

An das
Bundesverfassungsgericht
Schloßbezirk 3
76131 Karlsruhe

Verfassungsbeschwerde

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

Wir beantragen,

§ 5 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) in der Fassung von Artikel 1 des Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes vom 14.08.2009 (Bundesgesetzblatt Teil I, 2009, Nr. 54 vom 19.08.2009, S. 2821) für unvereinbar mit den Artikeln Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 sowie mit den Artikeln 3, 5 und 10 des Grundgesetzes und nichtig zu erklären.

Inhaltsübersicht

A.	GEGENSTAND DER VERFASSUNGSBESCHWERDE.....	4
B.	ANNAHMEVORAUSSETZUNGEN	8
C.	ZULÄSSIGKEIT DER VERFASSUNGSBESCHWERDE.....	9
D.	BEGRÜNDETHEIT DER VERFASSUNGSBESCHWERDE	11
I.	Verletzung der Art. 10 und Art. 2 Abs. 1, 1 Abs. 1 GG.....	11
1.	Schutzbereiche	11
2.	Grundrechtseingriff	12
a)	Art. 10 GG	12
b)	Art. 2 Abs. 1, 1 Abs. 1 GG	17
3.	Mangelnde Rechtfertigung.....	17
a)	Verletzung des Bestimmtheitsgebots	17
b)	Verletzung des Verhältnismäßigkeitsgebots	18
aa)	Legitimes Ziel	19
bb)	Verhältnismäßigkeit.....	19
(1)	Gewicht des Eingriffsinteresses an § 5 Abs. 1 S. 1 Nr. 1 BStG.....	19
(2)	Gewicht des beeinträchtigten Freiheitsinteresses	20
(a)	Maßgebliche Kriterien	20
(b)	Tragweite des § 5 Abs. 1 und 2 BStG	22
(c)	Insbesondere: Aussagekraft von Verkehrs- und Nutzungsdaten	24
(d)	Sicherheitsrisiken für Internetnutzer	25
(3)	Zentralisierung nicht erforderlich.....	27
(4)	Unverhältnismäßiges Erkennen und Beseitigen von Störungen und Fehlern (§ 5 Abs. 1 S. 1 Nr. 1 Var. 1 BStG)	28
(a)	Verkehrsdaten	29
(b)	Telemedien-Nutzungsdaten	31
(5)	Unverhältnismäßiges Erkennen und Beseitigen von Angriffen (§ 5 Abs. 1 S. 1 Nr. 1 Var. 2 BStG).....	34
(a)	Verkehrsdaten	39
(aa)	Schadprogramme.....	39
(bb)	Überflutung.....	40
(cc)	Einbruchsversuche	41
(b)	Telemedien-Nutzungsdaten	41
(aa)	Überflutung.....	42
(bb)	Einbruchsversuche	43
(6)	Unverhältnismäßige Abwehr von Schadprogrammen (§ 5 Abs. 1 S. 1 Nr. 2 BStG).....	44
(7)	Unverhältnismäßige Vorratsdatenspeicherung (§ 5 Abs. 2 BStG)	46
(8)	Die Rechtsprechung des Bundesverfassungsgerichts	47
II.	Verletzung des Art. 5 Abs. 1 S. 1 GG	50

1. Schutzbereich der Meinungsfreiheit.....	50
2. Schutzbereich der Informationsfreiheit	51
3. § 5 BStG als Eingriff in diese Grundrechte	53
4. Mangelnde Rechtfertigung.....	55
III. Verletzung des allgemeinen Gleichheitssatzes (Artikel 3 Abs. 1 GG)	55
1. Eingriff in den Schutzbereich des Art. 3 Abs. 1 GG	55
2. Rechtfertigungsmaßstab.....	56
3. Unterschiedliche Schutzwürdigkeit als Rechtfertigungsgrund?	58
4. Ergebnis.....	59

A. Gegenstand der Verfassungsbeschwerde

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

§ 5 BSI-Gesetz lautet:

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

(1) ¹Das 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.

