen Zwecken gespeicherte Daten zugreifen darf, steht hier nicht in Frage. Der Gerichtshof hat in der genannten Entscheidung demgegenüber nicht gefordert oder zugelassen, zur Aufklärung möglicher zukünftiger Straftaten oder Abwehr möglicher zukünftiger Gefahren rein vorsorglich das Kommunikations- und Bewegungsverhalten der gesamten Bevölkerung erfassen zu lassen. Gegen diese Annahme spricht auch die Anmerkung des Gerichtshofs, wonach Finnland das „Defizit“ in seinem Prozessrecht in einem späteren „Gesetz über die Ausübung der Meinungsfreiheit in Massenmedien“ angegangen sei.[80] Dieses Gesetz sah eine Befugnis zur Identifizierung von Kommunikationsteilnehmern auf richterliche Anordnung vor,[81] nicht jedoch eine anlasslose und flächendeckende Vorratsdatenspeicherung.

(b) Vorratsdatenspeicherung verzichtbar für die Strafverfolgung

In Sachen S. und Marper ist der Gerichtshof zutreffend der Behauptung der britischen Regierung entgegen getreten, die damals angefochtene Vorratsspeicherung sei „unabdingbar“ zur Verfolgung von Straftaten.[82] Dieser Behauptung hat der Gerichtshof erstens entgegen gehalten, dass England die Maßnahme selbst erst 2001 eingeführt habe.[83] Zwei-

[77] EGMR, K.U.-FI vom 02.12.2008, 2872/02.

[78] EGMR, K.U.-FI vom 02.12.2008, 2872/02, Abs. 9.

[79] EGMR, K.U.-FI vom 02.12.2008, 2872/02, Abs. 40.

[80] EGMR, K.U.-FI vom 02.12.2008, 2872/02, Abs. 49.

[81] EGMR, K.U.-FI vom 02.12.2008, 2872/02, Abs. 21.

[82] EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 115.

[83] EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 115.

tens hat er darauf hingewiesen, dass die Strafverfolgungsbehörden anderer Staaten auch ohne eine solche Maßnahme auskommen.[84]

Nichts anderes gilt auch für die Vorratsspeicherung von Telekommunikationsdaten zur Abwehr von Gefahren für die IT-Sicherheit. Als § 5 BSIG beschlossen wurde, praktizierte keine deutsche öffentliche Stelle eine anlasslose Aufzeichnung, Auswertung und Vorratsdatenspeicherung der dort genannten Daten, zumal dies gegen das geltende Recht verstoßen hätte. Das BSI selbst machte auch lange Zeit nach Inkrafttreten der Norm davon noch keinen Gebrauch. Die große Mehrzahl der öffentlichen Stellen (nämlich in den Ländern) und auch private Stellen kommen bis heute ohne § 5 BSIG vergleichbare Vorschriften aus.

Es gibt keinen empirischen Nachweis dafür, dass fachgerecht gesicherte („gehärtete“) und unterhaltene IT-Systeme ohne anlasslose Aufzeichnung, Auswertung und Vorratsdatenspeicherung des gesamten Informations- und Kommunikationsverhaltens messbar häufiger oder länger unter Störungen der Verfügbarkeit, Vertraulichkeit oder Integrität litten als Systeme, die eine solche Totalprotokollierung und –auswertung vornehmen. Die Frage ist unseres Wissens bislang auch nicht nach wissenschaftlichen Kriterien untersucht worden.

(aa) Minimale Relevanz für die Strafverfolgung

Dass auch mit Blick auf das Ziel einer Verfolgung etwaiger schwerer Straftaten kein „hinreichend dringendes soziales Bedürfnis“ nach einer permanenten, flächendeckenden Aufzeichnung des über Bundesnetze abgewickelten Telekommunikationsverhaltens der gesamten Bevölkerung besteht, bestätigt eine ausführliche Untersuchung aus Deutschland. Das Bundesjustizministerium hat bei dem unabhängigen Max-Planck-Institut für ausländisches und internationales Strafrecht eine Untersuchung des Zugriffs auf Verkehrsdaten zum Zweck der Strafverfolgung in Auftrag gegeben.[85] Das Institut hat eine repräsentative Stichprobe von 467 strafrechtlichen Ermittlungsverfahren untersucht, in denen Telekommunikations-Verkehrsdaten erhoben worden waren.

Ausweislich der repräsentativen Aktenanalyse des Max-Planck-Instituts konnten auch ohne Vorratsdatenspeicherung nur bei 4% der Zielanschlüssen die von den Strafverfolgungsbehörden angeforderten Verkehrsdaten nicht mehr oder nicht vollständig erlangt werden.[86]

Die Zahl von 4% bezieht sich auf Strafverfahren, in denen Verkehrsdaten angefordert wurden. Das Gutachten schätzt, dass im Untersuchungsjahr 2005 insgesamt 40.000 Be-

---

[84] EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 112.

[85] Albrecht/Grafe/Kilchling, Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO (im Folgenden: MPI-Forschungsbericht), http://www.bmj.bund.de/files/-/3045/MPI-GA-2008-02-13%20Endfassung.pdf.

[86] MPI-Forschungsbericht, 253.

schlüsse zur Herausgabe von Verkehrsdaten erlassen wurden.[87] Da in 467 der untersuchten Ermittlungsverfahren 1257 Beschlüsse erlassen wurden,[88] kann man von 2,7 Beschlüssen pro Verfahren ausgehen. Danach werden 2005 etwa 15.000 Ermittlungsverfahren bundesweit die Erhebung von Verkehrsdaten zum Gegenstand gehabt haben. Wenn in 4% dieser Verfahren Anfragen mangels gespeicherter Daten ergebnislos blieben, beträfe dies etwa 600 Verfahren bundesweit. Gemessen daran, dass in den Jahren 2003 und 2004 jeweils ca. 4,9 Mio. Ermittlungsverfahren bearbeitet wurden,[89] entspricht dies 0,01% aller Ermittlungsverfahren. Dies bestätigt, dass eine Vorratsdatenspeicherung nur in 0,01% aller strafrechtlichen Ermittlungsverfahren überhaupt einen Beitrag zur Strafverfolgung leisten kann.

Um den möglichen Nutzen einer Vorratsdatenspeicherung zu Strafverfolgungszwecken zu ermitteln, müssen indes von den Verfahren, in denen Abfragen wegen fehlender Verkehrsdaten ergebnislos blieben, noch diejenigen Verfahren in Abzug gebracht werden, die auf anderem Wege aufgeklärt werden konnten. Laut Studie blieb die Verkehrsdatenabfrage – trotz zu 96% vorhandener Daten – bei etwa 130 Beschuldigten erfolglos; dennoch wurde gegen etwa 45 von ihnen später Anklage erhoben.[90] Etwa ein Drittel der Verfahren mit erfolgloser Verkehrsdatenabfrage kann somit auf anderem Wege aufgeklärt werden.

Weiterhin müssen von den Verfahren, in denen Abfragen erfolglos blieben, noch diejenigen Verfahren in Abzug gebracht werden, die im Fall vorhandener Daten ebenfalls eingestellt worden wären. Auch in diesen Fällen leistet die Vorratsdatenspeicherung keinen Beitrag zur Verfolgung von Straftaten. Laut Studie wurden – trotz zu 96% vorhandener Daten – 60% der Verfahren eingestellt und in 23% der Verfahren Anklage erhoben.[91] Dies entspricht einer „Einstellungsquote“ von 72% der abgeschlossenen Verfahren; hinzu kommen noch die gerichtlichen Einstellungen und Freisprüche. In etwa drei Viertel der Verfahren würde eine Vorratsdatenspeicherung mithin schon deshalb keinen Beitrag zur Strafverfolgung leisten, weil die Verfahren selbst bei Vorliegen der angeforderten Verkehrsdaten eingestellt werden würden.

Unter Berücksichtigung all dieser Umstände ergibt sich, dass die Verfolgung von Straftaten zu gerade einmal 0,002% durch eine Vorratsspeicherung von Verkehrsdaten effektiviert werden könnte.[92] Schon allein durch Zufälle und statistische Einflüsse schwankt die jährliche Zahl der aufgeklärten Straftaten um ein hundertfaches dieses Betrags. Nicht an dieser Stelle berücksichtigt werden soll der Umstand, dass die meisten der weit zurück reichen-

[87] MPI-Forschungsbericht, 76.

[88] MPI-Forschungsbericht, 125.

[89] Statistisches Bundesamt, Staatsanwaltschaften - Fachserie 10 Reihe 2.6 - 2006, 13.

[90] MPI-Forschungsbericht, 391.

[91] MPI-Forschungsbericht, 390 f.

[92] 600 / 4.900.000 x 2/3 x (1-0,72) = 0,0023%.

den Verkehrsdatenanforderungen auf eine bloß allgemeine Erforschung des Kommunikationsumfelds eines Tatverdächtigen und nicht auf eine gezielte Abfrage gerichtet sind.[93]

Auf der anderen Seite ist zu berücksichtigen, dass die Strafverfolgungsbehörden die Nichtspeicherung oder Löschung von Verkehrsdaten (vgl. Art. 6 (1) RiL 2002/58/EG) zum Teil antizipieren und daher bereits keine entsprechenden Anordnungen beantragen dürften. Die Strafverfolgungsorgane haben bislang keine belastbaren Zahlen darüber vorgelegt, in wie vielen Verfahren jährlich dies der Fall sei. Eine Untersuchung des Bundeskriminalamts dürfte Fälle, in denen eine Anforderung von Verkehrsdaten mangels Erfolgsaussicht unterblieb, einschließen und nennt dennoch über mehrere Jahre hinweg nur 381 Fälle fehlender Verkehrsdaten.[94] Einzig das Land Rheinland-Pfalz hat gegenüber dem Bundesverfassungsgericht eine Schätzung vorgetragen, der zufolge 700 erfolglosen Auskunftersuchen 1.050 Fälle gegenüber stünden, in denen von vornherein wegen mutmaßlich gelöschter Daten keine Auskunft angefordert worden sei.[95] Auf dieser Grundlage müsste die Zahl der erfolglosen Auskunftersuchen mit 2,5 multipliziert werden, um auf die Gesamtheit der Fälle fehlender Verkehrsdaten zu schließen.[96] Auf dieser Grundlage könnte eine Vorratsdatenspeicherung in 0,006%[97] der registrierten Straftaten von Nutzen sein, was an der offensichtlichen Unverhältnismäßigkeit der die gesamte Bevölkerung treffenden Maßnahme nichts ändern würde.

Speziell die in Bundesnetzen anfallenden Daten, die Gegenstand des § 5 BSIG sind, dürften bei kaum einer unaufgeklärten Straftat eine Rolle spielen, da die wenigsten Straftaten über Bundesnetze begangen werden werden dürften.

(bb) Fehlende Relevanz für die Aufklärungsquote

Dass eine pauschale und generelle Vorratsdatenspeicherung in einer demokratischen Gesellschaft nicht zur Verfolgung von Straftaten erforderlich ist, belegt zweitens die Aufklärungsquote, die in Deutschland statistisch erfasst wird. Die Aufklärungsquote misst das Verhältnis der aufgeklärten zu den insgesamt registrierten Straftaten in einem Jahr.

Wenn man den Bereich der über das Internet begangenen Computerkriminalität betrachtet, hatte das Inkrafttreten des § 5 BSIG im Jahr 2009 keinerlei erkennbaren positiven Einfluss auf die registrierte Anzahl dieser Delikte (19.239 Fälle 2008, 28.820 Fälle 2009, 36.434 Fälle 2010) oder die Entwicklung der Aufklärungsquote (35,5% 2008, 32,9% 2009, 31,4% 2010). Es ist nicht ersichtlich, dass die Aufklärungsquote durch § 5 BSIG statistisch nach-

---

[93] MPI-Forschungsbericht, 115.

[94] Mahnken: Mindestspeicherungsfristen für Telekommunikationsverbindungsdaten - Rechtstatsachen zum Beleg der defizitären Rechtslage (2005), http://www.vorratsdatenspeicherung.de/images/bka_vorratsdatenspeicherung.pdf.

[95] Stellungnahme des rheinland-pfälzischen Ministeriums der Justiz vom 19.02.2008, 2 f.

[96] 700 x 2,5 = 700 + 1.050.

[97] 0,0023% x 2,5 = 0,0058%.

weisbar gesteigert worden wäre, zumal Fälle von Datenweitergaben nach § 5 BSIG nicht bekannt sind. Von einem Leerlaufen einzelner Straftatbestände ohne § 5 BSIG kann nach den genannten Zahlen ebenfalls keine Rede sein. Über das Internet begangene Computerkriminalität macht im Übrigen nicht einmal 1% der registrierten Straftaten aus. Zu 45% handelt es sich um Computerbetrug (§ 263a StGB), der kaum zulasten des Bundes begangen werden dürfte. Der Anstieg der polizeilich registrierten, über das Internet begangenen Computerkriminalität in den letzten Jahren ist durch die wachsende technische Kompetenz der Polizei, aber auch durch die allgemein zunehmende Verlagerung des Lebens in das Internet und dessen zunehmende Nutzung zu erklären. Die Zahl der insgesamt registrierten Straftaten ist rückläufig. Es besteht kein Anlass für den Einsatz derart drastischer Mittel.

Die Aufklärungsquote für Internetdelikte allgemein übertrifft mit 72,3% die allgemeine Aufklärungsquote von 56% deutlich.[98] Schon vor Inkrafttreten des § 5 BSIG wurde im Internetbereich eine weit überdurchschnittliche Aufklärungsquote erzielt.

Wie die Strafverfolgungsbehörden ohne Vorratsdatenspeicherung Internetdelikte aufklären, bedarf hier keiner näheren Erörterung. Es soll nur ein weiteres Mal darauf hingewiesen werden, dass im Bereich der postalischen Kommunikation, der unmittelbaren Kommunikation und des Bewegungsverhaltens generell keine Aufzeichnungen über das Verhalten der gesamten Bevölkerung in der Vergangenheit zur Verfügung stehen und gleichwohl nicht die Rede davon sein kann, dass eine Aufklärung bestimmter Typen von Straftaten deswegen regelmäßig leer liefe. Die durchschnittliche Aufklärungsquote von 55% kann generell erzielt werden, ohne dass systematisch das Kommunikations-, Bewegungs- und Informationsverhalten der gesamten Bevölkerung aufgezeichnet wird. Im Telekommunikationsbereich besteht auch ohne § 5 BSIG die bewährte Möglichkeit des Zugriffs auf Verkehrsdaten, die ohnehin zu betrieblichen Zwecken gespeichert sind oder aus besonderem Anlass im Einzelfall gespeichert werden. Diese Möglichkeiten haben in den letzten Jahren stets eine wirksame Strafrechtspflege auch im Bereich von Internetdelikten gesichert.

(cc) Unverhältnismäßigkeit

In dem Urteil in Sachen S. und Marper hat der Gerichtshof zutreffend die von der britischen Regierung vorgelegten Statistiken über die Zahl der erfolgreichen Abrufe aus der Datenbank hinterfragt. Er hat kritisiert, dass die Zahl der erfolgreichen Abrufe keinen Aufschluss darüber gebe, in wie viele Fällen ein erfolgreicher Abruf auch tatsächlich zur Verurteilung eines Straftäters geführt habe.[99] Auch sei nicht dargelegt, in wie vielen Fällen hierfür gerade die Vorratsspeicherung der Daten Nichtverurteilter erforderlich gewesen sei.[100] Die meisten der von der Regierung genannten erfolgreichen Abrufe wären auch ohne die bean-

[98] Bundeskriminalamt, Polizeiliche Kriminialstatistik 2011, 27 und 260.

[99] EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 116.

[100] EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 116.

standete Vorratsspeicherung möglich gewesen.[101] Wenngleich der Gerichtshof im Ergebnis davon ausging, dass die Vorratsspeicherung biometrischer Daten einen gewissen Beitrag zur Strafverfolgung leistete,[102] verwarf er sie gleichwohl als unverhältnismäßig weitgehend.

Nichts anderes gilt auch für die in § 5 BSIG vorgesehene Aufzeichnung, Auswertung und Vorratsspeicherung von Telekommunikations- und Internetnutzungsdaten. Die Bundesregierung legt schon keine Statistik darüber vor, ob und wie häufig eine automatisierte Auswertung im Sinne des § 5 BSIG überhaupt zur Meldung von Störungen, Fehlern oder Schadprogrammen geführt habe oder wie häufig auf gespeicherte Daten zugegriffen worden sei. Aus solchen Statistiken über die Zahl der Meldungen oder Zugriffe ergäbe sich ohnehin nicht, ob und in wie viele Fällen dies auch tatsächlich zur Abwehr einer Gefahr geführt habe. Auch ergäbe sich aus solchen Statistiken nicht, in wie vielen Fällen gerade eine anlasslose und flächendeckende Vorratsdatenspeicherung erforderlich gewesen sei und betrieblich gespeicherte oder im Einzelfall gespeicherte Daten oder andere Ermittlungsinstrumente nicht ausgereicht hätten.

Wie oben dargelegt, ist ein messbarer Beitrag gerade des § 5 BSIG zur IT-Sicherheit nicht festgestellt worden. Selbst wenn man davon ausginge, dass die Vorschrift einen gewissen Beitrag zur Erhöhung der Sicherheit leistete, greift eine flächendeckende und permanente Aufzeichnung des Kommunikations- und Informationsverhaltens über Bundesnetze doch unverhältnismäßig weit in das Grundrecht der Betroffenen auf Wahrung ihrer Privatsphäre und der Vertraulichkeit ihrer Information und Telekommunikation ein.

(c) Unzumutbar schwerer Grundrechtseingriff

Im Fall S. und Marper verwarf der Gerichtshof ferner die Argumentation der britischen Regierung, die bloße Aufbewahrung der Daten ohne ihre Nutzung könne sich auf die Betroffenen nicht nachteilig auswirken.[103] Der Gerichtshof wies vielmehr darauf hin, dass bereits der Vorhaltung personenbezogener Informationen eine „unmittelbare Auswirkung auf das Interesse der betroffenen Person am Schutz ihrer Privatsphäre“ zukomme, selbst wenn von den Informationen keinerlei Gebrauch gemacht werde.[104]

Ebenso zieht die § 5 BSIG vorgesehene Vorratsdatenspeicherung bereits konkrete Nachteile für die betroffenen Bürger nach sich, und zwar in folgender Hinsicht:

---

[101] EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 116.

[102] EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 117.

[103] EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 121.

[104] EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 121.

(aa) Staatliche Fehlurteile

Eine generelle und undifferenzierte Vorratsdatenspeicherung erhöht die allgemeine Gefahr, unschuldig einer Straftat verdächtigt zu werden:[105]

Erstens beziehen sich gesammelten Kommunikationsdaten stets nur auf den Inhaber eines Anschlusses. Wird der Anschluss von anderen Personen genutzt, dann kann der Inhaber leicht unschuldig in einen falschen Verdacht geraten.

Zweitens ermöglicht es der Zugriff auf Kommunikationsdaten den Behörden, nach dem Eliminierungsprinzip zu arbeiten. Dabei wird nicht, wie traditionell üblich, eine „heiße Spur" verfolgt, sondern es werden – etwa mit Hilfe von Kommunikationsdaten – eine (oft große) Gruppe von Personen ermittelt, die aufgrund bestimmter Merkmale als Täter in Betracht kommen (beispielsweise alle Personen, die innerhalb eines bestimmten Zeitraums dem Opfer einer Straftat E-Mails geschickt haben). Es kommt dadurch quasi zu einer Inflation an Verdächtigungen, aus der sich die so Erfassten nur noch im Wege einer Art Beweislastumkehr befreien können.[106] Weil ein Kommunikationsdatensatz ein Indiz gegen den Angeklagten bilden kann, muss dieser unter Umständen den Richter von seiner Unschuld überzeugen, um nicht zu Unrecht verurteilt zu werden.[107] Mangels eines Alibis wird Unschuldigen die Erschütterung der Indizienkette keineswegs immer gelingen. Aber auch, wenn sich die Unschuld einer Person noch vor ihrer Verurteilung herausstellt, kann ein falscher Verdacht ausreichen, um zu Hausdurchsuchungen, Untersuchungshaft, Bewegungseinschränkungen oder Aus- und Einreiseverboten zu führen, was mit schwerwiegenden Belastungen für die Betroffenen verbunden ist.

Folgende Fälle von Fehlurteilen aufgrund einer Analyse von Telekommunikationsdaten sind in Europa bereits bekannt geworden: In Österreich wurde ein Nigerianer mehrere Monate lang in Untersuchungshaft genommen, weil er wegen seiner zahlreichen Telefonkontakte als Anführer einer Rauschgiftbande in Verdacht geraten war.[108] Später stellte sich der Verdacht als unbegründet und der Nigerianer lediglich als gefragter Ratgeber in der schwarzen Gemeinschaft in Wien heraus.[109]

In Schweden gab es Fälle, in denen unschuldige Personen im Zusammenhang mit Ermittlungen wegen Netzkriminalität festgenommen wurden. Später stellte sich heraus, dass die

---

[105] BVerfGE 107, 299 (321).

[106] Hamm, TKÜV, 81 (86).

[107] Lisken/Denninger, Handbuch des Polizeirechte (2001), C 26.

[108] Krempl, Stefan: Die totale Informationsüberwachung, die Demokratie und die Hacker, Telepolis, Heise-Verlag, 28.12.2002, www.heise.de/ tp/ deutsch/ inhalt/ te/ 13870/ 1.html.

[109] Krempl, Stefan: Die totale Informationsüberwachung, die Demokratie und die Hacker, Telepolis, Heise-Verlag, 28.12.2002, www.heise.de/ tp/ deutsch/ inhalt/ te/ 13870/ 1.html.

wirklichen Straftäter den Internet-Zugangscode der festgenommenen Personen ohne deren Kenntnis missbraucht hatten.[110]

Zu Unrecht ins Visier der deutschen Kriminalpolizei ist ein 63-jähriger Mann aus Nürnberg geraten.[111] Er war angezeigt worden, da von seinem Internetanschluss aus kostenpflichtige Erotikseiten besucht wurden, ohne die angefallenen Kosten hierfür zu bezahlen. Das Fachdezernat der Kriminalpolizei konnte anhand der hinterlassenen „Internetspuren" (IP-Adressen) den 63-Jährigen als verantwortlichen Anschlussinhaber ermitteln. Der überraschte Mann versicherte jedoch, derartige Seiten niemals besucht zu haben. Durch weitere Ermittlungen kam man schließlich dem eigentlichen Täter auf die Spur. Er hatte den Internetzugang des zu Unrecht Verdächtigen über Funknetz (WLAN) genutzt.

Aufgrund des begrenzten Aussagegehalts von Telekommunikationsdaten und der Tatsache, dass der Zugriff auf Kommunikationsdaten oft eine Vielzahl von Personen betrifft, birgt der Zugriff auf Kommunikationsdaten ein besonderes Risiko falscher Verdächtigungen. Mithilfe von § 5 BSIG kann der Staat Kommunikations- und Interessenprofile erstellen und daraus falsche Verdachtsmomente zulasten unbescholtener Bürger ableiten. Weil § 5 BSIG eine ungleich umfangreichere Speicherung von Kommunikationsdaten als bisher zur Folge hat, ist davon auszugehen, dass auch die Anzahl der Zugriffe auf Kommunikationsdaten erheblich steigt. Damit erhöht sich auch das Risiko von Fehlentscheidungen in strafrechtlichen Ermittlungs- und Gerichtsverfahren.

(bb) Risiko von Datenpannen und des Missbrauchs durch Private

Die Aufzeichnung und Vorhaltung von Informationen über die Kommunikation und Internetnutzung der gesamten Bevölkerung schafft zudem unvermeidbare Risiken eines gesetzwidrigen Missbrauchs dieser Informationen. Dies zeigen die Erfahrungen der Vergangenheit:

2005-2007 veranlassten die polnische Polizei und zwei große Geheimdienste, dass die Kommunikationsdaten von mindestens 10 Journalisten gespeichert werden, um deren Quellen aufzudecken. Der Zugriff auf die Daten durch Polizei und Geheimdienste erfolgte ohne gerichtlichen Beschluss oder eine andere Legitimierung, und die Ermittlungen waren nicht Teil eines laufenden Verfahrens.[112]

---

[110] Kronqvist, Stefan (Leiter der IT-Kriminalitätsgruppe der nationalen schwedischen Strafverfolgungsbehörde): Submission to the European Commission for the Public Hearing on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, europa.eu.int/ ISPO/ eif/ InternetPoliciesSite/ Crime/ PublicHearingPresentations/ Kronqvist.html.

[111] Polizeipräsidium Mittelfranken, Zu Unrecht verdächtigt, 29.12.2006, http:// www.presseportal.de/ polizeipresse/ p_story.htx?nr=920697.

[112] The News.pl, Journalists' phones monitored in politically inspired investigation?, 8 October 2010, http://www.thenews.pl/1/9/Artykul/5241,Journalists-phones-monitored-in-politically-inspired-investigation.

Ein Mitarbeiter des deutschen Bundesnachrichtendienstes, der mit der Überwachung der elektronischen Kommunikation betraut war, nutzte 2007 seine technischen Möglichkeiten privat. Er spähte den Email-Verkehr eines Deutschen aus, weil dieser ein Verhältnis mit der Ehefrau des BND-Mitarbeiters hatte.[113]

Ein tschechischer Polizist fragte 2009 und 2010 im Auftrag einer privaten Sicherheitsfirma und politischer Kreise illegal Handy-Verbindungsdaten und Standortdaten über Personen des öffentlichen Lebens ab. Die Liste der so Ausspionierten umfasste den Vorsitzenden des tschechischen Verfassungsgerichtes, Journalisten zweier Tageszeitungen, Geschäftsleute aus der Sicherheits-, Energie- und Rüstungsbranche sowie mehrere Spitzenpolitiker verschiedener Parteien – darunter Vertraute von Staatspräsident Václav Klaus.[114]

Eine 40-jährige irische Polizeibeamtin wurde 2010 versetzt, weil sie nach der Trennung von ihrem Exfreund unter Missbrauch ihres Amtes dessen Telefon-Verbindungs- und Standortdaten abgerufen haben soll, um ihm hinterherzuspionieren.[115] Die Beamtin war in der für Terrorismus und organisierte Kriminalität zuständigen Abteilung der Zentrale der irischen Polizei für Telekommunikationsüberwachung zuständig.

In Großbritannien wurden 2007-2010 über 900 Disziplinarverfahren gegen Polizist/innen wegen des Verdachts der Verletzung des Datenschutzgesetzes geführt. 243 Beamte und Mitarbeiter der Polizei wurden wegen Datenschutzverletzungen strafrechtlich verurteilt, 98 wurden entlassen. Der Grund dafür war meist der Abruf polizeilicher Daten zu privaten Zwecken. Beispielsweise wurden polizeiliche Daten verwendet, um einem potenziellen Partner belästigende Nachrichten zu senden. Ausgeforscht wurden auch Exfrauen, Nachbarn und Arbeitskollegen von Polizist/innen.[116]

In Frankreich wertete der Inlandsgemeimdienst DCRI Verbindungsdaten aus, um die Quellen von Journalisten offenzulegen.[117] Zuvor hatte ein Staatsanwalt die Verbindungsdaten einer Richterin ausgewertet, um die Quellen investigativer Journalisten der Zeitung „Le Monde“ aufzudecken[118] – wiederum eine Verletzung des Quellenschutzes, wie ein Gericht später feststellte.[119]

---

[113] http://www.berliner-zeitung.de/archiv/bka-reform---das-bundeskriminalamt-soll-per-gesetz-mehr-befugnisse-bei-der-terrorabwehr-bekommen--neue-fahndungsmethoden-sollen-die-jagd-auf-staatsfeinde-erleichtern--beamter-unter-verdacht,10810590,10501420.html.

[114] http://www.pragerzeitung.cz/?c_id=17621.

[115] http://www.webcitation.org/5xTUKdNqb.

[116] http://www.bigbrotherwatch.org.uk/Police_databases.pdf.

[117] http://www.sueddeutsche.de/medien/poltische-affaeren-erschuettern-frankreich-staatsspionage-gegen-journalisten-1.1144365.

[118] http://www.oe24.at/welt/Sarkozy-droht-Spitzelaffaere/6900740.

[119] http://www.franceinfo.fr/france-justice-police-2011-05-06-affaire-woerth-bettencourt-l-enquete-du-procureur-courroye-sur-la-534584-9-11.html.

Daneben gab es zahllose Abhörskandale auch in Griechenland, Großbritannien, Italien, Portugal, der Slowakei und Slowenien.

Einen wirksamen Schutz vor Missbrauch ermöglicht alleine die Unterbindung der Protokollierung des Informations- und Kommunikationsverhaltens entsprechend dem Gebot der Datensparsamkeit.[120] Nur nicht gespeicherte Daten sind sichere Daten. § 5 BSIG stellt diese Erkenntnis auf den Kopf und ist deshalb mit dem Wesen des Art. 8 EMRK unvereinbar.

(cc) Abschreckungswirkung

Da mit der zwingenden Aufzeichnung des elektronischen Kommunikations- und Informationsverhaltens notwendig das Risiko verbunden ist, dass dem Betroffenen aus dem Bekanntwerden seiner Kontakte und Interessen Nachteile entstehen können, entfaltet § 5 BSIG eine Abschreckungswirkung. Die Vorratsdatenspeicherung hält in bestimmten Situationen davon ab, das Internet zu nutzen. Dies hat teilweise schwere Nachteile für Einzelpersonen und für unsere Gesellschaft insgesamt zur Folge. Dies belegen die deutschen Erfahrungen mit der Vorratsspeicherung von Kommunikationsdaten bei Telekommunikationsunternehmen.

Nach Umsetzung der Richtlinie 2006/24/EG zur Vorratsdatenspeicherung berichteten viele Menschen der Bürgerrechtsorganisation Arbeitskreis Vorratsdatenspeicherung, dass sie seit Inkrafttreten der Vorratsdatenspeicherung ihr Handy, E-Mail oder Internet seltener nutzen oder dass sie in ihrem privaten Umfeld solche Einschränkungen erleben. Amina R. aus Niedersachsen teilt beispielsweise mit, sie schränke sich stark in der E-Mail-Kommunikation mit ihrer Familie in Marokko ein, weil sie befürchtet, durch ihre Kontakte in diesen Staat verdächtig zu erscheinen. Anna T. (Name geändert) ist Opfer sexuellen Missbrauchs und tauschte sich früher in entsprechenden Foren und Chatrooms aus. Seit anhand ihrer IP-Adresse ihre Identität ermittelt werden konnte, zog sie sich aus diesem Austausch zurück und hatte somit keine Möglichkeit mehr, sich mit anderen anonymen Opfern auszutauschen. In dieselbe Sitiuation versetzt § 5 BSIG Angehörige von Bundesorganen, die bislang an ihrem Arbeitsplatz Selbsthilfeangebote nutzten.

Eine Vorratsdatenspeicherung schreckt weiters Informanten davon ab, vertrauliche Informationen an die Presse weiterzugeben, weil ihr Kontakt und ihre Identität anhand der Telekommunikationsdaten nachvollzogen werden kann. Ohne solche Informationen kann die Presse öffentliche Missstände nicht aufdecken und ihrer Kontrollfunktion gegenüber dem Staat nicht mehr nachkommen. Die Rundfunkjournalistin Hilde W. aus Thüringen schrieb dem Arbeitskreis Vorratsdatenspeicherung, sie recherchiere die Unterbringung von Flüchtlingen und Asylbewerbern in Thüringen, habe aber seit Inkrafttreten der Vorratsdatenspeicherung nach § 113a TKG Probleme, telefonisch oder per E-Mail Auskunft über sensible Daten wie illegale Flüchtlinge, Namen und Adressen zu erhalten. Der Journalist Gerrit W.

---

[120] Gola/Klug/Reif, Datenschutz- und presserechtliche Bewertung der „Vorratsdatenspeicherung“ (2007), 38; Rusteberg, VBlBW 2007, 171 (175).

aus Nordrhein-Westfalen befasst sich im Rahmen seiner Arbeit unter anderem mit Menschenrechtsverletzungen der EU-Agentur Frontex. Schon in den ersten Wochen nach Inkrafttreten der Vorratsdatenspeicherung nach § 113a TKG lehnten zwei Kontaktpersonen den Informationsaustausch via E-Mail ab. Der freiberufliche Journalist Peter H. aus Hessen schreibt, seit Inkrafttreten der Vorratsdatenspeicherung nach § 113a TKG sei die Kommunikation mit Informanten aus Firmen, Behörden, Parteien, Stadtverwaltungen und sonstigen Institutionen erschwert, teilweise auch unmöglich geworden. Auch § 5 BSIG führt zur Erfassung und Auswertung sämtlicher computergestützter Kontakte zwischen Presse und Bundesangehörigen über das Bundesnetz. Er untergräbt dadurch den Schutz journalistischer Quellen und beschädigt die Pressefreiheit.

Kommunikationsstörungen sind auch im Bereich der wirtschaftlichen und rechtlichen Beratung die Folge einer Vorratsdatenspeicherung, wo oftmals schon der Kontakt zu einem – möglicherweise auf ein bestimmtes Gebiet wie Steuerstrafrecht spezialisierten – Berater vertraulich bleiben muss. So stellte der Steuerberater Matthias M. aus Baden-Württemberg bei einigen Mandanten fest, dass sie den Weg der Kommunikation über das Telefon nach Inkrafttreten der Vorratsdatenspeicherung nach § 113a TKG scheuten. Dies hielt er für sehr bedenklich, weil in der Vergangenheit immer wieder der Fall eingetreten war, dass Mandanten angefragt haben, ob diese oder jene steuerliche Gestaltung noch mit dem Steuerrecht konform ist. Solche Fälle konnte Herr M. häufig telefonisch mit einem kurzen Ja oder Nein beantworten und dem Mandant aufzeigen, dass es immer besser ist, auf dem ‚Pfad der Tugend' zu bleiben. Seine Befürchtung war, dass es Mandanten zu kompliziert oder zeitaufwendig wird, derartige Dinge jedes Mal persönlich zu klären und somit auch schneller der Fall eintreten kann, dass sich die Mandanten mangels Beratung strafbar machen. Der Rechtsanwalt und Notar Dr. Engelbert S. aus Hessen hat wegen der Vorratsdatenspeicherung nach § 113a TKG Mandanten ernsthaft davor gewarnt, durch Telefon, Fax oder E-Mail mit ihm Kontakt aufzunehmen oder Schriftstücke zu übermitteln. Dies habe zu einem Rückgang von Anfragen geführt, weil persönliche Besuche mit höherem Aufwand verbunden sind. Der Wirtschafts- und Finanzberater Jens-Oliver W. berichtet, nach Inkrafttreten der Vorratsdatenspeicherung nach § 113a TKG sei mit einigen Mandanten eine telefonische Kommunikation nicht mehr möglich gewesen. Vermutlich werde er diese Mandanten nicht mehr betreuen können, da die Wege- und Zeitaufwandskosten in keinem Verhältnis mehr zum Verdienst stehen. § 5 BSIG zieht dieselben Nachteile nach sich, etwa wo Angehörige von Bundesorganen nicht mehr am Arbeitsplatz wirtschaftliche und rechtliche Beratung über das Internet ohne Furcht vor Rückverfolgung in Anspruch nehmen können.

Der Betriebsrat Joachim B. aus Bayern berichtete, dass sich Mitarbeiter nach Inkrafttreten des § 113a TKG nicht mehr per E-Mail an ihn wendeten, obwohl einige arbeitsrechtlich relevante Fälle möglichst unverzüglich geklärt werden müssten. Von § 5 BSIG gehen ähnliche Wirkungen auf die Arbeit von Personalräten aus.

Torsten T. aus Hessen ist Firmeninhaber und schaltete sein Mobiltelefon nach Inkrafttreten der Vorratsdatenspeicherung ab, weil er befürchtete, mit Straftaten in Verbindung gebracht zu werden, in deren Nähe er zufällig telefoniert hat. Die Deaktivierung des Mobiltelefons schade ihm jedoch wirtschaftlich. Ein ähnlicher Schaden geht von § 5 BSIG aus, wo Bundesbedienstete auf elektronische Kommunikation möglichst verzichten, um nicht erfasst zu werden.

Schließlich sind Menschen in besonderen Situationen (z.B. Notlagen, Krankheiten) zur Suche nach Informationen, zur Inanspruchnahme von Beratung und Hilfe sowie zum Austausch untereinander (z.B. Chatrooms für Opfer sexuellen Missbrauchs) nur bereit, wenn dies anonym und nicht rückverfolgbar möglich ist. Oftmals lässt sich bereits aus dem Kontakt zu einer bestimmten Beratungsstelle oder zu einem bestimmten Arzt auf die zugrunde liegende Erkrankung, Abhängigkeit o.ä. schließen. Der Sozialpädagoge und Suchtberater Konstantin H. aus Schleswig-Holstein berichtete, in der niedrigschwelligen Arbeit mit Drogenabhängigen sei die Zahl der telefonischen Kontakte seit dem 1.1.2008 und der damit in Deutschland einsetzenden Vorratsdatenspeicherung „stark zurückgegangen". Die Abhängigen fürchteten eine Strafverfolgung. Durch die Personalstruktur in der Beratungsstelle – ein Berater müsse 200 Klienten betreuen – sei eine andere als telefonische Beratung oft nicht möglich; zudem bedürften die Klienten aufgrund von Begleiterkrankungen wie Hepatitis oftmals akuter medizinischer Behandlung. Der Rückgang der telefonischen Beratungsanfragen könne den Gesundheitszustand der Betroffenen sehr verschlechtern. Der Facharzt Achim R., der in einem Berliner Klinikum arbeitet, berichtete von mehreren Patienten, die nach Inkrafttreten der Vorratsdatenspeicherung nach § 113a TKG von telefonischen Kontaktaufnahmen zwecks Beratung abgesehen hätten, wodurch medizinisch gefährliche Verzögerungen des Therapiebeginns entstanden seien. Beispielsweise habe sich die Behandlung einer Tumorerkrankung verzögert und sei der Tumor in der Zwischenzeit weiter gewachsen. Die Psychotherapeutin Cornelia P. aus Baden-Württemberg hat im Monat nach Inkrafttreten der Vorratsdatenspeicherung nahezu keine Anfragen per E-Mail oder Telefon nach Paartherapie, Eheberatung und Psychotherapie mehr erhalten. § 5 BSIG macht es Angehörigen von Bundesorganen in besonderen Situationen (z.B. Notlagen, Krankheiten) unmöglich, ohne Furcht vor Bekanntwerden ihrer Situation im Internet nach Informationen zu suchen, Beratung und Hilfe in Anspruch zu nehmen oder sich mit anderen Menschen in ähnlicher Situation auszutauschen (z.B. Chatrooms für Opfer sexuellen Missbrauchs). Auch der Bund selbst bietet Menschen in besonderen Situationen (z.B. Notlagen, Krankheiten) Informationen, Beratung und Hilfe im Internet an, die wegen § 5 BSIG jedoch nicht mehr ohne das Risiko eines Bekanntwerdens in Anspruch genommen werden kann.