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

(2) ¹Protokolldaten 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. ²Durch organisatorische und technische Maßnahmen ist sicherzustellen, dass eine Auswertung der nach diesem Absatz gespeicherten Daten nur automatisiert erfolgt. ³Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist. ⁴Eine nicht automatisierte Auswertung oder eine personenbezogene Verwendung ist nur nach Maßgabe der nachfolgenden Absätze zulässig. ⁵Soweit hierzu die Wiederherstellung des Personenbezugs pseudonymisierter Daten erforderlich ist, muss diese durch den Präsidenten des Bundesamts angeordnet werden. ⁶Die Entscheidung ist zu protokollieren.

(3) ¹Eine 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. ²Im 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.

³Ein Schadprogramm kann beseitigt oder in seiner Funktionsweise gehindert werden. ⁴Die 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) ¹Die 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. ²Die Unterrichtung kann unterbleiben, wenn die Person nur unerheblich betroffen wurde und anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat. ³Das 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. ⁴Der behördliche Datenschutzbeauftragte ist bei Ausübung dieser Aufgabe weisungsfrei und darf deswegen nicht benachteiligt werden (§ 4f Absatz 3 Bundesdatenschutzgesetz). ⁵Wenn der behördliche Datenschutzbeauftragte der Entscheidung des Bundesamtes widerspricht, ist die Benachrichtigung nachzuholen. ⁶Die Entscheidung über die Nichtbenachrichtigung ist zu dokumentieren. ⁷Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. ⁸Sie ist nach zwölf Monaten zu löschen. ⁹In den Fällen der Absätze 5 und 6 erfolgt die Benachrichtigung durch die dort genannten Behörden in entsprechender Anwendung der für diese Behörden geltenden Vorschriften. ¹⁰Enthalten diese keine Bestimmungen zu Benachrichtigungspflichten, sind die Vorschriften der Strafprozessordnung entsprechend anzuwenden.

(5) ¹Das 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. ²Es 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) ¹Für 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.

²Die Übermittlung nach Satz 1 Nummer 1 bedarf der vorherigen gerichtlichen Zustimmung.

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

(7) ¹Eine über die vorstehenden Absätze hinausgehende inhaltliche Auswertung zu anderen Zwecken und die Weitergabe von personenbezogenen Daten an Dritte sind unzulässig. ²Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. ³Werden 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. ⁴Erkenntnisse aus dem Kernbereich privater Lebensgestaltung sind unverzüglich zu löschen. ⁵Dies gilt auch in Zweifelsfällen. ⁶Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. ⁷Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. ⁸Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt. ⁹Werden 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 Beweis Zwecken 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) ¹Vor 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. ²Das Konzept hat dem besonderen Schutzbedürfnis der Regierungskommunikation Rechnung zu tragen. ³Die für die automatisierte Auswertung verwendeten Kriterien sind zu dokumentieren. ⁴Der 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).

B. Annahmeveraussetzungen

Der Verfassungsbeschwerde kommt grundsätzliche Bedeutung zu, weil sie verfassungsrechtliche Fragen aufwirft, die sich nicht ohne weiteres aus dem Grundgesetz beantworten lassen und noch nicht durch die verfassungsgerichtliche Rechtsprechung geklärt sind. Namentlich ist bislang nicht über die Zulässigkeit einer Vorratsspeicherung selbst von Internet-Nutzungsdaten unmittelbar durch eine staatliche Stelle entschieden worden. Dass die Zulässigkeit einer solchen Vorratsdatenspeicherung über den Einzelfall hinaus von grundlegender Bedeutung ist, liegt auf der Hand.

Die Annahme der Verfassungsbeschwerde ist daneben auch zur Durchsetzung der verletzten Grundrechte angezeigt. Die Grundrechtsverletzung hat in Anbetracht der hohen Eingriffsintensität besonderes Gewicht. Zudem hat sich der Gesetzgeber bewusst über Warnungen hinsichtlich der Unvereinbarkeit mit dem Grundgesetz hinweg gesetzt. Trotz massiver Kritik des Bundesrats¹ und von Sachverständigen,² in deren Rahmen auch ausdrücklich auf die Unvereinbarkeit mit den Grundrechten hingewiesen wurde,³ hat der Bundestag § 5 Abs. 1 und 2 BSIG-E im Kern unverändert verabschiedet, ohne die darin vorgesehene flächendeckende Vorratsdatenspeicherung auch nur ansatzweise verfassungsrechtlich zu rechtfertigen.