Regierungsbehörden (z.B. Nachrichtendienste) kommunizieren im Übrigen anonym, um im Internet recherchieren zu können, ohne als Regierungsbehörde identifizierbar zu sein. Zugleich sind Behörden darauf angewiesen, dass Menschen Straftaten anonym anzeigen

können, die andernfalls nicht gemeldet würden und unaufgeklärt blieben. Dies gilt für die anonyme Offenlegung verschiedenster Missstände wie Steuerhinterziehung oder Korruption (sogenanntes „Whistleblowing“). All dies erschwert oder vereitelt § 5 BSIG.

(dd) Meinungsumfragen belegen Abschreckungswirkung

Um einen repräsentativen Überblick über die Auswirkungen einer generellen und undifferenzierten Vorratsdatenspeicherung aller Verbindungsdaten zu gewinnen, ist eine repräsentative Umfrage des Meinungsforschungsinstituts Forsa unter 1.002 Bundesbürgern am 27./28. Mai 2008 in Auftrag gegeben worden.[121] Dem Umfrageergebnis zufolge würde die Mehrheit der Befragten wegen der damals praktizierten Vorratsdatenspeicherung davon absehen, per Telefon, E-Mail oder Handy Kontakt zu einer Eheberatungsstelle, einem Psychotherapeuten oder einer Drogenberatungsstelle aufzunehmen, wenn sie deren Rat benötigten (517 der Befragten). Hochgerechnet entspricht dies über 43 Mio. Deutschen. Jede dreizehnte Person gab an, wegen der Verbindungsdatenspeicherung bereits mindestens einmal darauf verzichtet zu haben, Telefon, Handy oder E-Mail zu benutzen (79 der Befragten). Hochgerechnet entspricht dies 6,5 Mio. Deutschen. Jede sechzehnte Person hatte den Eindruck, dass andere Menschen seit Beginn der Vorratsdatenspeicherung seltener per Telefon, Handy oder E-Mail Kontakt mit ihr aufnehmen (62 der Befragten). Hochgerechnet entspricht dies 5 Mio. Deutschen. Besonders stark war die Veränderung des Kommunikationsverhaltens unter Menschen mit geringem Bildungsniveau (Haupt- oder Grundschulabschluss).

Des weiteren gab der Deutsche Fachjournalistenverband eine Online-Befragung (Vollerhebung) freier Journalisten in Auftrag, die vom 8. bis 27. April 2008 durchgeführt wurde.[122] Es nahmen 1.630 freie Journalisten teil. Jeder vierzehnte Journalist erklärte, die Vorratsdatenspeicherung nach § 113a TKG habe sich bereits negativ auf die Kommunikation mit seinen Informanten ausgewirkt. Jeder fünfte hielt abschreckende Auswirkungen der Vorratsdatenspeicherung zumindest für möglich.[123]

Die genannten Umfragen weisen nach, dass bereits von einer generellen und undifferenzierten Vorratsdatenspeicherung und dem ihr inhärenten Risiko einer Offenlegung oder Auswertung der protokollierten Informationen schwere Nachteile ausgehen, unabhängig von der Frage, ob auf die Daten später tatsächlich zugegriffen wird oder nicht. Viele Menschen können wegen § 5 BSIG in bestimmten Situationen bereits auf elektronische Kontaktaufnahmen verzichtet haben, weil sie etwaige Nachteile infolge der Protokollierung des Kontakts nicht verhindern können. Tausende von Journalisten und Berufsgeheimnisträger werden in ihrer beruflichen Tätigkeit durch die globale Protokollierung sämtlicher elektroni-

---

[121] http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf.

[122] Meyen/Springer/Pfaff-Rüdiger, Freie Journalisten in Deutschland, http://www.dfjv.de/ fileadmin/ user_upload/ pdf/ DFJV_Studie_Freie_Journalisten.pdf.

[123] a.a.O., 22.

scher Kontakte mit Angehörigen und Mitarbeitern von Bundesorganen gestört. Jede zweite Person würde im Fall der Hilfsbedürftigkeit keine elektronische Hilfe über das Bundesnetz mehr in Anspruch nehmen. Es liegt auf der Hand, dass in vielen dieser Fälle auch eine persönliche Kontaktaufnahme zu einer Hilfseinrichtung unterbleiben wird und dass daraus – etwa in Fällen von Gewaltproblemen – Gesundheits- und Lebensgefahren für die Betroffenen und ihre Mitmenschen erwachsen können.

Im Fall S. und Marper argumentierte der EGMR, die Vorratsspeicherung biometrischer Daten sei im Fall besonderer Personengruppen besonders schädlich, nämlich im Fall von Minderjährigen.[124] Wie oben gezeigt, ist auch die Vorratsspeicherung von Kommunikationsdaten für bestimmte Personengruppen besonders schädlich.

(ee) Bedeutung von Anonymität für unsere Gesellschaft

Gary Marx nennt insgesamt 15 Funktionen von Anonymität in unserer Gesellschaft,[125] welche § 5 BSIG beeinträchtigt:

- Erleichterung des Informations- und Kommunikationsflusses über öffentliche Angelegenheiten durch Schutz des Informationsgebers (z.B. Hotlines zur anonymen Anzeige von Problemen oder Verstößen durch Whistle Blower, anonyme Informanten der Presse).
- Ermöglichung der wissenschaftlichen Erforschung von Sachverhalten, über die nur im Schutz der Anonymität Auskunft gegeben wird (z.B. Telefonstudien über Sexualverhalten, strafbares Verhalten, Gesundheit).
- Zu verhindern, dass die Offenlegung des Urhebers einer Nachricht die Wahrnehmung ihres Inhalts verhindert oder beeinflusst (z.B. wegen Vorurteilen gegen den Autor).
- Förderung des Meldens, Informierens, Kommunizierens, Austauschs und der Selbsthilfe im Hinblick auf Zustände oder Handlungen, die stigmatisieren, nachteilig sind oder intim (z.B. Hilfe für und Austausch der Betroffenen von Drogenmissbrauch, Gewalt in der Familie, abweichender sexueller Identität, psychischer oder physischer Krankheiten, AIDS oder anderer Sexualkrankheiten, Schwangerschaft; Kauf von Verhütungsmitteln, Medikamenten oder bestimmten Magazinen).
- Ermöglichung von Hilfe trotz Strafbarkeit oder gesellschaftlicher Verachtung (z.B. anonyme Beratung von Drogenabhängigen, anwaltliche Beratung von Beschuldigten).
- Schutz der Unterstützer unbeliebter Handlungen vor Verpflichtungen, Forderungen, Vorverurteilung, Verwicklungen oder Rache (z.B. Schutz der Identität verdeckter Ermittler oder von Polizist/innen oder von Menschenrechtsorganisationen).

---

[124] EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 124.

[125] Marx, What's in a Name? Some Reflections on the Sociology of Anonymity (1999), http://web.mit.edu/gtmarx/www/anon.html.

- Wahrnehmung wirtschaftlicher Interessen durch Einschaltung von Mittelsmännern/-frauen, um zu vermeiden, dass der Hintergrund einer geschäftlichen Transaktion bekannt wird (z.B. anonyme Testkäufe, anonyme Versteigerungen).
- Schutz der eigenen Zeit, des eigenen Raums und der eigenen Person vor unerwünschtem Eindringen (z.B. durch Stalker, Fans oder Werbetreibende).
- Dafür zu sorgen, dass Entscheidungen ohne Ansehung der Person getroffen werden (z.B. anonyme Bewerbung).
- Schutz der eigenen Reputation und Ressourcen vor Identitätsdiebstahl (Handeln anderer unter dem eigenen Namen).
- Verfolgten Personen die sichere Teilnahme am öffentlichen Leben ermöglichen (z.B. sich illegal aufhaltende Flüchtlinge).
- Durchführung von Ritualen, Spielen und Feiern, welche das Verbergen der eigenen Identität oder das Annehmen einer fremden Identität zum Gegenstand haben und denen eine förderliche Wirkung auf die Persönlichkeitsentwicklung und psychische Gesundheit zugeschrieben wird (z.B. Rollenspiele).
- Förderung des Experimentierens und Eingehens von Risiken ohne Furcht vor Konsequenzen, Scheitern oder Gesichtsverlust (z.B. Auftreten unter dem anderen Geschlecht in einem Chatroom).
- Schutz der eigenen Persönlichkeit, weil die eigene Identität andere schlichtweg nichts angeht.
- Erfüllung traditioneller Erwartungen (z.B. die traditionelle Möglichkeit, nicht rückverfolgbare und anonyme Briefe schreiben zu können).

In all diesen Situationen kann eine freie, unbefangene und in allem vertrauliche Kommunikation nur im Schutz fehlender Rückverfolgbarkeit erfolgen und verhindert § 5 BSIG das Gebrauchmachen von grundrechtlich geschützten Freiheiten.

(d) Verletzung der Unschuldsvermutung

Im Fall S. und Marper leitete der EGMR aus dem Grundgedanken der Unschuldsvermutung ab, dass Nichtverurteilte einen Anspruch darauf hätten, nicht ebenso wie verurteilte Straftäter behandelt zu werden. In einer solchen Gleichbehandlung von Ungleichem liege eine Stigmatisierung der Betroffenen.[126]

Dasselbe gilt für § 5 BSIG. Nach dieser Vorschrift wird nicht nur das Kommunikationsverhalten Verdächtiger aufgezeichnet und ausgewertet, sondern sogar das Kommunikationsverhalten gänzlich Unverdächtiger und Unbeteiligter. Rechtschaffene Bürger haben aber einen Anspruch darauf, nicht allesamt wie potenziell Verdächtige einer Straftat behandelt

[126] EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, Abs. 122.

zu werden. Nur bei dem Verdacht einer Straftat darf der Staat die Aufzeichnung von Informationen über die Telekommunikation einer Person anordnen.

(e) Weitere Rechtsprechung

Im Jahr 2007 hat der EGMR ausdrücklich entschieden, dass die Sammlung der Verkehrsdaten von Arbeitnehmern des öffentlichen Dienstes nur „in bestimmten Situationen" notwendig sein kann[127], also keinesfalls permanent, global und pauschal, wie es Gegenstand von § 5 BSIG ist.

Das deutsche Bundesarbeitsgericht hat zur Aufzeichnung des Verhaltens von Arbeitnehmern per Videoüberwachung entschieden,[128] dass eine Aufzeichnung nur bei Vorliegen eines auf konkrete Personen bezogenen Verdachts einer strafbaren Handlung verhältnismäßig sei und dann auch nur die konkret verdächtigen Personen erfasst werden dürften. Sobald der Täter oder die Täterin ermittelt sei, sei die Aufzeichnung unverzüglich einzustellen, spätestens jedoch nach vier Wochen. – § 5 BSIG hat eine Aufzeichnung des Verhaltens von Bediensteten und Angehörigen des Bundes zum Gegenstand, und zwar ihrer E-Mail-Kommunikation und Internetnutzung. § 5 BSIG beschränkt die Aufzeichnung aber nicht auf Fälle eines auf konkrete Personen bezogenen Verdachts einer strafbaren Handlung (einschließlich Computerdelikten) und auf die konkret verdächtigen Personen, wie es aus Verhältnismäßigkeitsgründen geboten wäre.

Nach der Rechtsprechung des Bundesverfassungsgerichts können auf eine Norm, welche die Erhebung personenbezogener Daten lediglich durch das Gebot der Erforderlichkeit zur Erfüllung bestimmter Aufgaben begrenzt, keine Grundrechtseingriffe von erheblichem Gewicht gestützt werden.[129] § 5 BSIG ermächtigt zu tiefgreifenden Grundrechtseingriffen, begrenzt die Erhebung personenbezogener Daten aber lediglich durch das Gebot der Erforderlichkeit zur Erfüllung bestimmter Aufgaben. Dies genügt dem Verhältnismäßigkeitsgebot nicht.

Das Bundesverfassungsgericht hat weiter entschieden, dass allgemein gesteigerte Risiken von Rechtsgutgefährdungen oder –verletzungen („allgemeine Bedrohungslage") Grundrechtseingriffe von erheblichem Gewicht nicht rechtfertigen, sondern „eine konkrete Gefahr für hochrangige Rechtsgüter" gegeben sein muss.[130] Eine allgemeine Bedrohungslage, deren Realisierung „praktisch nie ausgeschlossen" ist, genügt dem nicht.[131] Zur Begründung führte das Gericht aus, die Befugnis zur Rasterfahndung gleiche den zu Zwecken der strategischen Kontrolle vorgenommenen Eingriffen in das Fernmeldegeheimnis insofern,

---

[127] EGMR, Copland-UK (2007), MMR 2007, 431 (432), Abs. 48.

[128] BAGE 127, 276.

[129] *BVerfG*, NVwZ 2007, 688, Abs. 53 f.

[130] BVerfGE 115, 320 (320), Ls. 1.

[131] BVerfGE 115, 320 (364).

als auch sie verdachtslos erfolgende Grundrechtseingriffe in großer Streubreite vorsehe.[132] Auch § 5 BSIG sieht Grundrechtseingriffe in großer Streubreite vor, die ohne jeden Verdacht vorgenommen werden. Die Erfassung der näheren Umstände jeglicher elektronischer Kommunikation über Bundesnetze ist ein derart tiefgreifender Grundrechtseingriff, dass er – wie eine Rasterfahndung – allenfalls zur Abwehr einer konkreten Gefahr für hochrangige Rechtsgüter zulässig sein kann. Die Beseitigung möglicher Anlagenstörungen oder -fehler einer beliebigen informationstechnischen Anlage des Bundes – etwa des Computers eines Behördenmitarbeiters – stellt offenkundig kein wichtiges Rechtsgut dar, welches eine globale und pauschale Erfassung der näheren Umstände sämtlicher Kommunikation mit Bundesorganen rechtfertigen könnte.

Im Jahr 2008 urteilte das deutsche Bundesverfassungsgericht, dass die automatisierte flächendeckende und anlasslose Erhebung der Kennzeichen von Kraftfahrzeugen selbst dann unverhältnismäßig ist, wenn die Daten nur mit Fahnungsausschreibungen abgeglichen und, wenn das Kennzeichen nicht zur Fahndung ausgeschrieben ist, ohne menschliche Kenntnisnahme sofort wieder gelöscht werden.[133] Hiervon ausgehend ist offensichtlich, dass die von § 5 BSIG angeordnete Erfassung, Auswertung und Vorratsdatenspeicherung als flächendeckende und anlasslose Maßnahme, deren Ergebnisse nicht sogleich wieder gelöscht werden, unverhältnismäßig ist. Im Vergleich zum Kraftfahrzeugverkehr ist unsere Fernkommunikation weitaus sensibler und schutzbedürftiger, wie oben gezeigt worden ist. Das Kommunikationsverhalten einer Person und ihr soziales Netzwerk lässt noch größere Rückschlüsse auf ihre Persönlichkeit zu als ihre Bewegungen.

Soweit das Bundesverfassungsgericht mit Urteil vom 2. März 2010 eine anlasslose, flächendeckende Vorratsdatenspeicherung unter bestimmten Voraussetzungen als verhältnismäßig bezeichnet hat, kann dies nicht überzeugen. Dem Urteil fehlt eine Auseinandersetzung mit den empirischen Nachweisen des eklatanten Missverhältnisses zwischen Tragweite einer Vorratsdatenspeicherung auf der einen und ihrem Ertrag auf der anderen Seite. Auch fehlt eine Auseinandersetzung mit den Belegen für die ebenso hohe Aufklärungsrate ohne Vorratsdatenspeicherung. Das Urteil setzte sich ferner nicht mit der Europäischen Menschenrechtskonvention und der diesbezüglichen Rechtsprechung des EGMR[134] und des Verfassungsgerichtshofs Rumäniens[135] auseinander, obwohl das Grundgesetz nach Möglichkeit konventionskonform auszulegen ist.[136] Dem Urteil fehlt auch eine Auseinandersetzung mit der früheren Rechtsprechung des Bundesverfassungs-

[132] BVerfGE 115, 320 (359).

[133] BVerfG, Urteil vom 11.03.2008, Az. 1 BvR 2074/05 und 1 BvR 1254/07, http://www.bverfg.de/entscheidungen/rs20080311_1bvr207405.html.

[134] EGMR, S. und Marper-GB vom 04.12.2008, 30562/04 und 30566/04, NJOZ 2010, 696.

[135] Verfassungsgerichtshof Rumäniens, 1258 vom 08.10.2009, http://www.vorratsdatenspeicherung.de/content/view/342/79/lang,de/.

[136] BVerfG, 2 BvR 1481/04 vom 14.10.2004, Absatz-Nr. 32.

gerichts, mit welcher eine allumfassende, permanente Vorratsdatenspeicherung nicht in Einklang zu bringen ist.[137] Die Entscheidung ist dementsprechend vom Bundesdatenschutzbeauftragten[138] und in der Literatur[139] kritisiert worden. Eine inhaltliche Widerlegung der Argumente des Bundesverfassungsgerichts ist bereits an anderer Stelle erfolgt, worauf verwiesen werden kann.[140] Es bleibt anzumerken, dass das Bundesverfassungsgericht seine Rechtsprechung bereits in anderen Fällen im Hinblick auf ein höheres europäisches Grundrechtsschutzniveau korrigieren musste.[141]

Selbst wenn man die Maßstäbe des Bundesverfassungsgerichtsurteils vom 02.03.2010 zugrunde legen wollte, würde § 5 BSIG diesen Anforderungen im Übrigen nicht gerecht. Das Bundesverfassungsgericht hat in seiner Entscheidung vom 2.3.2010 zur Vorratsdatenspeicherung betont, dass die Zulässigkeit der vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten aufgrund der EG-Richtlinie zur Vorratsdatenspeicherung eine Ausnahme bleiben müsse.[142] Die in § 5 BSIG vorgesehene Protokollierung ist in der EG-Richtlinie nicht vorgesehen und sprengt deren Ausnahmecharakter. Maßgeblich für die Rechtfertigungsfähigkeit einer Vorratsdatenspeicherung soll laut Bundesverfassungsgericht insbesondere sein, dass die Datenspeicherung nicht direkt durch staatliche Stellen erfolge, dass sie nicht auch die Kommunikationsinhalte erfasse und dass auch die Speicherung der aufgerufenen Internetseiten grundsätzlich untersagt sei.[143] Die in § 5 BSIG vorgesehene Speicherung erfolgt demgegenüber direkt durch staatliche Stellen und umfasst gerade auch die Speicherung jeder abgerufenen Internetseite, also den Inhalt der Kommunikation. In seiner Entscheidung hat das Bundesverfassungsgericht maßgeblich darauf abgestellt, dass die §§ 11 ff. TMG die Diensteanbieter nach dem Telemediengesetz grundsätzlich zur Löschung von nicht für die Abrechnung erforderlichen Daten verpflichteten (vgl. § 13 Abs. 4 Nr. 2, § 15 TMG) und so verhinderten, dass die Internetnutzung inhaltlich festgehalten werde und damit rekonstruierbar bleibe.[144] Im Bereich der vielen Telemedien des Bundes beseitigt § 5 BSIG nun aber gerade diese Löschungspflichten des TMG und zielt umgekehrt darauf ab, dass die Nutzung dieser Internetangebote inhaltlich festgehalten wird und damit rekonstruierbar gemacht wird. Dem Bundesverfassungsgericht zufolge ist eine Gesetzgebung, die auf eine möglichst flächendeckende vorsorgliche Spei-

---

[137] Näher Schriftsatz vom 13.08.2008 im Verfahren 1 BvR 256/08, http://www.vorratsdatenspeicherung.de/images/schriftsatz_2008-08-13.pdf, 33.

[138] http://www.daten-speicherung.de/index.php/ziercke-greift-ak-vorrat-an/.

[139] Forgó/Grügel, K&R 2010, 218 ff.

[140] Schriftsatz vom 12.08.2010 im Verfahren 1 BvR 1299/05, http://daten-speicherung.de/data/TKG-Verfassungsbeschwerde_Schriftsatz_2010-08-12.pdf, 4 ff.

[141] BverfG NJW 2008, 1793 – Caroline II; BVerfG NJW 2011, 1931 – Sicherungsverwahrung II.

[142] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 218.

[143] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 218.

[144] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 270.

cherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielt, mit den Grundrechten unvereinbar.[145]

Anders als das Bundesverfassungsgericht hat der rumänische Verfassungsgerichtshof die Europäische Menschenrechtskonvention zum Maßstab seiner Prüfung eines Gesetzes zur Vorratsdatenspeicherung gemacht und eine Verletzung des Art. 8 EMRK festgestellt. Der Gerichtshof führte in der Begründung seines Urteils vom 08.10.2009 aus, dass das Gesetz zur Vorratsdatenspeicherung die in der Strafprozessordnung vorgesehenen Ausnahmen vom Fernmeldegeheimnis „zur Regel" mache. Im Fall einer Vorratsdatenspeicherung könne von Fernmeldegeheimnis und Meinungsfreiheit nicht mehr „frei und unzensiert Gebrauch gemacht werden". Eine allgemeine Vorratsdatenspeicherung wecke in den Menschen „die berechtigte Sorge um die Wahrung ihrer Privatsphäre und die Furcht vor einem möglichen Missbrauch". Die dauerhafte und die gesamte Bevölkerung betreffende Vorratsdatenspeicherung drohe die Unschuldsvermutung „auszuhebeln", erkläre die gesamte Bevölkerung zu potenziellen Straftätern und erscheine „exzessiv". Die Erfassung aller Verbindungsdaten könne deshalb „nicht als vereinbar mit den Bestimmungen der Verfassung und der Europäischen Menschenrechtskonvention erachtet werden".[146]

Nach diesem Maßstab verletzt auch § 5 BSIG Art. 8 EMRK. § 5 BSIG macht die in bestimmten Ausnahmefällen gestattete Aufzeichnung, Auswertung und Vorratsdatenspeicherung zur Regel und führt dazu, dass von Fernmeldegeheimnis und Meinungsfreiheit über Bundesnetze nicht mehr frei und unzensiert Gebrauch gemacht werden kann. Die in § 5 BSIG gestattete allgemeine Aufzeichnung, Auswertung und Vorratsdatenspeicherung weckt in den Betroffenen die berechtigte Sorge um die Wahrung ihrer Privatsphäre und die Furcht vor einem möglichen Missbrauch. Die dauerhafte und potenziell die gesamte Bevölkerung betreffende Vorratsdatenspeicherung droht die Unschuldsvermutung auszuhebeln, erklärt die gesamte Bevölkerung zu einer potenziellen Gefahr für die IT-Sicherheit und ist exzessiv.

2011 hat sich dann auch der tschechische Verfassungsgerichtshof nicht überzeugt gezeigt, dass eine unterschiedslose und vorsorgliche Speicherung von Verkehrsdaten nahezu jeder elektronischer Kommunikation im Hinblick auf die Intensität des Eingriffs und die Vielzahl der privaten Nutzer elektronischer Kommunikation erforderlich und verhältnismäßig sei.[147] Der Verfassungsgerichtshof äußerte mit Blick auf die vielflätigen Umgehungsmöglichkeiten Zweifel daran, ob eine unterschiedslose und vorsorgliche Speicherung von Verkehrsdaten ein wirksames Mittel ist, um ihren ursprünglichen Zweck (Schutz vor Gefahren und Verhü-

[145] BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 218.

[146] Englische Urteilsübersetzung: http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html, deutsche Urteilsübersetzung: http://www.vorratsdatenspeicherung.de/content/view/342/1/lang,de/#Urteil.

tung besonders schwerer Straftaten) zu erreichen. Eine Analyse von Zahlen des deutschen Bundeskriminalamts habe zu dem Ergebnis geführt, dass die unterschiedslose und vorsorgliche Speicherung von Verkehrsdaten wenig Auswirkungen bei der Verringerung der Zahl der begangenen schweren Straftaten hatte. Auch bei § 5 BSIG besteht das Problem, dass sich Internetkennungen leicht fälschen und wechseln lassen. Es gibt keinen empirischen Nachweis dafür, dass fachgerecht gesicherte („gehärtete“) und unterhaltene IT-Systeme ohne anlasslose Aufzeichnung, Auswertung und Vorratsdatenspeicherung des gesamten Informations- und Kommunikationsverhaltens messbar häufiger oder länger unter Störungen der Verfügbarkeit, Vertraulichkeit oder Integrität litten als Systeme, die eine solche Totalprotokollierung und –auswertung vornehmen.

(f) Drohender Dammbruch

Wir bitten den Gerichtshof zu berücksichtigen, dass die Zulassung einer Vorratsdatenspeicherung im Fall des § 5 BSIG allgemein einen Dammbruch für den Schutz der Privatsphäre bedeuten würde. Die globale Speicherung von Daten allein für eine mögliche künftige staatliche Verwendung würde allmählich alle Lebensbereiche erfassen, denn die vorsorgliche Protokollierung personenbezogener Daten ist für den Staat stets und in allen Bereichen nützlich.[148] Aus jedem personenbezogenen Datum können sich im Einzelfall einmal Schlüsse bezüglich einer Gefahr oder Straftat ergeben. Das Grundrecht auf Achtung der Privatsphäre und das gesamte Datenschutzrecht beruhen indes auf dem Gedanken, dass nicht bereits die bloße Möglichkeit, dass ein Datum irgendwann in der Zukunft einmal gebraucht werden könnte, dessen Speicherung rechtfertigt, weil ansonsten sämtliche personenbezogene Daten unbegrenzt auf Vorrat gespeichert werden dürften. Dies aber wäre eine unverhältnismäßige und unangemessene Beeinträchtigung des Persönlichkeitsrechts der Betroffenen, denen aus der Aufbewahrung und späteren Verwendung personenbezogener Daten schwere Nachteile entstehen können.

Mit der Aufgabe des Verbots einer anlasslosen, permanenten oder flächendeckenden Speicherung personenbezogener Daten auf Vorrat würden letztlich das gesamte Grundrecht auf Datenschutz und ihm folgend das gesamte Datenschutzrecht obsolet. Denn die Grundidee des Datenschutzes liegt gerade darin, die informationelle Selbstbestimmung zum Regelfall und den staatlichen Eingriff gegen den Willen des Betroffenen zum Ausnahmefall zu definieren. Die Vorratsdatenspeicherung verkehrt die Grundidee der informationellen Selbstbestimmung in ihr Gegenteil.

Wenn eine flächendeckende Erfassung persönlicher Lebenssachverhalte ins Blaue hinein selbst bei der besonders sensiblen und geschützten Telekommunikation und Internetnutzung zulässig wäre, wäre sie auch überall sonst zulässig. Die Vorratsspeicherung von Te-

147 Urteil vom 22.03.2011, 24/10, englische Urteilsübersetzung: http://www.concourt.cz/clanek/pl-24-10, deutsche Urteilsübersetzung (Auszug): http://www.vorratsdatenspeicherung.de/content/view/437/79/lang,de/.

148 Klug/Reif, RDV 2008, 89 (93).

lefongesprächen, Bewegungen der Nutzer von Mobiltelefonen und Smartphones, Flugreisen und Nahverkehrsfahrten, von Fahrzeugbewegungen auf Autobahnen, von Aufzeichnungen privater Überwachungskameras, von Einkäufen in Geschäften und Ausleihvorgängen in Büchereien sind allesamt Beispiele einer Vorratsspeicherung, die in einigen Staaten geplant oder bereits realisiert sind und in Europa auch schrittweise eingeführt würden. Es drohte auch eine Totalerfassung von Schiffs- und Bahnreisen, des Brief- und Postverkehrs einschließlich der bestellten Zeitschriften und Zeitungen, der Stromnutzung und von Warenbestellungen. Dass dieses Szenario nicht imaginär ist, zeigen die unermesslichen „Data Warehouses" der USA, in denen schon heute über die gesamte Bevölkerung Telekommunikations-Verkehrsdaten,[149] Flugreisedaten,[150] Zahlungsverkehrsdaten[151] und Daten aus den verschiedensten privaten Datenbanken zusammen geführt werden.[152]

(5) Unverhältnismäßiges Erkennen und Beseitigen von Störungen und Fehlern (§ 5 Abs. 1 S. 1 Nr. 1 Var. 1 BSIG)

Im Einzelnen ergibt sich die Unverhältnismäßigkeit der Regelungen des § 5 BSIG aus folgenden Umständen:

§ 5 Abs. 1 S. 1 Nr. 1 BSIG ermächtigt das BSI, die näheren Umstände der elektronischen Kommunikation mit Bundesbehörden (§ 2 Abs. 8 BSIG) aufzuzeichnen und automatisiert auszuwerten, um Störungen und Fehler zu erkennen und zu beseitigen. Dies betrifft namentlich Verkehrsdaten über die computergestützte Kommunikation von und mit Bundesorganen und deren Mitglieder und Beschäftigte (z.B. per E-Mail, Internettelefonie oder Instant Messaging) sowie Daten über die Nutzung öffentlicher Telemedien von und durch Bundesorgane und deren Mitglieder und Beschäftigte (§ 2 Abs. 8 S. 2 BSIG).

§ 5 Abs. 1 S. 1 Nr. 1 BSIG ist schon deswegen zur Beseitigung der meisten Störungen ungeeignet, weil aus der Maßnahme gewonnene Erkenntnisse über Störungen oder Fehler nicht verwendet werden dürfen. Eine Verwendung der gewonnenen Erkenntnisse ist nach dem klaren Wortlaut des § 5 BSIG nur zulässig, wenn der Verdacht eines Schadprogramms besteht (§ 5 Abs. 1 und 3 BSIG). Erkenntnisse über Störungen oder Fehler, die auf anderen Ursachen beruhen, darf das BSI demnach nicht nutzen oder weiter geben. Da die vom BSI erhobenen Verkehrsdaten dem Fernmeldegeheimnis unterliegen, ist auch eine anonymisierte Weitergabe nicht zugelassen (vgl. § 5 Abs. 1 S. 3 BSIG).

---

[149] New York Times vom 24.12.2005, http://www.nytimes.com/2005/12/24/politics/24spy.html; USA Today vom 05.11.2006, http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

[150] Wikipedia-Eintrag „Automated Targeting System", http://en.wikipedia.org/wiki/Automated_Targeting_System.

[151] New York Times vom 23.06.2006, http://www.nytimes.com/2006/06/23/washington/23intel.html.

[152] Electronic Privacy Information Center, http://epic.org/privacy/choicepoint/.

(a) Kommunikationsverkehrsdaten

Nach der früheren Rechtslage war dem BSI die Aufzeichnung der näheren Umstände jeder Individualkommunikation mit Bundesbehörden und Bundesangehörigen nicht erlaubt.[153] Auch die Behörden des Bundes selbst durften Informationen über ein- und ausgehende Kommunikation bisher nur nach Maßgabe des Bundesdatenschutzgesetzes und des Mitbestimmungsrechts verarbeiten. Das Erstellen eines Verzeichnisses aller ein- und ausgehender Kommunikationsvorgänge war nach § 13 Abs. 1 BDSG unzulässig, weil die Aufgaben der Behörde auch ohne eine solche Kontaktliste erfüllt werden konnten. Erst recht unzulässig war bisher ein behördenübergreifendes Gesamtverzeichnis sämtlicher Kommunikationsvorgänge mit Behörden und Bediensteten des Bundes.

Die Aufzeichnung der näheren Umstände von Individualkommunikation mit Bundesbehörden ist der Sache nach ungeeignet, dazu beizutragen, Störungen oder Fehler an der Technik des Bundes zu erkennen oder zu beseitigen. Die Begründung des Regierungsentwurfs des Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes legt nicht dar, wie Verkehrsdaten geeignet sein sollen, zur Beseitigung von Anlagenfehlern beizutragen. Es ist nicht erkennbar, dass jemals irgendeine Bundesbehörde personenbezogene Verkehrsdaten benötigt hätte, um eine Störung zu erkennen oder zu beseitigen. Im gesamten Gesetzgebungsverfahren wurde zu keinem Zeitpunkt von einem der Beteiligten ein solcher Fall genannt.

Nach der Gesetzesbegründung sollen Logfiles von Servern, Firewalls usw. erhoben und automatisiert ausgewertet werden.[154] Das bedeutet, dass nach § 5 Abs. 1 S. 1 Nr. 1 BSIG beispielsweise jede E-Mail von und an Behördenmitarbeiter, jeder Zugriff auf das Internetportal einer Bundesbehörde und jeder Klick eines Behördenmitarbeiters im Internet aufgezeichnet und protokolliert werden soll. Dass eine solche personenbezogene Totalprotokollierung mit anschließender Auswertung zur Erkennung und Beseitigung von Störungen der Informationstechnik erforderlich sei, behaupten die Gesetzesbegründung und der BSI-Präsident selbst nicht. Beide messen der Ermächtigung nur im Zusammenhang mit der Erkennung und Abwehr von Angriffen Bedeutung zu.[155]

Erkennen lassen sich Störungen anhand von Verkehrsdaten nicht, außer vielleicht das Ausbleiben von Verbindungen. Um solche Verfügbarkeitsstörungen zu erkennen, ist es aber nicht erforderlich, gerade personenbezogene Verkehrsdaten zu erheben. Schon aus der bloßen Anzahl der über einen bestimmten Zeitraum hergestellten Verbindungen, wel-

---

[153] Helmbrecht, INA-Drs. 16(4)570 A, 6: „bislang nur nach ausdrücklicher Einwilligung der betroffenen Bundesbediensteten zulässig".

[154] Bundesregierung, BT-Drs. 16/11967, 14.

[155] Bundesregierung, BT-Drs. 16/11967, 14: „um Anzeichen für bevorstehende IT-Angriffe zu finden"; Helmbrecht, INA-Drs. 16(4)570 A, 6: „Hierdurch erst können Anzeichen für bevorstehende oder laufende IT-Angriffe erkannt und diese nachhaltig bekämpft werden."

che die Empfängerbehörde im Bereich dienstlicher Kommunikation ohne Eingriff in das Fernmeldegeheimnis erheben darf, lassen sich technische Störungen erkennen, ohne dass dazu personenbeziehbar – gar flächendeckend und permanent – aufzeichnet werden müsste, wer mit wem in Verbindung gestanden hat.

Selbst wenn man die grundsätzliche Eignung unterstellen wollte, genügte jedenfalls die Herstellung von Testverbindungen durch die Behördenmitarbeiter selbst (z.B. Test-E-Mails) zur Erkennung von Störungen und Fehlern. Es würde also genügen, wenn die Behörde eigene Testverbindungen herstellt oder herstellen lässt und deren nähere Umstände aufzeichnet und auswertet, um Störungen oder Fehler zu erkennen.

All dies gilt entsprechend für die Eingrenzung und Beseitigung von Störungen und Fehlern. Die Erhebung von Verkehrsdaten ist hierzu nicht geeignet. Insbesondere gilt dies für die Erhebung personenbezogener Verkehrsdaten. Jedenfalls genügt die Erhebung der Verkehrsdaten eigener Testverbindungen der Behörde, um Störungen und Fehler einzugrenzen und zu beseitigen.

§ 5 BSIG ist auch deshalb nicht erforderlich, weil schon die frühere Rechtslage wirksame Maßnahmen zur Störungsbeseitigung und Fehlerbehebung erlaubt hat. Im Bereich der dienstlichen Kommunikation unterliegen die näheren Umstände der bei Bundesbehörden ein- und ausgehenden Verbindungen nicht dem Fernmeldegeheimnis. Bundesbehörden können folglich bereits nach Maßgabe des Bundesdatenschutzgesetzes Informationen über bei ihnen ein- und ausgehende Verbindungen erheben und auswerten, soweit dies im Einzelfall geeignet, erforderlich und verhältnismäßig sein sollte, um Störungen und Fehler an ihrer Informationstechnik zu erkennen und zu beseitigen. Im Bereich der privaten Kommunikation von Behördenmitarbeitern erlaubte § 100 TKG Bundesbehörden schon immer die Verarbeitung anfallender Verkehrsdaten, soweit dies im Einzelfall geeignet, erforderlich und verhältnismäßig sein sollte, um Störungen und Fehler an Kommunikationsanlagen zu erkennen und zu beseitigen. Über diese vorbestehende Rechtslage hinaus sind die erweiterten Befugnisse nach § 5 BSIG zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes nicht erforderlich.

Dass dem Bund der Verzicht auf die in § 5 BSIG vorgesehenen Grundrechtseingriffe ohne weiteres möglich und zumutbar ist, belegt die frühere Rechtslage, die für andere Anlagenbetreiber als den Bund (z.B. Länder, Privatpersonen) bis heute unverändert fortgilt und folglich auch vom Gesetzgeber für ausreichend gehalten wird. Die Funktionsfähigkeit der Informationstechnik des Bundes ist nicht etwa schutzbedürftiger als die Informationstechnik Privater, etwa im Vergleich zur Informationstechnik von Energieversorgern, Gefahrguttransportunternehmen, Banken, Börsen, Krankenhäusern, Medien usw. Das Bundesinnenministerium selbst stellt die Bedeutung der Informationstechnik in diesen Bereichen auf

eine Stufe mit der Bedeutung der Informationstechnik in Behörden, Verwaltung und Justiz.[156]

Auch die Telekommunikations-Datenschutzrichtlinie der EU hält eine permanente, rein prophylaktische Verkehrsdatensammlung zur Beseitigung etwaiger Störungen nicht für erforderlich. Dies ergibt sich eindeutig aus Erwägungsgrund 29 der RL 2002/58/EG, wonach Verkehrsdaten nur „in Einzelfällen" zur Ermittlung von Störungen und Fehlern verarbeitet werden können. Nach der Rechtsprechung des EuGH ist ein Erwägungsgrund, der genauere Vorgaben als der Richtlinientext enthält, bei der Auslegung des Rechtsakts zu berücksichtigen.[157] Bei den Beratungen über die Richtlinie 2009/136/EG hat der Gemeinschaftsgesetzgeber einen Vorschlag[158] des Rates zur Änderung der Richtlinie 2002/58/EG, der TK-Anbieter ohne Beschränkung auf Einzelfälle zur Verkehrsdatenverarbeitung zwecks Gewährleistung der „Netz- und Informationssicherheit" ermächtigt hätte, ausdrücklich abgelehnt. Der Vorschlag war zuvor von Bürgerrechts-, Journalisten-, Anwalts- und Verbraucherschutzverbänden, von der deutschen Konferenz der Datenschutzbeauftragten des Bundes und der Länder[159] und auch vom Europäischen Datenschutzbeauftragten scharf kritisiert worden.