¹ BR-Drs. 62/09 (Beschluss), 5.

² BITKOM, Positionspapier vom 05.03.2009, 6; Deutscher Anwaltverein (DAV), Stellungnahme 2009-31 vom April 2009, INA-Drs. 16(4)588, 3; Breyer, Stellungnahme vom 07.05.2009, INA-Drs. 16(4)570 F, 14 ff.; Pfitzmann, Stellungnahme vom 07.05.2009, INA-Drs. 16(4)570 B, 1; Pohl (Präsident der Gesellschaft für Informatik e.V.), Stellungnahme vom 05.05.2009, INA-Drs. 16(4)570 C, 1 f.; Schaar, Stellungnahme vom 23.03.2009, INA-Drs. 16(4)570, 2.

³ Deutscher Anwaltverein (DAV), Stellungnahme 2009-31 vom April 2009, 3; Breyer, Stellungnahme vom 07.05.2009, INA-Drs. 16(4)570 F, 18.

C. Zulässigkeit der Verfassungsbeschwerde

Wir sind durch das angegriffene Gesetz unmittelbar, selbst und gegenwärtig in unseren Grundrechten betroffen. Andere zumutbare Abhilfemöglichkeiten, insbesondere die Anrufung der Fachgerichte, bestehen nicht.

Die Voraussetzung der eigenen und gegenwärtigen Betroffenheit ist erfüllt, wenn der Beschwerdeführer darlegt, dass er mit einiger Wahrscheinlichkeit durch die auf den angegriffenen Vorschriften beruhenden Maßnahmen in seinen Grundrechten berührt wird.⁴ 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, auswerten und drei Monate lang auf Vorrat speichern.

Unmittelbare Betroffenheit ist gegeben, wenn die angegriffenen Bestimmungen, ohne eines weiteren Vollzugsakts zu bedürfen, die Rechtsstellung des Beschwerdeführers verändern.⁵ Unmittelbare Betroffenheit ist aber auch dann anzunehmen, wenn der Beschwerdeführer gegen einen denkbaren Vollzugsakt nicht oder nicht in zumutbarer Weise vorgehen kann.⁶ Ein Vorgehen gegen den Vollzug ist insbesondere dann unzumutbar, wenn der Beschwerdeführer keine Kenntnis von dem Vollzug erlangt.⁷

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

⁴ BVerfGE 115, 118 (137) m.w.N.

⁵ BVerfGE 115, 118 (137) m.w.N.

⁶ BVerfGE 115, 118 (137) m.w.N.

⁷ BVerfGE 109, 279 (306).

soll eine Benachrichtigung nur „hinsichtlich der auch nichtautomatisiert verwendeten Daten“ erfolgen.⁸ 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“.⁹ 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 verarbeiteten Informationen vorgesehen ist. Hinsichtlich der Maßnahme nach § 5 Abs. 2 BSIG wird eine Auskunft daran scheitern, dass die Daten in pseudonymisierter (verschlüsselter¹⁰) 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,¹¹ 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

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

⁹ Rechtsausschuss des Bundestages; BT-Drs. 16/13259, 6.

¹⁰ Rechtsausschuss des Bundestages; BT-Drs. 16/13259, 6.

¹¹ BVerfGE 102, 197 (208).

ten hat,¹² 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.

Schließlich muss der Rechtsweg gegen den Gesetzesvollzug auch dann nicht in Anspruch genommen werden, wenn die Entscheidung von keiner weiteren tatsächlichen und rechtlichen Klärung abhängt und diejenigen Voraussetzungen gegeben sind, unter denen das Bundesverfassungsgericht gemäß § 90 Abs. 2 Satz 2 BVerfGG sofort entscheiden kann.¹³ So liegt es hier: Zur Entscheidung über die Vereinbarkeit des § 5 BSIG bedarf es keiner tatsächlichen oder rechtlichen Klärung durch die Fachgerichte, und die Verfassungsbeschwerde ist von allgemeiner Bedeutung (§ 90 Abs. 2 S. 2 Var. 1 BVerfGG). Die angefochtene Norm betrifft nämlich jeden Bundesbürger, der per Internet mit einer Bundesbehörde kommuniziert oder Informationen einsieht.

Die angefochtene Norm ist am Tag nach ihrer Verkündung in Kraft getreten.¹⁴ Damit ist die Beschwerdefrist des § 93 Abs. 3 BVerfGG gewahrt.

D. Begründetheit der Verfassungsbeschwerde

Die Verfassungsbeschwerde ist begründet, weil § 5 Abs. 1 und 2 BSIG mit den Grundrechten auf informationelle Selbstbestimmung (Art. 2 Abs. 1, Art. 1 Abs. 1 GG), auf Gleichbehandlung (Art. 3 GG), auf Meinungs- und Informationsfreiheit (Art. 5 GG) und auf Gewährleistung des Fernmeldegeheimnisses (Art. 10 GG) unvereinbar ist. Die weiteren Absätze des § 5 BSIG sind für nichtig zu erklären, weil sie auf den Absätzen 1 und 2 aufbauen und ohne diese keinen Sinn ergeben.

I. Verletzung der Art. 10 und Art. 2 Abs. 1, 1 Abs. 1 GG

1. Schutzbereiche

Das aus der Freiheitsgarantie des Art. 2 Abs. 1 GG und dem Schutz der Menschenwürde des Art. 1 GG folgende allgemeine Persönlichkeitsrecht umfasst die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen seine persönliche Lebenssachverhalte erhoben, gespeichert, verwendet oder weiter gegeben werden.¹⁵ Ein persönlicher Lebenssachverhalt liegt bereits dann vor, wenn die Verknüpfung des Lebenssachverhalts mit der zugehörigen Person möglich ist.¹⁶

¹² BVerfG, 1 BvR 2074/05 vom 11.3.2008, Absatz-Nr. 155.

¹³ BVerfG, 1 BvR 1936/05 vom 3.1.2007, Absatz-Nr. 15.

¹⁴ Art. 3 des Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes.

¹⁵ St. Rspr. seit BVerfGE 65, 1 (42 f.); in neuerer Zeit etwa BVerfGE 103, 21 (32 f.).

¹⁶ 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).

Soweit Informationen über den Fernmeldeverkehr betroffen sind, geht Art. 10 GG dem Grundrecht auf informationelle Selbstbestimmung vor. Art. 10 GG schützt vor den spezifischen Risiken für die Vertraulichkeit eines Kommunikationsvorgangs, die sich aus der Distanz der Kommunikation und aus der Einschaltung von Kommunikationsmittlern ergeben. Das Fernmeldegeheimnis bezweckt, die Kommunizierenden so zu stellen wie sie bei unmittelbarer Kommunikation stünden. Der Schutz des Fernmeldegeheimnisses erstreckt sich deswegen nicht auf Informationsweitergaben, die ein Kommunikationspartner willentlich veranlasst. Solche Verarbeitungen könnten auch im Fall der unmittelbaren Kommunikation erfolgen und sind nicht mehr von Schutzzweck des Fernmeldegeheimnisses erfasst.