Von der mangelnden Eignung und Erforderlichkeit der Erhebung von Verkehrsdaten Dritter zur Störungserkennung oder –beseitigung abgesehen ist es eklatant unverhältnismäßig, nur wegen der abstrakten, nie auszuschließenden Möglichkeit einer Störung ohne besonderen Anlass flächendeckend Informationen über sämtliche mit Bundesbehörden und –mitarbeitern hergestellten Verbindungen zu erheben. Die von § 5 Abs. 1 BSIG gestattete anlasslose grundrechtseingreifende Erhebung und Auswertung aller Daten „ins Blaue hinein" ist mit dem Wesen des Art. 8 EMRK unvereinbar.[160]

(b) Telemedien-Nutzungsdaten

Soweit § 5 Abs. 1 S. 1 Nr. 1 BSIG auch zur Sammlung und Auswertung personenbezogener Informationen über die Nutzung von Telemedien des Bundes ermächtigt, gelten die vorstehenden Ausführungen zu Verkehrsdaten im Wesentlichen entsprechend.

Die rein vorsorgliche Aufzeichnung von Informationen über die Nutzung von Telemedien war Bundesorganen bisher verboten. Nach § 13 des Telemediengesetzes haben – auch öffentliche (§ 1 Abs. 1 S. 2 TMG) – Anbieter von Telemedien im Internet „sicherzustellen, dass [...] die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der

---

[156] BMI: Nationaler Plan zum Schutz der Informationsinfrastrukturen, http://www.bmi.bund.de/cae/servlet/contentblob/121734/publicationFile/13577/Nationaler_Plan_Schutz_Informationsinfrastrukturen.pdf, 21.

[157] EuGH, EuZW 2004, 400 Rdnr. 22.

[158] Gemeinsamer Standpunkt des Rates v. 9.2.2009, 2007/0248 (COD).

[159] http://www.datenschutz-bayern.de/dsbk-ent/DSK_76-ElektronischeKommunikation.html.

[160] Vgl. Bundesrat, BT-Drs. 16/12225, 3.

sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht [...] werden“. Dieses Protokollierungsverbot ist der Kern des deutschen Telemedien-Datenschutzrechts und stellt sicher, dass so wenige Daten über Internetnutzer wie möglich den vielfältigen Sicherheitsrisiken der Informationstechnik ausgesetzt werden. Der Gesetzgeber verbietet damit eine Vorratsdatenspeicherung. Er verfolgt mit dem Verbot einer Vorratsdatenspeicherung den – gegenüber einer möglichen Missbrauchsbekämpfung höherwertigen – Zweck, sensible Daten einer Vielzahl von Nutzern vor unberechtigten und missbräuchlichen Zugriffen auf Informationen über ihre private Internetnutzung zu schützen. Damit kommt er einer verfassungsrechtlichen Pflicht aus dem Grundrecht auf informationelle Selbstbestimmung nach. Das Bundesverfassungsgericht betont in ständiger Rechtsprechung das „strikte Verbot der Sammlung personenbezogener Daten auf Vorrat“.[161] Der Bundesgerichtshof hat jüngst ein „Recht des Internetnutzers auf Anonymität“ anerkannt.[162]

Die Aufzeichnung der Information, wer wann welches Telemedium wie genutzt hat, ist nicht geeignet, dazu beizutragen, Störungen oder Fehler an der Technik des Bundes zu erkennen oder zu beseitigen. Die Begründung des Gesetzentwurfs legt nicht dar, wie Nutzungsdaten geeignet sein sollen, zur Beseitigung von Anlagenfehlern beizutragen. Es ist nicht erkennbar, dass eine Bundesbehörde jemals Nutzungsdaten benötigt hätte, um eine Störung ihrer Anlagen zu erkennen oder zu beseitigen. Im gesamten Gesetzgebungsverfahren wurde zu keinem Zeitpunkt von einem der Beteiligten auch nur ein solcher Fall genannt.

Erkennen lassen sich Störungen anhand von Nutzungsdaten nicht, außer vielleicht eine ausbleibende oder übermäßig häufige Nutzung. Um solche Verfügbarkeitsstörungen zu erkennen, ist es aber nicht erforderlich, gerade personenbezogene Nutzungsdaten zu erheben. Schon aus der bloßen Anzahl der in einem bestimmten Zeitraum erfolgten Nutzungen, welche die Behörde auch ohne § 5 BSIG anonym erheben darf, lassen sich technische Störungen erkennen, ohne dass dazu personenbezogen – gar flächendeckend und permanent – aufzeichnet werden müsste, wer welche Internetseiten aufgerufen, Suchworte eingegeben und Forenbeiträge geschrieben hat. Anhand anonymer Daten können der Netzwerkverkehr beobachtet, Störungen erkannt und statistische Auswertungen vorgenommen werden. Hierzu bedarf es § 5 BSIG folglich ebenfalls nicht.

Selbst wenn man entgegen der tatsächlichen Gegebenheiten die grundsätzliche Eignung einer Sammlung von Nutzungsdaten zur Störungsbeseitigung unterstellen wollte, genügte jedenfalls die Testnutzung durch die Behörde selbst zur Erkennung von Störungen und Fehlern an ihren Anlagen. Es würde also genügen, wenn die Behörde eigene Tests ihrer Telemedien durchführt oder durchführen lässt und deren Daten aufzeichnet und auswertet, um Störungen oder Fehler zu erkennen.

---

[161] So ausdrücklich BVerfG, 1 BvR 518/02 vom 4.4.2006, Abs.-Nr. 105 - Rasterfahndung.

[162] BGH, NJW 2009, 2888 (2893), Abs. 42.

All dies gilt entsprechend für die Eingrenzung und Beseitigung von Störungen und Fehlern. Die Erhebung von Nutzungsdaten ist hierzu nicht geeignet. Insbesondere gilt dies für die Erhebung personenbezogener Nutzungsdaten. Jedenfalls genügt die Erhebung der Nutzungsdaten eigener Testnutzungen der Behörde, um Störungen und Fehler eingrenzen und beseitigen zu können.

§ 5 BSIG ist auch deshalb nicht erforderlich, weil schon die frühere Rechtslage hinreichend wirksame Maßnahmen zur Störungsbeseitigung und Fehlerbehebung erlaubt hat. Schon nach § 15 Abs. 1 TMG durften Nutzungsdaten erhoben und verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen. Wenn es zur Wiederherstellung der Verfügbarkeit eines Telemediums im Einzelfall erforderlich wäre, Nutzungsdaten zu erheben, erlaubte dies mithin bereits § 15 Abs. 1 TMG. Über diese vorbestehende Rechtslage hinaus sind die erweiterten Befugnisse nach § 5 BSIG zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes nicht erforderlich.

Zur Beseitigung von Störungen brauchen öffentliche Anbieter von Telemedien im Internet keine personenbezogenen Protokolle über das Verhalten ihrer Nutzer. DoS-Angriffe, unbefugte Manipulationen, Viren oder andere Infiltrierungen können nicht verhindert werden, indem man Daten sammelt. Vielmehr muss die vom Anbieter genutzte Hardware und Software so eingerichtet werden, dass sie solchen Angriffen stand hält. Sicherheitsmechanismen wie Firewalls und Software-Aktualisierungen funktionieren ohne personenbezogene Surfprotokolle.

Dass dem Bund der Verzicht auf die in § 5 BSIG vorgesehenen Grundrechtseingriffe ohne weiteres möglich und zumutbar ist, belegt die frühere Rechtslage, die für andere Anlagenbetreiber als den Bund (z.B. Länder, Privatpersonen) bis heute unverändert fortgilt und folglich auch vom Gesetzgeber für ausreichend gehalten wird. Bei der letzten Novellierung des Telemedienrechts im Jahre 2007 hat der Gesetzgeber zu Recht keine Aufgabe des gesetzlichen Protokollierungsverbots für erforderlich gehalten. Bei der Beratung des angefochtenen Gesetzes hat der Bundestag aus dem Regierungsentwurf eine geplante Ermächtigung der Telemedienanbieter zur Protokollierung des Nutzungsverhaltens ausdrücklich gestrichen.[163]

Die Praxis bestätigt den fehlenden Bedarf an personenbezogenen Protokollen über Internetnutzer. Große deutsche Telemedien wie die Portale www.bmj.bund.de, www.bmbf.de, www.bfdi.bund.de, www.bundesrechnungshof.de, www.auswaertiges-amt.de und www.bundeskriminalamt.de werden sicher und zuverlässig bereitgestellt, ohne IP-Adressen oder andere personenbeziehbare Informationen über ihre Nutzer zu sammeln.

[163] Rechtsausschuss, BT-Drs. 16/13259, 8.

In einem Grundsatzurteil aus dem Jahr 2007 gegen das Bundesjustizministerium entschied das Amtsgericht Berlin-Mitte, dass die „Störungsbeseitigung“ keine generelle Sammlung von IP-Adressen oder anderer personenbezogener Informationen über Nutzer rechtfertigt.[164] Das Bundesjustizministerium musste seine Praxis anpassen und stellt sein Internetportal seither sicher und zuverlässig ohne Sammlung personenbezogener Daten zur Verfügung.

Selbst wenn man die Eignung und Erforderlichkeit der Erhebung von Nutzungsdaten zur Störungserkennung oder -beseitigung – entgegen der tatsächlichen Gegebenheiten – unterstellen wollte, ist es grob unverhältnismäßig, nur wegen der theoretischen, nie auszuschließenden Möglichkeit einer Störung ohne besonderen Anlass flächendeckend Informationen über sämtliche Inanspruchnahmen von Telemedien des Bundes zu erheben. Die von § 5 Abs. 1 BSIG gestattete anlasslose grundrechtseingreifende Erhebung und Auswertung aller Daten „ins Blaue hinein“ lassen die Menschenrechte nicht zu.[165]

(6) Unverhältnismäßiges Erkennen und Beseitigen von Angriffen (§ 5 Abs. 1 S. 1 Nr. 1 Var. 2 BSIG)

§ 5 Abs. 1 S. 1 Nr. 1 BSIG ermächtigt das BSI, die näheren Umstände der elektronischen Kommunikation mit Bundesbehörden (§ 2 Abs. 8 BSIG) aufzuzeichnen und automatisiert auszuwerten, um Angriffe auf die Informationstechnik des Bundes zu erkennen und zu „beseitigen“. Betroffen sind wiederum Verkehrsdaten über die computergestützte Kommunikation mit Bundesbehörden (z.B. E-Mail) sowie Daten über die Nutzung öffentlicher Telemedien von Bundesorganen (§ 2 Abs. 8 S. 2 BSIG).

§ 5 Abs. 1 S. 1 Nr. 1 BSIG ist schon deswegen zur Abwehr von Angriffen ungeeignet, weil aus der Maßnahme gewonnene Erkenntnisse über Angriffe regelmäßig nicht verwendet werden dürfen. Eine Verwendung der gewonnenen Erkenntnisse ist nach dem klaren Wortlaut des § 5 BSIG nur zulässig, wenn der Verdacht eines Schadprogramms besteht (§ 5 Abs. 1 und 3 BSIG). Erkenntnisse über nicht-automatisierte Angriffe darf das BSI danach nicht nutzen oder weiter geben. Da die vom BSI erhobenen Verkehrsdaten dem Fernmeldegeheimnis unterliegen, ist auch eine anonymisierte Weitergabe nicht zugelassen (vgl. § 5 Abs. 1 S. 3 BSIG). Insoweit ist § 5 Abs. 1 S. 1 Nr. 1 BSIG von vornherein zur Abwehr von Angriffen ungeeignet.

Zur Abwehr von Angriffen auf die Informationstechnik des Bundes ist eine personenbezogene Protokollierung des Informations- und Kommunikationsverhaltens auch ganz regelmäßig nicht erforderlich. Der Begriff des „Angriffs auf die Informationstechnik des Bundes“ lässt sich definieren als der Versuch oder die Vorbereitung einer Beeinträchtigung der

---

[164] AG Berlin, Urt. v. 27.03.2007, 5 C 314/06.

[165] Vgl. Bundesrat, BT-Drs. 16/12225, 3.

Verfügbarkeit oder Vertraulichkeit öffentlicher Computersysteme unter Verwendung von Kommunikationstechnik des Bundes.

Laut Regierungsbegründung soll die vorgesehene Protokollierung erstens durch Auswertung des Datenvolumens zur Angriffsabwehr beitragen.[166] Das Datenvolumen kann allerdings bereits anhand anonymer Protokolle ausgewertet werden, so dass die in § 5 BSIG vorgesehene Erhebung personenbezogener Daten nicht erforderlich ist. Die Regierungsbegründung nennt zweitens „das automatisierte ‚Absurfen' von aus dem Bundesnetz heraus aufgerufenen URLs, um sog. Phishingseiten zu identifizieren." [167] Phishingseite ist eine Webseite, die den Nutzer über die Person ihres Betreibers täuscht, um ihn zur Eingabe persönlicher Daten (z.B. PINs, TANs, Passwörter) zu veranlassen. Phishingseiten stellen jedoch bereits keinen Angriff auf die Informationstechnik des Bundes im Sinne des § 5 Abs. 1 S. 1 Nr. 1 BSIG dar. Außerdem können die abgerufenen URLs bereits anhand anonymer Protokolle der von Bundesbediensteten abgerufenen URLs ausgewertet werden, so dass die in § 5 BSIG vorgesehene Erhebung personenbezogener Daten nicht erforderlich ist.

Der damalige BSI-Präsident führte weiter an, auf der Grundlage des § 5 Abs. 1 BSIG sollten „Detektionstools" eingesetzt werden.[168] Damit dürften sog. „Einbruchserkennungsvorrichtungen" („Intrusion Detection Systems") gemeint sein. Es handelt sich dabei um eine Art Alarmanlage, die verdächtige oder außergewöhnliche Kommunikationsmuster automatisiert feststellen und melden soll.

Hierzu ist anzumerken, dass Angriffe durch eine Erkennung und Aufzeichnung des Angriffs nicht abgewehrt werden können. Zur Abwehr von Angriffen ist vielmehr die regelmäßige Schließung von Sicherheitslücken durch Updates und Patches sowie der Einsatz zugriffsbeschränkender Firewalls unabdingbar und ganz regelmäßig genügend. Der Einsatz dieser Verfahren und Technologien bei den Bundesbehörden erfolgt bereits heute und ist mit keinem Grundrechtseingriff verbunden. In einer Entschließung vom 06./07.11.2008 führt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder zutreffend aus:

> *„Es ist daher nicht erforderlich, zur Gewährleistung der Netz- und Informationssicherheit einzelfallunabhängig personenbezogene Verkehrsdaten zu speichern. Die Anbieter von Telekommunikationsdiensten sind aufgefordert, ihre Systeme so sicher zu gestalten, dass Angriffe von vornherein erfolglos bleiben."*[169]

Da diese Verfahren zur „Härtung" von Informationstechnik ohnehin eingesetzt werden müssen und die Ausnutzung bekannter Sicherheitslücken verhindern, verbleiben für weitere Maßnahmen nur noch unbekannte Angriffswege. Die automatisierte Auswertung von

---

[166] Bundesregierung, BT-Drs. 16/11967, 14.

[167] Bundesregierung, BT-Drs. 16/11967, 14.

[168] Helmbrecht, INA-Drs. 16(4)570 A, 6.

[169] http://www.datenschutz.hessen.de/k76.htm#entry2919.

Kommunikations- und Informationsprotokollen ist denkbar schlecht geeignet, unbekannte Angriffswege aufzudecken. Fox führt dazu aus:[170] Das beobachtbare Kommunikationsverhalten unterliege starken „Schwankungen“, die sich von Anomalien praktisch nicht unterscheiden ließen und daher in erheblichem Ausmaß Fehlalarme auslösten. Fehlalarme binden laut Fox so viele Ressourcen, dass eine gezielte Sicherheitsarbeit insgesamt eher behindert wird. Wegen der Fehlalarme seien viele Erkennungssysteme schon deaktiviert worden oder ihre Meldungen würden nicht mehr beachtet. Viele Angriffe (z.B. Trojaner) entfalteten zudem ein Kommunikationsverhalten, das die Alarmierungsschwelle nicht überschreite, da es von „normalem“ Nutzungsverhalten nicht unterschieden werden könne. Auffällige Angriffe hingegen, wie z.B. die eine massive Auslastung und Verlangsamung von Servern verursachende DoS-Attacke, bemerke man auch ohne personenbezogene Protokollierung. Insgesamt bleibe der Einsatz von „Einbruchserkennungsvorrichtungen“ „ohne einen erkennbaren Sicherheitsgewinn“.[171]

Das BSI selbst bewertet „Einbruchserkennungssysteme“ öffentlich mit den folgenden Worten:

> *„Die Wahl der Parametereinstellung ist äußerst kritisch und kann leicht zu Fehlalarmen bzw. zum Übersehen von Angriffen führen. Es werden keine klaren Aussagen getroffen; es kann lediglich von einer Wahrscheinlichkeit für einen Angriff gesprochen werden.*
>
> *Anomalieerkennung ist derzeit noch Gegenstand der aktuellen Forschung und weit von der praktischen Einsetzbarkeit entfernt.*“[172]

Im Leitfaden des BSI für die Einführung von Intrusion-Detection-Systemen[173] heißt es zu Telemedien-Angeboten im Internet:

> *„Allgemeine Informationsbereitstellung über statische Webseiten [...]*
>
> *In diesem Szenario werden auf einem Webserver Informationen zum Abruf über das Internet bereitgestellt. [...]*
>
> *Die Betrachtung der Einflussgrößen zeigt, dass in diesem Szenario der sicherheitstechnische Zusatznutzen bei Einsatz eines IDS eher gering ist. [...]*
>
> *Typische Angriffe auf Webserver nutzen entweder Schwächen der Serverprogramme oder Schwachstellen bei der Realisierung dynamischer Inhalte aus. Bei einer rein statischen Bereitstellung von Daten kann ein angemessener Schutz des Webangebots in der Regel mit bestehenden Mitteln realisiert werden. Bestehende Restrisiken sind auch ohne Einsatz eines IDS tolerierbar.*“

---

[170] Fox, DuD 2005, 422.

[171] Fox, DuD 2005, 422.

[172] https://www.bsi.bund.de/cln_136/ContentBSI/Themen/sinet/Uebersicht/angriff.html.

[173] https://www.bsi.bund.de/cae/servlet/contentblob/486992/publicationFile/30698/Leitfadenv10_pdf.pdf.