Das Fernmeldegeheimnis schützt auch Telekommunikation, welche der Nutzung und Bereitstellung elektronischer Informations- und Kommunikationsdienste dient. Dies gilt auch dann, wenn die übertragenen Informationen öffentlich zugänglich sind, wie es etwa bei Telemedien der Fall sein kann. Da eine Unterscheidung zwischen Individual- und Massenkommunikation ohne eine der Schutzfunktion des Grundrechts zuwiderlaufende Anknüpfung an den Inhalt der jeweils übermittelten Information nicht möglich ist, ist bereits in der Speicherung der die Internetnutzung als solche betreffenden Daten ein Eingriff zu sehen.¹⁷ Dabei ist wohlgemerkt der Inhalt öffentlich zugänglicher Informationen als solcher nicht von Art. 10 Abs. 1 Var. 3 GG geschützt, sondern nur die Übermittlung dieses Inhalts an eine ihn abrufende Person sowie die näheren Umstände dieses Abruf- und Übermittlungsvorgangs. Der Staat greift also nur dann nicht in Art. 10 Abs. 1 Var. 3 GG ein, wenn er auf öffentlich zugängliche Informationen wie jeder andere zugreift, etwa mittels eines eigenen Internet-Anschlusses.¹⁸

2. Grundrechtseingriff

a) Art. 10 GG

§ 5 Abs. 1 und 2 BSIg greift in unser Fernmeldegeheimnis ein, indem das Bundesamt für Sicherheit in der Informationstechnik ermächtigt wird, Informationen über unsere informationstechnische Telekommunikation (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. Es ist anerkannt, dass ein Arbeitgeber jedenfalls dann zur Wahrung des Fernmeldegeheimnisses verpflichtet ist, wenn er seinen Angehörigen die private Nutzung seiner Kommunikationsmittel erlaubt. Dies ist bei vielen Bundesorganen der Fall, etwa bei der Bundes-

¹⁷ Vgl. BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 192.

¹⁸ BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. 293.

gung für Arbeit oder bei der Bundespolizei.¹⁹ Auch dem Beschwerdeführer zu 2 ist 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 Grundrecht auf Gewährleistung des Fernmeldegeheimnisses beider Kommunizierenden ein. Denn das Fernmeldegeheimnis 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 anerkannt, dass er in das Fernmeldegeheimnis eingreift (§ 11 BSIG).

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“).²⁰ 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 anonymen 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.²¹ Werden die einer Behörde vorliegenden Informationen einer anderen Behörde zugänglich gemacht, so wird damit in die Grundrechte des Betroffenen eingegriffen.²² Das Fernmeldegeheimnis als *lex specialis* zum Grundrecht auf informationelle Selbstbestimmung schützt mithin die Telekommunikation mit Bundesbehörden und –organen vor einer Einschaltung anderer Bundesbehörden in den Kommunikationsvorgang.

Soweit das Mithören durch einen Dritten im Einverständnis mit einem Kommunikationspartner keinen Eingriff in das Fernmeldegeheimnis des anderen Kommunikationspartners

¹⁹ Nach Ziff. 3.5 der „Richtlinie Telekommunikation Bund“ kann die private Nutzung dienstlicher Telekommunikationsanlagen zugelassen werden.

²⁰ BVerfG, 1 BvR 962/87 vom 18.12.1987, NJW 1988, 959.

²¹ Heußner, RDV 1988, 9; Simitis, BDSG, Einl., Rn. 36 m.w.N.

²² BVerwG, NJW 2005, 2330.

bedeutet,²³ liegt ein solcher Fall hier nicht vor. Weder hat der Kommunikationspartner des Bürgers dem BSI die Einschaltung „freiwillig ermöglicht“²⁴ (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.

Im Übrigen greift § 5 Abs. 1 und 2 BSIg jedenfalls insoweit in das Fernmeldegeheimnis ein, wie Mitarbeiter von Bundesbehörden mit Erlaubnis ihres Dienstherrn privat kommunizieren. Eine Aussonderung dieser Kommunikationsvorgänge ist dem BSI technisch nicht möglich. Schon um insoweit das Fernmeldegeheimnis zu wahren, muss § 5 Abs. 1 und 2 BSIg insgesamt dessen Anforderungen entsprechen.

Dem Grundrechtseingriff durch § 5 Abs. 1 BSIg steht nicht entgegen, dass die automatisierte Auswertung der erhobenen Daten grundsätzlich unverzüglich zu erfolgen hat und die Daten nach erfolgtem Abgleich sofort und spurlos zu löschen sind. Dem Wortlaut nach schützt das Grundrecht auf informationelle Selbstbestimmung vor jeglicher Erhebung, Speicherung, Verwendung und Weitergabe persönlicher Lebenssachverhalte.²⁵ Dasselbe muss für das spezielle Fernmeldegeheimnis in dessen Anwendungsbereich gelten. Die Erhebung von Protokoll- und Inhaltsdaten und sowie ihre automatisierte Auswertung stellt zweifellos eine Erhebung und Verwendung personenbeziehbarer Lebenssachverhalte dar. Nach bislang ständiger Rechtsprechung liegt schon in der Erfassung personenbezogener Daten ein Grundrechtseingriff, weil die Datenerhebung eine nachfolgenden Datenverarbeitung ermöglicht. An einem Eingriff fehlt es nur, soweit Daten ungezielt und allein technikbedingt miterfasst, unmittelbar nach der Erfassung aber technisch wieder spurlos, anonym und ohne die Möglichkeit, einen Personenbezug herzustellen, ausgesondert werden.²⁶ 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 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.

²³ BVerfG, 1 BvR 1611/96 vom 9.10.2002.

²⁴ BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. 291.

²⁵ St. Rspr. seit BVerfGE 65, 1 (42 f.); in neuerer Zeit etwa BVerfGE 103, 21 (32 f.).

²⁶ BVerfGE 100, 313 (366); BVerfGE 107, 299 (328); BVerfGE 115, 320 (343); BVerfG, NJW 2008, 1505 (1506 f.).

Eine spätere Löschung kann die voran gegangenen Grundrechtseingriffe nicht ungeschehen machen. Grundrechtsdogmatisch und aus Gründen der Rechtssicherheit überzeugt es nicht, die Eingriffsqualität einer Maßnahme von zeitlich nachgelagerten, noch nicht feststehenden Schritten abhängig zu machen.

Auch der Schutzzweck des Fernmeldegeheimnisses spricht für die Annahme eines Grundrechtseingriffs. Das Grundrecht soll die unbefangene Inanspruchnahme der grundrechtlich geschützten Freiheiten der Betroffenen gewährleisten.²⁷ 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. Schon von diesem Risiko von Nachteilen geht eine abschreckende Wirkung auf die unbefangene Telekommunikation aus.

In seiner Entscheidung zum Kfz-Massenabgleich hat das Bundesverfassungsgericht die Auffassung vertreten, eine automatisierte Erfassung von Kraftfahrzeugkennzeichen zwecks Abgleichs mit dem Fahndungsbestand greife nicht in das Grundrecht auf informationelle Selbstbestimmung ein, wenn das betroffene Kennzeichen nach dem Abgleich mit dem Fahndungsbestand ohne weitere Auswertung sofort und spurlos wieder gelöscht werde. In einem solchen Fall habe sich das behördliche Interesse an den betroffenen Daten noch nicht „derart verdichtet“, dass ein Grundrechtseingriff anzunehmen sei. Diese Formel ist abzulehnen, weil in ihr eine Vorverlagerung der rechtfertigenden Abwägung in die Eingriffsprüfung zum Ausdruck kommt. Das Bundesverfassungsgericht hat die von ihm postulierte Einschränkung des Grundrechts auf informationelle Selbstbestimmung auch selbst nicht konsequent verfolgt. Fehlte dem Kfz-Kennzeichenabgleich im Nichttrefferfall die Eingriffsqualität, so wären die nicht im Fahndungsbestand gespeicherten Personen von der Maßnahme nicht in ihren Rechten betroffen und könnten sich nicht dagegen zur Wehr setzen. Das Bundesverfassungsgericht sieht hingegen zutreffend „jeden Kraftfahrzeughalter, dessen Fahrzeug auf den Straßen des betroffenen Bundeslandes unterwegs ist“, als betroffen an, selbst wenn sein Kennzeichen nicht in polizeilichen Datenbeständen verzeichnet ist.²⁸ Betroffener einer Überwachung sei „jeder, in dessen Persönlichkeitsrechte durch die Maßnahme eingegriffen wird“. ²⁹ Hier hat das Gericht also doch einen Grundrechtseingriff durch den Datenabgleich angenommen. Im weiteren hat das Gericht umfangreich dargestellt, unter welchen Voraussetzungen ein Kfz-Massenabgleich gesetzlich zugelassen werden darf³⁰ – nicht anders, als wenn darin ein Grundrechtseingriff gesehen

²⁷ BVerfGE 100, 313 (376); BVerfG, NJW 2005, 2603 (2609).