Vor dem Innenausschuss des Deutschen Bundestages hat der Sachverständige Prof. Dr. Hartmut Pohl, der Inhaber eines Lehrstuhls für Informationssicherheit der Hochschule Bonn-Rhein-Sieg ist, ausgeführt:[174]

> „*Das Gesetz erweckt den Eindruck, als würden diese Schadprogramme vom Himmel fallen und würden uns überfluten. Das ist ein völlig falscher Eindruck. Schadprogramme können nur Schaden anrichten, wenn sie tatsächlich eine Sicherheitslücke ausnutzen. Wenn die Sicherheitslücke geschlossen ist, dann nutzt auch ein Schadprogramm nichts. Ein aktuelles Beispiel ist der schon erwähnte Conficker-Wurm, der eine Sicherheitslücke, die längst gepatcht und korrigiert war, ausnutzte und deswegen Schaden anrichten konnte, weil viele Anwender die Fehlerkorrekturen nicht eingefahren haben. Eine Diskussion von Schadprogrammen, wie sie im Gesetzentwurf vorgesehen ist, die Untersuchungen und der Versuch, sie abzuwehren, ist aus meiner Sicht völlig nutzlos und kratzt an der Oberfläche der Informationssicherheit. Wir müssen uns an die Ursachen halten. Die Ursache ist jeweils eine Sicherheitslücke, zu der eine ganze Reihe von Schadprogrammen zugeordnet werden können und die Schadprogramme können dann diese Sicherheitslücke ausnutzen. Die Diskussion über Schadprogramme ist überflüssig. Wir müssen uns auf die Sicherheitslücken konzentrieren. Das ist auch der Stand der Technik in Unternehmen, die sich nicht dazu verleiten lassen zu protokollieren, wer greift auf unsere Systeme wann zu und sendet etwas, sondern, wenn ein Angriff stattgefunden hat, wird nicht eruiert, wer der Täter ist, es wird eruiert, wo liegt die Sicherheitslücke, und die wird geschlossen. Das ist der Stand der Technik.*
>
> *Wenn ich ein Beispiel aus dem Brandschutz bringen darf: Wenn Sie sich hier umsehen, es werden Sicherheitsmaßnahmen ergriffen, im Schrank ist ein Feuerlöscher, es gibt eine Sprinkleranlage, die Decke ist schwer entflammbar – selbst wenn es hier brennt, geht der Brand nicht aus dem Raum hinaus. Ganz wichtig, Sie sehen auch die Hinweise auf die Fluchtwege, wir kommen noch hinaus – auch wenn es hier brennt, der Brand geht nicht in die anderen Räume. Sie würden sehr lachen, wenn jemand fordert, wir wollen vor dem Raum eine Videokamera aufstellen und kontrollieren, protokollieren, auswerten und speichern, wer in den Raum hinein- und wer hinausgeht. Das ist kein Brandschutz, das ist Überwachung. So formuliert das Gesetz, vergleichbar in § 5, und deswegen muss § 5 aus meiner Sicht völlig gestrichen werden. Wir sollten im Gegenteil die Bundesregierung verpflichten, ab Ende 2009 ausschließlich zertifizierte Produkte einzusetzen, um wenigstens ein gewisses Sicherheitsniveau bei der Bundesverwaltung zu erreichen.*“

---

[174] Pohl, Protokoll Nr. 16/94 der Anhörung am 11.05.2009, http://www.bundestag.de/ausschuesse/a04/anhoerungen/Anhoerung_21/Protokoll.pdf, 15 f.

Es ist nochmals darauf hinzuweisen, dass die Systeme des Bundes über Jahre hinweg ohne personenbezogene Totalprotokollierung funktionierten, dass dies bei anderen kritischen Infrastrukturen bis heute der Fall ist und dass Systeme mit personenbezogener Totalprotokollierung und Auswertung im Ergebnis keineswegs häufiger verfügbar sind oder weniger Datenpannen erleiden. Vor dem Hintergrund, dass Einbruchserkennungssysteme im Ergebnis keinen statistisch signifikanten Nutzen entfalten, ist es jedenfalls unverhältnismäßig, eine globale und pauschale Erfassung der Telekommunikation mit Bundesorganen vorzunehmen, um derartige Systeme einzusetzen.

Ob es verhältnismäßig sein kann, anonym den Datenverkehr zu sichten und auf Auffälligkeiten zu überprüfen, kann dahin stehen. Auch ob unter der Voraussetzung, dass konkrete Tatsachen auf einen erfolgreichen Angriff hinweisen, die zeitlich befristete und gezielte Aufzeichnung personenbezogener Informationen über das Informations- oder Kommunikationsverhalten bestimmter Quellen zur Gefahrenabwehr verhältnismäßig sein kann, kann offen bleiben. Jedenfalls sprengt § 5 Abs. 1 S. 1 Nr. 1 BSIG dadurch die Grenzen der Verhältnismäßigkeit, dass er zu einer vollkommen anlasslosen und flächendeckenden personenbezogenen Aufzeichnung und Auswertung von Informationen über das gesamte Informations- und Kommunikationsverhalten ermächtigt. Die Tiefe des damit verbundenen Eingriffs in die Grundrechte der Bürger und Behördenmitarbeiter steht offensichtlich außer Verhältnis zu dem damit erhofften, nicht nachweisbaren Sicherheitsgewinn.

(a) Verkehrsdaten

Die in § 5 Abs. 1 S. 1 Nr. 1 BSIG vorgesehene Aufzeichnung der näheren Umstände von Individualkommunikation mit Bundesbehörden soll der Abwehr von Angriffen auf die Informationstechnik des Bundes dienen. Fraglich ist, wie solche Angriffe mittels Individualkommunikation begangen werden können. Möglich ist erstens der Versand von Schadprogrammen per E-Mail. Möglich ist zweitens die Überflutung der Kommunikationstechnik (z.B. Mailserver) mit Nachrichten. Drittens kann versucht werden, in die Kommunikationstechnik (z.B. Mailserver) einzudringen.

(aa) Schadprogramme

Die Aufzeichnung von Verkehrsdaten über Individualkommunikation trägt nicht dazu bei, E-Mails mit Schadprogrammen zu erkennen, zurückzuweisen oder unschädlich zu machen. Erkannt werden können solche E-Mails nur durch eine Analyse ihres Inhalts.

Das BSI beabsichtigt, im Fall eines anderweitig festgestellten Schadprogramms anhand von Verkehrsdaten nachzuprüfen, welche anderen Nachrichten über dieselbe Quelle (z.B. Mailserver) versandt worden sind, um zu überprüfen, ob auch bei anderen Empfängern ein Schadprogramm aktiviert worden ist. Eine Vorratsspeicherung von Verkehrsdaten zu diesem Zweck ist jedoch weder erforderlich noch verhältnismäßig. Verkehrsdaten sind nicht erforderlich, weil bei Feststellung eines Schadprogramms ohnehin die gesamte Bundesverwaltung ihre Systeme auf das Vorhandensein des Schadprogramms überprüfen und

aufgefundene Programme beseitigen muss („Virenscanner“). Es ist nicht erkennbar, dass eine Bundesbehörde jemals mithilfe von Verkehrsdaten Schadprogramme aufgefunden hat, die nicht schon durch den Einsatz eines Virenscanners aufgefunden worden wären. Im gesamten Gesetzgebungsverfahren wurde zu keinem Zeitpunkt von einem der Beteiligten ein solcher Fall genannt. Es wäre auch unverantwortlich, nur Schadprogrammen aus derselben Quelle nachzugehen, zumal Angreifer eine Vielzahl – mitunter Hunderttausende („Farming“) – unterschiedlicher Quellen zur Einschleusung von Schadprogrammen einsetzen. Erkennung, Beseitigung und Abwehr des festgestellten Schadprogramms sind allesamt mithilfe von Software („Virenscanner“) auch ohne die Verwendung personenbezogener Daten möglich. Im Übrigen sind schon in den mit Schadprogrammen infizierten, bekannten E-Mails Protokolldaten enthalten, die man bei dem Empfänger auswerten könnte, wenn dies erforderlich wäre. Einer zusätzlichen zentralen Erfassung des gesamten Kommunikationsverkehrs mit Mitarbeitern von Bundesorganen – es handelt sich um rund 500.000 Menschen – bedarf es nicht. Selbst wenn damit Sicherheitsvorteile verbunden wären (was nicht der Fall ist), stünde der damit verbundene Eingriff in das Fernmeldegeheimnis vollkommen außer Verhältnis zu dem Zusatznutzen der Maßnahme gegenüber den sonst verfügbaren milderen Mitteln.

(bb) Überflutung

Kommunikationstechnik kann für Angriffe eingesetzt werden, indem eine übergroße Vielzahl von Nachrichten an einen Computer (Server) adressiert wird und dadurch dessen Verfügbarkeit beeinträchtigt wird. Die personenbezogene Aufzeichnung der näheren Umstände von Individualkommunikation mit Bundesbehörden ist indes nicht geeignet, dazu beizutragen, solche Angriffe zu erkennen oder abzuwehren. Die Begründung des Gesetzentwurfs legt derartiges nicht dar. Es ist nicht erkennbar, dass eine Bundesbehörde jemals personenbezogene Verkehrsdaten benötigt hätte, um einen Verfügbarkeitsangriff zu erkennen oder abzuwehren. Im gesamten Gesetzgebungsverfahren wurde zu keinem Zeitpunkt von einem der Beteiligten ein solcher Fall genannt.

Anhand von Verkehrsdaten lässt sich allenfalls das Ausbleiben von Verbindungen oder eine verzögerte Funktionsweise der Kommunikationstechnik erkennen. Um solche Verfügbarkeitsstörungen zu erkennen, ist es aber nicht erforderlich, gerade personenbezogene Verkehrsdaten zu erheben. Schon aus der bloßen Anzahl der über einen bestimmten Zeitraum hergestellten Verbindungen, welche die Empfängerbehörde im Bereich dienstlicher Kommunikation ohne Eingriff in das Fernmeldegeheimnis erheben darf, lassen sich technische Störungen erkennen, ohne dass dazu personenbeziehbar – gar flächendeckend und permanent – aufgezeichnet werden müsste, wer mit wem in Verbindung gestanden hat.

Selbst wenn man die grundsätzliche Eignung unterstellen wollte, genügte jedenfalls die Herstellung von Testverbindungen durch die Behördenmitarbeiter selbst (z.B. Test-E-Mails) zur Erkennung von Verfügbarkeitsstörungen. Es würde also genügen, wenn die Be-

hörde regelmäßig eigene Testverbindungen herstellt oder herstellen lässt und deren nähere Umstände aufzeichnet und auswertet, um Verfügbarkeitsstörungen zu erkennen.

Zur Abwehr von Verfügbarkeitsangriffen sind ganz andere technische Maßnahmen erforderlich, welche die Erhebung personenbezogener Daten nicht erfordern und dennoch die Verfügbarkeit der Informationstechnik im Fall von Angriffen gewährleisten. Die eingesetzte Kommunikationstechnik muss so gestaltet („gehärtet“) werden, dass sie durch Überflutungen nicht beeinträchtigt wird. Maßnahmen unter Anknüpfung an die Quellen einer Überflutung sind schon deshalb nicht zum Schutz vor Angriffen geeignet, weil derartige Angriffe heutzutage über eine Vielzahl – mitunter Hunderttausende – von Quellen erfolgen.

Im Übrigen ist bereits oben gezeigt worden, dass die Rechtsordnung in Bundesdatenschutzgesetz und § 100 TKG auch ohne § 5 BSIG ausreichende und angemessene Befugnisse zur Erkennung, Eingrenzung und Beseitigung von Störungen vorsieht. Dass dem Bund der Verzicht auf die in § 5 BSIG vorgesehenen Grundrechtseingriffe ohne weiteres möglich und zumutbar ist, belegt die frühere Rechtslage, die für andere Anlagenbetreiber als den Bund (z.B. Länder, Privatpersonen) bis heute unverändert fortgilt und folglich auch vom Gesetzgeber für ausreichend gehalten wird.

Selbst wenn man die Erhebung von Verkehrsdaten zur Erkennung oder Abwehr von „Überflutungen“ – entgegen der tatsächlichen Gegebenheiten – als geeignet und erforderlich erachten wollte, ist es jedenfalls grob unverhältnismäßig, wegen des nie auszuschließenden Dauerrisikos eines Angriffs ohne besonderen Anlass flächendeckend Informationen über sämtliche mit Bundesbehörden und –mitarbeitern hergestellten Verbindungen zu erheben, wie es § 5 Abs. 1 S. 1 Nr. 1 BSIG vorsieht.

(cc) Einbruchsversuche

Informationstechnik kann eingesetzt werden, um unberechtigten Zugriff auf Computersysteme zu erlangen („Hacking“). Dies kann unter Ausnutzung von Sicherheitslücken erfolgen oder auch durch Ausprobieren der Zugangsdaten Berechtigter.

Bezüglich Einbruchsversuchen muss nicht darauf eingegangen werden, ob die Erhebung personenbezogener Daten über Zugriffsversuche geeignet, erforderlich und verhältnismäßig ist, um unberechtigte Zugriffe zu erkennen und abzuwehren. Denn jedenfalls Verkehrsdaten sind hierzu nicht geeignet. Kommunikationsdienste wie E-Mail erlauben es nicht, in einen Computer einzubrechen. Deswegen ist die Erhebung von Verkehrsdaten von vornherein ungeeignet zur Abwehr von Einbruchsversuchen.

Das Fernmeldegeheimnis schützt nur Telekommunikation, also die Vermittlung von Nachrichten (vgl. §§ 88, 3 Nrn. 22 und 23 TKG). Personen oder Computersysteme, die Sicherheitslücken eines anderen Computersystems auskundschaften oder ausnutzen, nutzen nicht den über das System bereit gestellten Telekommunikationsdienst und genießen daher nicht das Fernmeldegeheimnis. Ein Telekommunikationsdienst wird regelmäßig nur über bestimmte Zugänge bereit gestellt. Wer über andere Zugänge (Ports) versucht, in ein

System einzudringen, ist nicht Nutzer des bereit gestellten Telekommunikationsdienstes und genießt nicht den Schutz des Fernmeldegeheimnisses. Im Bereich von Zugängen, über die kein Telekommunikationsdienst bereit gestellt wird, können öffentliche Stellen daher auch ohne § 5 BSIG nach Maßgabe des Bundesdatenschutzgesetzes angemessene Vorkehrungen zum Schutz ihrer Systeme treffen.

§ 5 BSIG ist somit weder geeignet noch erforderlich, um vor Einbruchsversuchen zu schützen.

(b) Telemedien-Nutzungsdaten

Auch die in § 5 Abs. 1 S. 1 Nr. 1 BSIG vorgesehene Aufzeichnung von Informationen über die Nutzung von Telemedien soll der Abwehr von Angriffen auf die Informationstechnik des Bundes dienen. Fraglich ist, wie solche Angriffe durch die Nutzung von Telemedien begangen werden können. Möglich ist erstens die Überflutung der zur Bereitstellung von Telemedien des Bundes genutzten Kommunikationstechnik (z.B. Webserver) mit Anfragen. Zweitens kann versucht werden, in die Kommunikationstechnik des Bundes einzudringen.

(aa) Überflutung

Die zur Bereitstellung von Telemedien verwendete Informationstechnik kann Ziel von Angriffen werden, indem eine übergroße Vielzahl von Anfragen an einen Server adressiert wird und dadurch dessen Verfügbarkeit beeinträchtigt wird. Die Aufzeichnung der näheren Umstände der Telemediennutzung ist allerdings nicht geeignet, dazu beizutragen, solche Angriffe zu erkennen oder abzuwehren. Die Begründung des Gesetzentwurfs legt derartiges nicht dar. Es ist nicht erkennbar, dass eine Bundesbehörde jemals Nutzungsdaten benötigt hätte, um einen Verfügbarkeitsangriff zu erkennen oder abzuwehren. Im gesamten Gesetzgebungsverfahren wurde zu keinem Zeitpunkt von einem der Beteiligten ein solcher Fall genannt.

Anhand von Nutzungsdaten lässt sich allenfalls das Ausbleiben der Nutzung oder eine Verzögerung der Bereitstellung eines Telemediums erkennen. Um solche Verfügbarkeitsstörungen zu erkennen, ist es aber nicht erforderlich, gerade personenbezogene Nutzungsdaten zu erheben. Schon aus der bloßen Anzahl der über einen bestimmten Zeitraum hergestellten Verbindungen, welche die Behörde anonym erheben darf, lassen sich technische Störungen erkennen, ohne dass dazu personenbeziehbar – gar flächendekkend und permanent – aufgezeichnet werden müsste, wer welche Internetseiten aufgerufen, Suchworte eingegeben oder Forenbeiträge geschrieben hat. Selbst wenn man die grundsätzliche Eignung unterstellen wollte, genügten jedenfalls regelmäßige Testnutzungen durch die Behörde selbst zur Erkennung von Verfügbarkeitsangriffen.

Zur Abwehr von Verfügbarkeitsangriffen sind ganz andere technische Maßnahmen erforderlich, welche die Erhebung personenbezogener Daten nicht erfordern und dennoch die Verfügbarkeit der Informationstechnik gewährleisten. Die eingesetzte Kommunikationstechnik muss so gestaltet („gehärtet“) werden, dass sie durch Überflutungen nicht beein-

trächtigt wird. Maßnahmen unter Anknüpfung an die Quelle einer Überflutung sind schon deshalb nicht geeignet, weil derartige Angriffe heutzutage über eine Vielzahl – mitunter Hunderttausende („Farming“) – von Quellen (Servern) erfolgen.

In den Empfehlungen des BSI zum Schutz vor verteilten Denial of Service-Angriffen im Internet werden unter anderem die folgenden Maßnahmen vorgeschlagen:[175]

- Einsatz von Paketfiltern bei Serverbetreibern
- Etablierung eines Notfallplans
- Sichere Konfiguration der Server
- Restriktive Rechtevergabe und Protokollierung
- Einsatz von Open-Source-Produkten
- Auswahl geeigneter und IT-sicherheitsbewußter Serverbetreiber
- Vermeidung aktiver Inhalte
- Tägliche Überprüfung von Dateien auf Viren und Angriffsprogrammen
- Zuverlässiger und aktueller Virenschutz und das Abschalten aktiver Inhalte im Browser, ggf. auch der Einsatz von Hilfsprogrammen zum Online-Schutz des Clients (beispielsweise PC-Firewalls)
- IT-Grundschutz für Rechner mit Internet-Anschluss
- Zeitnahes Einspielen von Sicherheits-Updates
- Tool-Einsatz und Schulung der Mitarbeiter

Keine dieser Schutzmaßnahmen erfordert die in § 5 BSIG vorgesehenen Grundrechtseingriffe. Auch soweit eine „automatische Angriffserkennung“ durch ständige Überwachung typischer Kennwerte (Speicherauslastung, Stacks, Netzauslastung, ...) empfohlen wird, sind dazu ausschließlich anonyme Daten erforderlich und nicht etwa personenbeziehbare Daten.

Im Übrigen lässt schon § 15 Abs. 1 TMG die Erhebung und Verarbeitung personenbezogener Nutzungsdaten zu, sollte dies einmal zur Wiederherstellung der Verfügbarkeit eines Telemediums einmal erforderlich sein. Dass dem Bund der Verzicht auf die in § 5 BSIG vorgesehenen Grundrechtseingriffe ohne weiteres möglich und zumutbar ist, belegt die frühere Rechtslage, die für andere Anlagenbetreiber als den Bund (z.B. Länder, Privatpersonen) bis heute unverändert fortgilt und folglich auch vom Gesetzgeber für ausreichend gehalten wird.

Selbst wenn man die Erhebung von Nutzungsdaten zur Erkennung oder Abwehr von „Überflutungen“ – entgegen der tatsächlichen Gegebenheiten – als geeignet und erforder-

[175] https://www.bsi.bund.de/cln_136/ContentBSI/Themen/sinet/Gefaehrdungen/DDoSAngriffe/ddos.html.

lich erachten wollte, wäre es jedenfalls grob unverhältnismäßig, wegen des nie auszuschließenden Dauerrisikos eines Angriffs ohne besonderen Anlass flächendeckend Informationen über das gesamte Informationsverhalten auf Telemedien des Bundes zu erheben, wie es § 5 Abs. 1 S. 1 Nr. 1 BSIG vorsieht.

(bb) Einbruchsversuche

Die zur Bereitstellung von Telemedien verwendete Informationstechnik kann Ziel von Angriffen werden, die darauf abzielen, unberechtigt Zugriff auf die Systeme zu erlangen („Hacking“). Dies kann unter Ausnutzung von Sicherheitslücken erfolgen oder auch durch „Ausprobieren“ der Zugangsdaten von Berechtigten.

In den meisten Fällen ist die Erhebung von Nutzungsdaten schon deshalb nicht zur Verhinderung unberechtigter Zugriffe erforderlich, weil unberechtigte Zugriffe nicht unter Nutzung eines Telemediums erfolgen. Soweit die §§ 13, 15 TMG die Aufbewahrung von Nutzungsdaten über die Dauer des Nutzungsvorgangs hinaus untersagen, gilt dieses Protokollierungsverbot nur für „personenbezogene Daten eines Nutzers“ (§ 15 TMG). Nutzer ist, wer „Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen“ (§ 2 TMG). Personen oder Computersysteme hingegen, die Sicherheitslücken eines anderen Computersystems auskundschaften oder ausnutzen, nutzen nicht den bereit gestellten Informations- oder Kommunikationsdienst und sind daher keine Nutzer im Sinne des Gesetzes. Ein Telemedium wird regelmäßig nur über bestimmte Zugänge bereit gestellt. Wer über andere Zugänge (Ports) versucht, in ein System einzudringen, ist nicht Nutzer des bereit gestellten Telemediums und genießt nicht den gesetzlichen Protokollierungsschutz. Im Bereich von Zugängen, über die kein Telemedium bereit gestellt wird, können öffentliche Stellen daher auch ohne § 5 BSIG nach Maßgabe des Bundesdatenschutzgesetzes angemessene Vorkehrungen zum Schutz ihrer Systeme treffen. § 5 BSIG bedarf es folglich nicht, um nicht öffentliche Zugänge zu schützen.

Allerdings können auch zugangsbeschränkte Telemedien unberechtigt genutzt werden, namentlich wo die Nutzung eine Authentifizierung voraussetzt. Es ist denkbar, dass ein Angreifer mögliche Zugangsdaten „durchprobiert“. Zur Erkennung solcher Angriffe, die sich durch die außergewöhnliche Häufigkeit von Zugriffsversuchen auszeichnen, bedarf es einer Protokollierung personenbezogener Nutzungsdaten nicht, weil die Zahl der Zugriffsversuche anonym erhoben werden kann. Eine Protokollierung von Zugriffsversuchen ist auch nicht geeignet, um Angriffe abzuwehren, weil eine bloße Aufzeichnung den Angreifer offenkundig nicht von dem Angriff abhält. Auch eine Sperrung der für den Angriff eingesetzten Quelle ist untauglich, weil eine beliebige Vielzahl anderer Rechner zur Fortsetzung der Zugriffsversuche eingesetzt werden können. Taugliches und milderes Mittel ist es beispielsweise, die Bearbeitung von Zugriffsversuchen so stark zu verzögern, dass ein „Durchprobieren“ zeitlich unmöglich wird.

Jedenfalls betrifft die soeben diskutierte Fallkonstellation nur Authentifizierungsformulare von Telemedien und rechtfertigt daher von vornherein nicht die in § 5 Abs. 1 S. 1 Nr. 1 BSIG vorgesehene Erfassung der Nutzung sämtlicher öffentlich zugänglicher Telemedien. Im Übrigen liegt für Authentifizierungsformulare ein milderes und ebenso geeignetes Mittel darin, dass anlässlich der Authentifizierung die Einwilligung der Nutzer in die Erhebung ihres Zugangsverhaltens eingeholt wird. Auch insoweit bedarf es einer besonderen gesetzlichen Eingriffsermächtigung nicht.

(7) Unverhältnismäßige Abwehr von Schadprogrammen (§ 5 Abs. 1 S. 1 Nr. 2 BSIG)

§ 5 Abs. 1 S. 1 Nr. 2 BSIG ermächtigt das BSI, die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auszuwerten, um Schadprogramme zu erkennen und abzuwehren. Betroffen sind hier nicht nur Verkehrsdaten über die computergestützte Kommunikation mit Bundesbehörden (z.B. E-Mail) sowie Daten über die Nutzung öffentlicher Telemedien von Bundesorganen (§ 2 Abs. 8 S. 2 BSIG). Vielmehr sind hier auch der Inhalt computergestützter Kommunikation mit Bundesbehörden (z.B. E-Mails) sowie die von öffentlichen Telemedien von Bundesorganen abgerufenen und dorthin übertragenen Inhalte betroffen. Da auf die Auswertung von Verbindungsdaten zur Abwehr von Schadprogrammen bereits eingegangen worden ist,[176] wird im Folgenden nur noch die Auswertung von Nutzungsdaten sowie von Informations- und Kommunikationsinhalten behandelt.

Die Befugnis zur Auswertung des Datenverkehrs nach § 5 Abs. 1 S. 1 Nr. 2 BSIG ist zunächst insoweit nicht zur Erkennung oder Abwehr von Schadprogrammen geeignet, wie der ausgehende Datenverkehr in Rede steht. An Dritte übertragene Informationen können offensichtlich keine Schadprogramme in technische Systeme des Bundes einbringen. Die Auswertung des ausgehenden Datenverkehrs ist auch nicht erforderlich, um Schadprogramme anhand ihrer Außenkommunikation zu erkennen, weil zu diesem Zweck auf den Systemen des Bundes ohnehin Erkennungssoftware („Virenschutz“) eingesetzt werden muss. Diese Schadprogramm-Erkennung auf den Systemen selbst funktioniert sehr viel besser als der Versuch, aus dem Heuhaufen des gesamten Datenverkehrs die Nadel der Außenkommunikation von Schadprogrammen herauszusuchen, zumal viele Schadprogramme nicht nach außen kommunizieren.

Soweit der eingehende Datenverkehr (z.B. Internetnutzung oder E-Mail-Korrespondenz von Bundesangehörigen) in Rede steht, ist die Befugnis zur Auswertung von Nutzungsdaten nach § 5 Abs. 1 S. 1 Nr. 1 BSIG und des Datenverkehrs nach § 5 Abs. 1 S. 1 Nr. 2 BSIG ebenfalls nicht zur Erkennung oder Abwehr von Schadprogrammen erforderlich. Auch ohne § 5 BSIG ist es dem Empfänger von Daten nämlich gestattet, eingehende Daten automatisiert auf Schadprogramme durchsuchen zu lassen („Virenscanner“) und Maß-

[176] Seite 62 ff.

nahmen zur Abwehr etwa aufgefundener Schadprogramme zu treffen (vgl. § 14 BDSG). Es bedarf keiner Ermächtigung einer Zentralbehörde, sich in die behördliche oder private Kommunikation mit Bundesorganen und ihren Angehörigen einzuschalten und die übermittelten Inhalte automatisiert auszuwerten. Insoweit wird auf die obigen Ausführungen Bezug genommen.[177]

Jedenfalls sprengt § 5 BSIG dadurch die Grenzen der Verhältnismäßigkeit, dass er zu einer personenbezogenen, vollkommen anlasslosen und flächendeckenden Aufzeichnung und Auswertung von Informationen über das gesamte Informations- und Kommunikationsverhalten im Verhältnis von Bürger und Bund ermächtigt. Die Tiefe des damit verbundenen Eingriffs in die Grundrechte der Bürger und Bundesangehörigen steht offensichtlich außer Verhältnis zu dem damit erhofften, nicht nachweisbaren Sicherheitsgewinn im Vergleich zu den auch ohne § 5 BSIG verfügbaren und erforderlichen Schutzmöglichkeiten.

(8) Unverhältnismäßige Vorratsdatenspeicherung (§ 5 Abs. 2 BSIG)

§ 5 Abs. 2 BSIG ermächtigt das Bundesamt für Sicherheit in der Informationstechnik, die näheren Umstände der elektronischen Kommunikation mit Bundesbehörden (§ 2 Abs. 8 BSIG) drei Monate lang auf Vorrat zu speichern. Dies betrifft namentlich Verkehrsdaten über die computergestützte Kommunikation mit Bundesbehörden (z.B. E-Mail) sowie Daten über die Nutzung öffentlicher Telemedien von Bundesorganen (§ 2 Abs. 8 S. 2 BSIG).

§ 5 Abs. 2 BSIG ist zur Erreichung seines Zwecks bereits ungeeignet, weil seine Voraussetzungen nicht eintreten können. Die Vorschrift setzt tatsächliche Anhaltspunkte für die Annahme voraus, dass Protokolldaten zur Unschädlichmachung aufgefundener Schadprogramme oder zur Erkennung oder Abwehr von Schadprogrammen „erforderlich sein können“. Es ist jedoch oben bereits ausgeführt worden, weshalb Verkehrs- und Nutzungsdaten weder zur Erkennung, noch zur Abwehr oder Beseitigung von Schadprogrammen erforderlich sind. Zur Vermeidung von Wiederholungen wird auf die obigen Ausführungen Bezug genommen.[178]

Geht man hingegen – entgegen der hier vertretenen Auffassung – von der Eignung der Norm aus, so ist die darin vorgesehene globale und pauschale Vorratsdatenspeicherung jedenfalls grob unverhältnismäßig. Dass § 5 Abs. 2 BSIG eine globale und pauschale Vorratsdatenspeicherung vorsieht, ergibt sich aus den folgenden Überlegungen:

§ 5 Abs. 2 BSIG soll zu einer Vorratsdatenspeicherung ermächtigen, wenn tatsächliche Anhaltspunkte für die Annahme bestehen, dass die zu speichernden Daten bei Feststellung eines Schadprogramms zur Abwehr hiervon oder von anderen Schadprogrammen ausgehender Gefahren „erforderlich sein können“. Das BSI beabsichtigt, im Fall eines anderweitig festgestellten Schadprogramms anhand von Vorratsdaten nachzuprüfen, welche

[177] Seite 28 ff.

[178] Seite 62.

anderen Verbindungen über dieselbe Quelle (Server) hergestellt worden sind, um zu überprüfen, ob auch bei anderen Empfängern ein Schadprogramm aktiviert worden ist. Dass eine Vorratsdatenspeicherung zu diesem Zweck nicht erforderlich ist und mildere, geeignetere Mittel zur Verfügung stehen, ist bereits oben ausgeführt worden.[179] Unterstellte man mit dem Gesetzgeber und dem BSI jedoch die Erforderlichkeit dieser Vorgehensweise, so lägen die Voraussetzungen des § 5 Abs. 2 S. 1 Var. 1 BSIG immer und permanent vor. Tatsächliche Anhaltspunkte lassen sich stets darin erblicken, dass Bundesorgane – wie jeder Internetnutzer – Versuchen zur Einschleusung von Schadprogrammen ausgesetzt sind (etwa in Form von Spam-E-Mails) und dass mitunter wohl auch (bei dem Bund wie bei Bürgern) eine Infektion mit Schadprogrammen auftritt. Nach Auffassung des Gesetzgebers und des BSI ist die präventive Aufzeichnung sämtlicher Verbindungen immer erforderlich, um im Fall der Feststellung eines Schadprogramms überprüfen zu können, welche anderen Verbindungen über dieselbe Quelle (Server) hergestellt worden sind.

Dementsprechend führte der damalige Präsident des BSI zu § 5 Abs. 2 BSIG-E aus:[180]

> „*Eine ausreichende Frist vor einer endgültigen Löschung ist zwingend erforderlich, da Schadprogramme in der Regel erst mit einem zeitlichen Verzug von mehreren Tagen oder Wochen detektiert werden können. Wird ein neues Schadprogramm gefunden, besteht die Notwendigkeit, rückwirkend zu untersuchen, ob das Programm bereits zuvor innerhalb der Bundesverwaltung verbreitet wurde. Nur auf diese Weise können etwaige Schäden, die durch das Schadprogramm verursacht werden, vermieden oder begrenzt werden.*“

Die mit der Anwendung betraute Behörde hält die in § 5 Abs. 2 BSIG vorgesehene Vorratsdatenspeicherung also unabhängig vom Einzelfall stets für „zwingend erforderlich“. Das BSI legt die Norm als Ermächtigung zu einer anlassunabhängigen und flächendeckenden Vorratsdatenspeicherung aus und wird sie auch so anwenden.

Es ist bereits ausgeführt worden, dass die mit einer globalen und pauschalen Aufzeichnung und Aufbewahrung von Informationen über die Kommunikation mit Bundesbehörden verbundenen Nachteile grob außer Verhältnis zu dem vermeintlichen damit verbundenen Nutzen steht.[181] Selbst wenn damit in seltenen Einzelfällen Sicherheitsvorteile verbunden wären (was nicht der Fall ist), stünde der damit verbundene Eingriff in die freie Kommunikation jedenfalls vollkommen außer Verhältnis zu dem Zusatznutzen der Maßnahme gegenüber den ohnehin verfügbaren milderen Mitteln.

---

[179] Seite 62.

[180] Helmbrecht, INA-Drs. 16(4)570 A, 7.

[181] Seite 62 ff.

(9) Ergebnis

Insgesamt ist festzuhalten, dass die in § 5 BSIG vorgesehene generelle, flächendeckende und permanente Aufzeichnung, Auswertung und Vorratsspeicherung des Informations- und Kommunikationsverhaltens der gesamten Bevölkerung über Bundesnetze das Verhältnismäßigkeitsgebot eklatant verletzt. Die staatlichen Behörden benötigen § 5 BSIG höchst selten, während mehr als 99% der von der Maßnahme Betroffenen[182] vollkommen unschuldig, unverdächtig und ungefährlich sind. Eine generelle Vorratsspeicherung von Telekommunikationsdaten, wie sie § 5 BSIG vorsieht, ist daher mit Art. 8 EMRK unvereinbar.[183]

Die aufgezeigten schädlichen Nebenwirkungen der in § 5 BSIG vorgesehenen allgemeinen Aufzeichnung, Auswertung und Vorratsspeicherung des Informations- und Kommunikationsverhaltens der gesamten Bevölkerung über Bundesnetze stehen in keinem Verhältnis zu dem praktischen Zusatznutzen einer solchen Maßnahme für die vom Gesetzgeber angestrebten Zwecke. Mit Ausnahme des Bundes arbeiten alle öffentlichen und privaten Behördennetzbetreiber seit Jahren erfolgreich ohne Befugnis zur anlasslosen Erfassung, Auswertung und Vorratsspeicherung personenbezogener Kommunikationsdaten. Es ist empirisch nicht zu belegen, dass die Netze dieser Anbieter häufiger gestört wären oder Fehler aufwiesen, dass aus den Netzen dieser Anbieter mehr rechtswidrige Nachrichten versandt oder Angriffe verübt würden oder dass diese Netze häufiger oder länger von Dritten gesperrt wären als die Netze von Anbietern, die eine anlasslose Vorratsspeicherung praktizieren. Die Vertraulichkeit, Verfügbarkeit und Integrität von Netzen ist in der

---

[182] Schaar, http://www.heise.de/ct/aktuell/meldung/62231.

[183] So zur Vorratsdatenspeicherung allgemein: Milford, The Data Retention Directive (2008), http://www.petermilford.com/downloads/Data_Retention_PMilford.pdf, 128; Mitrou, Communications Data Retention (2008), http://www.infosectoday.com/Articles/Communications_Data_Retention.pdf, 426; Feiler, The Data Retention Directive (2008), http://rechtsprobleme.at/doks/feiler-DataRetentionDirective.pdf, 26 ff; Deutscher Anwaltverein, Stellungnahme vom August 2007, http://www.anwaltverein.de/ 03/ 05/ 2007/ 41-07.pdf, 35 f.; Breyer, Telecommunications Data Retention and Human Rights (2005), http://www.daten-speicherung.de/data/data_retention_and_human_rights_essay.pdf, 372; Goemans/Dumortier, Mandatory retention of traffic data in the EU (2003), https://www.law.kuleuven.be/icri/publications/440Retention_of_traffic_data_Dumortier_Goemans.pdf, 19 f.; Art. 29-Gruppe der EU, Stellungnahme 5/2002, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp64_de.pdf und Stellungnahme 9/2004, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp99_de.pdf; Covington & Burling, Memorandum of laws concerning the legality of data retention with regard to the rights guaranteed by the European Convention on Human Rights vom 10.10.2003, http://www.statewatch.org/news/2003/oct/ Data_Retention_Memo.pdf, 3; Empfehlung des Europäischen Parlaments zu der Strategie zur Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität (2001/2070(COS)) vom 06.09.2001, Dokument Nr. T5-0452/2001, Buchst. H; EDSB-Konferenz, Europäische Datenschutzbeauftragte: Statement at the International Conference in Cardiff (09.-11.09.2002) on mandatory systematic retention of telecommunication traffic data, BT-Drs. 15/888, 176.

Praxis auch ohne generelle Vorratsdatenspeicherung in vollem Umfang gewährleistet. Bei dieser Sachlage ergibt die Abwägung eindeutig, dass Speicherinteressen in Einzelfällen hinter den Grundrechtsschutz der nahezu ausschließlich unbeteiligten Internetnutzer zurücktreten müssen.

Der Wunsch, technische Anlagen zu schützen, kann nicht das Grundrecht auf Datenschutz aushebeln. Die EMRK setzt ersichtlich auf ein weitaus voraussetzungsreicheres System des Rechtsgüterschutzes als eine generelle und undifferenzierte Aufzeichnung des Verhaltens der gesamten Bevölkerung. Zwar besteht ein legitimes Interesse am Schutz von Rechtsgütern. Doch darf, wo mehrere Prinzipien in Widerstreit geraten können, nicht eines auf Kosten des anderen schematisch oder gar absolut zu Geltung gebracht werden; insofern ist es von vornherein unstatthaft, eine Diskussion um Schutzmaßnahmen zu führen, ohne den Ausgleich zwischen öffentlichen Interessen und Privatheit mit einzubeziehen. Wissen und Aufklärung gehören zur Demokratie ebenso wie der rechtsstaatliche und schonende Umgang mit personenbezogenen Daten. Mit der Forderung nach totaler Nachvollziehbarkeit jeglicher elektronischer Information und Kommunikation werden gläserne Verhältnisse verlangt, der Bürger soll dem Staat zeigen, was er tut und wer er ist. Ein Rechtsstaat benötigt und erlaubt indes kein jakobinisches Schwert, mit dem man die Hülle privater Abwehrrechte durchschlagen könnte, um die „wahren" Verhältnisse offenzulegen. In einer Demokratie erfolgt der Schutz technischer Anlagen gezielt und anlassbezogen und nicht durch Totalkontrolle und –speicherung jeglichen Informations- und Kommunikationsverhaltens. Dies muss auch im Internetzeitalter gelten.

Die Menschenrechte der EMRK verlangen von den Unterzeichnerstaaten, zwischen dem Schutz technischer Anlagen und den Auswirkungen auf die Grundrechte der Betroffenen einen angemessenen Ausgleich herzustellen. An einem solchen rechtsstaatlichen Ausgleich fehlt es hier. Mit einer globalen und pauschalen Auswertung und Aufzeichnung wird dem öffentlichen Anliegen, die Informationstechnik zu schützen, kaum Rechnung getragen, aber jedenfalls zu einseitig der Vorrang gegenüber den berechtigten Interessen der Kommunizierenden und sich Informierenden an der Wahrung ihrer Privatsphäre eingeräumt.

In dieser Situation bleibt in Anlehnung an den Gerichtshof zu konstatieren, dass „die umfassende und wahllose" Aufzeichnung, Auswertung und Aufbewahrung von Informationen über jegliche Information und Kommunikation rechtstreuer Bürger über Bundesnetze keinen gerechten Ausgleich zwischen den widerstreitenden öffentlichen und privaten Interessen trifft und Deutschland in dieser Hinsicht jeden akzeptablen Ermessensspielraum überschritten hat.[184] § 5 BSIG stellt einen unverhältnismäßigen Eingriff in das Grundrecht der Kläger auf Achtung ihres Privatlebens dar, der nicht als notwendig in einer demokratischen Gesellschaft angesehen werden kann.

[184] Vgl. EGMR, S. und Marper-UK, Urteil vom 4.12.2008, Bsw. Nr. 30.562/04 und 30.566/04.

II. Verletzung des Art. 10 EMRK

1. Schutzbereich

Art. 10 Abs. 1 S. 1 und 2 EMRK bestimmt: „Jeder hat Anspruch auf freie Meinungsäußerung. Dieses Recht schließt die Freiheit der Meinung und die Freiheit zum Empfang und zur Mitteilung von Nachrichten oder Ideen ohne Eingriffe öffentlicher Behörden und ohne Rücksicht auf Landesgrenzen ein." Art. 10 EMRK schützt also unter anderem die Mitteilung und den Empfang von Tatsachen und Meinungen[185]. In technischer Hinsicht geschützt sind alle Kommunikationsformen[186], also auch die Nutzung der Telekommunikationsnetze. Es kommt nicht darauf an, ob es sich um private oder um öffentliche, um individuelle oder um Massenkommunikation handelt[187].

Dass das Recht auf freie Meinungsäußerung den Anspruch auf anonyme Meinungsäußerung umfasst, hat der US-amerikanische Oberste Gerichtshof (Supreme Court) schon früh anerkannt. Er hat dies in der Entscheidung Talley v. California[188] damit begründet, dass die „anonyme Meinungsäußerung" eine wertvolle Rolle für den „Fortschritt der Menschheit" gespielt habe. Verfolgte Gruppen seien im Lauf der Geschichte nur im Schutz der Anonymität in der Lage gewesen, Unterdrückungspraktiken und -gesetze zu kritisieren. Auch könne eine „Identifizierung und die Furcht vor Vergeltung von vollkommen friedlichen Diskussionen wichtiger öffentlicher Angelegenheiten abschrecken". Eine Pflicht zur Nennung der Verantwortlichen auf Flugzetteln hat der Gerichtshof daher als Verstoß gegen die Meinungsfreiheit verworfen.

In einer späteren Entscheidung[189] hat der Oberste Gerichtshof ausgeführt, Anonymität stelle oft ein „Schutzschild vor der Tyrannei der Mehrheit" dar. Nur im Schutz der Anonymität könne man seine Meinung äußern, ohne dass sie (auch unbewusst) allein wegen der Person des Äußernden (z.B. wegen seines Geschlechts, seiner Rasse, seiner Hautfarbe, seiner Religion, seiner Herkunft) abgelehnt werde. Auf diese Weise helfe die Anonymität der Verbreitung von Ideen. Anonyme Meinungsäußerungen „exemplifizieren den Zweck des Grundrechtskatalogs und insbesondere der Meinungsfreiheit: unbeliebte Personen vor Vergeltung in einer intoleranten Gesellschaft zu schützen – und ihre Ideen vor Unterdrükkung". Der Oberste Gerichtshof hat auch anerkannt, dass Vereine die Liste ihrer Mitglieder nicht offen legen müssen.[190] Es müsse möglich bleiben, anonym Mitglied eines unbeliebten Vereins zu sein, um die Freiheit auch unpopulärer Meinungen zu gewährleisten.

---

[185] Frowein/Peukert-Frowein, Art. 10, Rn. 5; Kugelmann, EuGRZ 2003, 16 (20) m.w.N.

[186] Frowein/Peukert-Frowein, Art. 10, Rn. 5; Kugelmann, EuGRZ 2003, 16 (19).

[187] Vgl. Frowein/Peukert-Frowein, Art. 10, Rn. 15 ff.

[188] 362 U.S. 60 (1960).

[189] McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995).

[190] NAACP v. Alabama ex. rel. Patterson, 357 U.S. 449 (1958).

Gewährleistet ist schließlich auch das Recht, sich anonym zu informieren.[191] Dies gebietet der Zweck der Meinungsfreiheit. Anonyme Informationskanäle erweitert den Zuhörerkreis von Meinungsäußerungen und erlaubt einen unbefangenen Zugang zu einer breiten Auswahl an Informationen. Dies ist etwa für die Verbreitung der Anliegen stigmatisierter und finanzschwacher „kleiner Leute" besonders wichtig. Wenn Menschen das Stigma vermeiden können, das mit dem Anhören bestimmter Tatsachen und Meinungen verbunden ist, werden sie eher bereit sein, sich damit vorurteilsfrei auseinanderzusetzen.

In den letzten Jahren haben die US-amerikanischen Instanzgerichte das Recht auf Anonymität auch auf das Internet angewandt. Der Washington District Court entschied 2001,[192] das Recht auf anonyme Meinungsäußerung sei von grundlegender Bedeutung für die Verabschiedung der US-amerikanischen Verfassung selbst gewesen, weil sowohl Befürworter („Federalist Papers") wie auch Widersacher ohne Namensnennung über die Ratifizierung der Verfassung stritten. Das Gericht entschied wörtlich: „Das Internet begünstigt den reichhaltigen, vielfältigen und weitreichenden Austausch von Ideen. Die Möglichkeit, seine Meinung im Internet äußern zu können, ohne dass die andere Seite alle Tatsachen über die eigene Identität kennt, kann offene Kommunikation und robuste Debatte fördern."[193] Larios hat eine Übersicht über die US-amerikanische Rechtsprechung zum Schutz der Anonymität von Internetnutzern durch das Grundrecht auf freie Meinungsäußerung veröffentlicht.[194]

Auch in Europa haben sich die politische Opposition und der Widerstand gegen die Obrigkeit immer wieder der Anonymität bedienen müssen. Berühmte Schriftsteller wie Erich Kästner oder Kurt Tucholsky schrieben nicht unter ihrem eigenen Namen. 1849 veröffentlichte der Rechtswissenschaftler Theodor Mommsen einen Kommentar über die in der neuen Verfassung von 1848 garantierten „Grundrechte des deutschen Volkes" – anonym. Im gleichen Jahr veröffentlichte Adolph Streckfuß sein Werk „Das freie Preußen. Geschichte des Berliner Freiheitskampfes vom 18. März 1848 und seine Folgen", ohne seinen Namen zu nennen.

Mit Urteil vom 25.03.2010 hat der Oberste Gerichtshof Israels bekräftigt, dass ein „Recht auf Anonymität" besteht.[195] Unter Bezugnahme auf die Rechtsprechung des US-amerikanischen Supreme Court führte der Gerichtshof aus, dass Bestandteil des Rechts

---

[191] Crump, 56 Stanford Law Review (2003), http://www.thefreelibrary.com/Data+retention%3A+privacy,+anonymity,+and+accountability+online.-a0110534145.

[192] Doe v. 2TheMart.com, 140 F.Supp.2d 1088.

[193] Doe v. 2TheMart.com, 140 F.Supp.2d 1088.

[194] Larios, Rutgers Law Record, Vol. 37, p. 36, 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1640133.

[195] Oberster Gerichtshof Israels, 4447/07 vom 25.03.2010, http://elyon1.court.gov.il/files/07/470/044/p10/07044470.p10.htm, Absatz-Nr. 11.

auf freie Meinungsäußerung auch das Recht auf anonyme Meinungsäußerung sei. Teilweise setze die Möglichkeit und Bereitschaft zur Äußerung einer Meinung voraus, dass dies anonym geschehen könne. Ursache könnten persönliche Gefühle wie Scham oder Mutlosigkeit sein, externer Druck oder die Besorgnis über Reaktionen der Außenwelt. Mitunter sei die Anonymität aber auch Bestandteil der zu äußernden Botschaft. Sie verhindere etwa, dass Annahmen über den Verfasser die geäußerte Meinung überlagern und verfälschen. Anonymität sei zugleich auch im Rahmen des Grundrechts auf Privatsphäre geschützt und ein wichtiger Bestandteil dieses Rechts. Anonymität gebe dem Betroffenen Kontrolle über Informationen über ihn. Im Bereich des Internets komme der Anonymität eine verstärkte Bedeutung zu. Das Internet ermögliche eine freie Meinungsäußerung in besonderem Maße. Auch im Rahmen des Rechts auf Privatsphäre komme der Anonymität im Internet besondere Bedeutung zu. Bei der Internetnutzung fielen – zum Teil unfreiwillig – Informationen über das Nutzungsverhalten an. Im Laufe der Zeit bildete sich so eine Datenbank mit persönlichen Daten, Meinungen und Interessen. Während früher alle Handlungen im Schutz der eigenen Wohnung vor Blicken von außen geschützt gewesen seien, könne im Zeitalter des Internets direkt und indirekt tief „in die Seele der Person eingedrungen“ werden. Diese Verletzung der Privatsphäre müsse „minimiert“ werden. Je größer die Möglichkeiten einer Auswertung des Nutzungsverhaltens, desto eher sei eine erhebliche Verhaltensänderung auf Seiten der Nutzer zu erwarten.

Soweit sich der Anwendungsbereich des Art. 10 EMRK mit dem des Art. 8 EMRK überschneidet, fragt es sich, ob ein Spezialitätsverhältnis anzunehmen ist oder ob beide Normen nebeneinander anzuwenden sind.[196] Dass Art. 8 EMRK nicht in jedem Fall das speziellere Grundrecht ist, ergibt sich daraus, dass Art. 8 EMRK die Privatsphäre allgemein schützt und nicht nur die Verbreitung von Tatsachenbehauptungen und Meinungen. Aber auch in Fällen, in denen sowohl Art. 8 EMRK als auch die Meinungsfreiheit einschlägig ist, weisen die Grundrechte unterschiedliche Schutzrichtungen auf: Während Art. 8 EMRK die Vertraulichkeit des Privatlebens schützen soll, schützt die Meinungsfreiheit das Recht, Tatsachenbehauptungen und Meinungen überhaupt frei äußern und verbreiten zu dürfen. Vor staatlicher Kenntnisnahme einer Äußerung schützt die Meinungsfreiheit nicht. Umgekehrt schützt Art. 8 EMRK nicht das Recht der freien Meinungsäußerung. Es ist nicht gerechtfertigt, durch die Annahme eines Spezialitätsverhältnisses die Meinungsfreiheit auf dem Gebiet der räumlich distanzierten Kommunikation quasi aufzuheben, zumal Art. 10 EMRK die freie Wahl des für eine Meinungsäußerung eingesetzten Mediums gewährleistet. In Anbetracht der unterschiedlichen Schutzzwecke müssen die Grundrechte aus Art. 8 und 10 EMRK nebeneinander anwendbar sein (Idealkonkurrenz). Dies bedeutet im Ergebnis, dass sich die Anforderungen beider Grundrechte kumulieren.

[196] Zur Diskussion Kugelmann, EuGRZ 2003, 16 (20) m.w.N.

2. § 5 BSIG als Eingriff

Es stellt sich die Frage, ob eine vorbeugende, generelle Aufzeichnung der näheren Umstände der Information und Kommunikation einen Eingriff in die Meinungsfreiheit darstellt. Der Zweck des Art. 10 EMRK gebietet es, dem Staat auch eine mittelbare Behinderung der freien Kommunikation als Eingriff zuzurechnen, wenn diese typischerweise und vorhersehbar den unbefangenen Austausch von Meinungen und Tatsachenbehauptungen beeinträchtigt.

Die in § 5 BSIG vorgesehene Aufzeichnung von Verkehrs- und Nutzungsdaten und Auswertung von Kommunikationsinhalten ermöglicht es, aufzudecken, wer per Individualkommunikation oder über Telemedien bestimmte Meinungen oder Tatsachenbehauptungen geäußert oder abgerufen hat. Die gilt etwa dort, wo der Bund Internet-Meinungsforen[197] oder Kontaktformulare anbietet. Über diese Kanäle kann der Bürger seine Meinung wegen § 5 BSIG nicht mehr ohne das Risiko einer Nachverfolgung anonym äußern. Auch kann man Meinungen und Informationen nicht mehr ohne das Risiko einer Nachverfolgung anonym abrufen.

Die in § 5 BSIG vorgesehene Informationserfassung und -auswertung kann von dem unbefangenen Gebrauch der Meinungs- und Informationsfreiheit abschrecken.[198] Die Identifizierbarkeit jeder Person, die eine bestimmte Meinung äußert, begründet die Gefahr, dass der Einzelne aus Furcht vor Repressalien oder sonstigen negativen Auswirkungen sich dahingehend entscheidet, seine Meinung gegenüber Bundesorganen nicht zu äußern. Dieser Gefahr der Selbstzensur soll das Grundrecht auf freie Meinungsäußerung gerade entgegen wirken.[199] Eine abschreckende Wirkung ist besonders in Bezug auf die Rückverfolgbarkeit staatskritischer Meinungen und Tatsachendarstellungen zu erwarten, deren freier Austausch in einer Demokratie von besonders hohem Wert ist.

§ 5 BSIG schreckt auch von dem unbefangenen Abruf öffentlich zugänglicher Telemedien des Bundes ab. Diese Gefahr besteht etwa dort, wo aus dem Seitenabruf wegen des Inhalts der Seite oder des Telemediums auf politische Meinungen, religiöse Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben des Internetnutzers geschlossen werden kann. Beispielsweise ermittelte das Bundeskriminalamt bis 2008 gegen Nutzer des Portals www.bka.de, die mit „signifikanter Zugriffsfrequenz“ Informationen über bestimmte kriminelle oder terroristische Vereinigungen von dem Portal abriefen. Die entsprechenden Nutzer wurden anhand ihrer IP-Adresse über § 113 TKG identifiziert und mit verschiedenen Datenbanken abgeglichen. Die aufgezeigte Verfahrensweise hat die Bundes-

---

[197] Beispielsweise http://www.bmg.bund.de/bmg_forum/ und http://www.cio.bund.de/kbst_forum/, wo ausdrücklich auch die IP-Adressen der Nutzer festgehalten werden.

[198] Vgl. BGH, NJW 2009, 2888.

[199] Vgl. BGH, NJW 2009, 2888.

regierung auf parlamentarische Anfragen öffentlich bestätigt.[200] Identifizierung und Datenbankabgleich wurden nach unbestrittenen Presseinformationen bei einer dreistelligen Anzahl von Personen durchgeführt, die in keinerlei Verbindung mit einer Straftat standen. In dem Pressebericht heißt es:[201]

> „*Ursprünglich hatte das BKA die Identität von 417 Personen feststellen wollen. Dabei handelte es sich nicht um Tatverdächtigte, sondern offenbar um alle Personen, die sich zwischen dem 28. März und dem 18. April diesen Jahres auf den Internetseiten des Bundeskriminalamtes über die ‚Militante Gruppe' informieren wollten. Weil aber ein großer Teil der IP-Adressen von Providern stammte, die diese nur kurze Zeit speichern, wurde die Identifizierung von ‚nur' rund 120 Telekom-Kunden beantragt. Das BKA habe ‚einen weiteren Teil' der IP-Adressen ‚Presseorganen bzw. einzelnen Firmen oder Universitäten' zugeordnet, heißt es. ‚Anhand dieser Daten werden weiterführende polizeiliche Ermittlungen wie unter anderem die Identifizierung weiterer Mitglieder der ‚militanten gruppe' (mg) ermöglicht', begründen die Beamten ihren Antrag.*"

Wenngleich § 5 BSIG eine derartige Verwendung der gespeicherten Daten nicht erlaubt, begründet doch schon die Erfassung von Nutzungsdaten die Gefahr von daraus resultierenden Nachteilen. Bereits von diesem Risiko geht eine abschreckende Wirkung aus. In Zeiten immer wiederkehrender Datenpannen und Datenmissbrauchs – auch bei Behörden – ist die Befürchtung von Nachteilen aufgrund von § 5 BSIG nicht irrational. Bis zur Einführung der Vorschrift hat der Gesetzgeber selbst anerkannt, dass von einer globalen und pauschalen Erfassung des Informations- und Kommunikationsverhaltens inakzeptable Risiken ausgehen (vgl. § 96 TKG, 15 TMG).

Die abschreckende Wirkung einer Erfassung des Informations- und Kommunikationsverhaltens schadet der Meinungsfreiheit und unserem Gemeinwesen überhaupt. Denn nur umfassende Informationen, die man ungehindert und unbefangen zur Kenntnis nehmen kann, ermöglichen eine freie Meinungsbildung und -äußerung für den Einzelnen wie für die Gemeinschaft.[202] Nur auf der Grundlage eines freien und unbefangenen Informationszugangs kann der Bürger informiert politische Entscheidungen treffen und am freiheitlichen demokratischen Gemeinwesen mitwirken. Ein nicht rückverfolgbarer Informationszugang ist heutzutage elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens.

Das Risiko einer Identifizierung kann nicht zumutbar durch Möglichkeiten anonymer Telekommunikationsnutzung aufgefangen werden, weil die Nutzung dieser Möglichkeiten zu-

---

[200] BT-Prot. 16/117, 22; BT-Drs. 16/6938.

[201] Tagesspiegel vom 30.09.2007, http://www.tagesspiegel.de/politik/deutschland/BKA-Datenschutz;art122,2390884.

[202] Vgl. BVerfGE 27, 71 (81).

sätzliche Kosten verursachen kann, die verfügbaren Dienste in ihrer Wirkung teilweise intransparent sind und weil zu ihrer Nutzung meist ein gewisses technisches Grundverständnis erforderlich ist, über das nicht jeder verfügt.

§ 5 BSIG behindert somit durch seine abschreckende Wirkung typischerweise und vorhersehbar den Austausch von Meinungen und Tatsachenbehauptungen. Nach dem modernen Eingriffsbegriff sind diese Wirkungen dem Staat als Grundrechtseingriff zuzurechnen. Ein Eingriff in die Meinungsfreiheit und die Informationsfreiheit liegt somit vor.

3. Mangelnde Rechtfertigung

Der Eingriff des § 5 BSIG in das Recht auf freie Meinungsäußerung ist nicht gerechtfertigt, weil § 5 BSIG das Gebot der Normenklarheit und das Verhältnismäßigkeitsgebot verletzt.

§ 5 BSIG stellt einen tiefgreifenden Eingriff in das Recht auf freien und unbefangenen Informationsaustausch dar. Die in § 5 BSIG vorgesehene Vorratsdatenspeicherung beseitigt die Möglichkeit des anonymen Informationsaustauschs über Bundesnetze fast vollständig. Jede Meinungsäußerung soll erfasst werden.

Wie bereits zu Art. 8 EMRK aufgezeigt, ist es evident unverhältnismäßig, alle Grundrechtsträger der Möglichkeit des anonymen und dadurch unbefangenen Informationsaustauschs zu berauben, nur um gegen den Missbrauch einiger weniger leichter vorgehen zu wollen.[203] Dies gilt insbesondere in Anbetracht der Tatsache, dass sich die Sicherheit von Informationssystemen in der Praxis auch ohne eine generelle und undifferenzierte Erfassung, Auswertung und Vorratsspeicherung des Meinungsaustauschs unbescholtener Bürger gewährleisten lässt. Technische Schutzmaßnahmen zur „Härtung“ der Informationstechnik sowie erforderlichenfalls ein anlassbezogenes Vorgehen ermöglichen einen ebenso guten, in jedem Fall aber einen hinreichenden Schutz informationstechnischer Systeme.

Zur Vermeidung von Wiederholungen wird im Übrigen auf die diesbezüglichen Ausführungen zu Art. 8 EMRK Bezug genommen,[204] die für Art. 10 EMRK entsprechend gelten.

---

[203] Wie hier: Crump, 56 Stanford Law Review (2003), http://www.thefreelibrary.com/Data+retention%3A+privacy,+anonymity,+and+accountability+online.-a0110534145.

[204] Seite 15 ff.

Sollte das Hohe Gericht wegen fehlender Ausführungen oder wegen mangelnder Substantiierung unseres Vortrags eine rechtlich nachteilhafte Entscheidung beabsichtigen, so wird um vorherige Gewährung rechtlichen Gehörs gebeten, also um einen Hinweis und um Einräumung einer Gelegenheit zur Ergänzung der Ausführungen.

Datum *Unterschrift des Beschwerdeführers zu 1*

Datum *Unterschrift des Beschwerdeführers zu 2*