²⁸ BVerfGE 120, 378 (396 f.).

²⁹ BVerfGE 120, 378 (396 f.).

³⁰ BVerfGE 120, 378 (429 f.).

worden wäre. Auch sonst hat das Gericht an seine Einschränkung des Schutzbereichs keine Konsequenzen geknüpft und nicht anders entschieden, als bei Anwendung der bewährten Schutzbereichsdefinition aus dem Volkszählungsurteil zu entscheiden gewesen wäre. Da die nur cursorisch begründete Linie des Urteils zur automatisierten Kennzeichenerfassung zu den aufgezeigten Widersprüchen führt, muss wieder zu der bewährten Rechtsprechung zurück gekehrt werden. Danach greift die Erfassung und Erhebung von Protokoll- und Inhaltsdaten ebenso in die Grundrechte der Betroffenen ein wie die anschließende Auswertung der erhobenen Daten.

Selbst wenn man der vorbezeichneten Rechtsprechung folgen wollte, läge in § 5 Abs. 1 BSIG ein Grundrechtseingriff. Das Bundesverfassungsgericht hat einen Eingriff in das Recht auf informationelle Selbstbestimmung nur abgelehnt, wenn der Abgleich der erhobenen Kfz-Kennzeichen mit dem Fahndungsbestand unverzüglich vorgenommen wird.³¹ Anders als im Fall der automatisierten Kennzeichenerkennung sieht § 5 Abs. 1 BSIG jedoch nicht nur einen bloßen Abgleich der erhobenen Daten mit einem vorhandenen „Fahndungsbestand“ vor, sondern eine „Auswertung“ der erhobenen Daten. Nach der Gesetzesbegründung sollen Logfiles von Servern, Firewalls usw. erhoben und automatisiert ausgewertet werden.³² 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.³³ 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 einen konkreten Gefährdungstatbestand begründet. Damit unterscheidet sich die „unverzügliche Auswertung“ nach § 5 Abs. 1 BSIG grundlegend von dem „unverzüglichen Abgleich“ von Kfz-Kennzeichen mit dem Fahndungsbestand, über den das Bundesverfassungsgericht 2008 zu entscheiden hatte. Das Gebot der „unverzüglichen Auswertung“ gewährleistet nicht, dass die erhobenen Daten unmittelbar nach der Erfas-

³¹ BVerfGE 120, 378 (399).

³² Bundesregierung, BT-Drs. 16/11967, 14.

³³ Helmbrecht, INA-Drs. 16(4)570 A, 6.

sung wieder gelöscht werden. Werden erfasste Daten aber im Speicher festgehalten und können sie gegebenenfalls Grundlage weiterer Maßnahmen werden, so liegt auch nach der Rechtsprechung des Bundesverfassungsgerichts ein Grundrechtseingriff vor.³⁴

Die in § 5 Abs. 2 BSI vorgesehene Pseudonymisierung steht dem Grundrechtseingriff nicht entgegen. Ein Eingriff in das Fernmeldegeheimnis liegt bereits dann vor, wenn die Verknüpfung des Lebenssachverhalts mit der zugehörigen Person möglich ist.³⁵ 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 BSI). Im Übrigen sind Internetnutzungs- und -verkehrsdaten regelmäßig bereits pseudonymisiert. IP-Adressen und E-Mail-Adressen stellen meist Pseudonyme dar. 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 Klurname des Absenders oder Empfängers angegeben ist oder wenn die E-Mail-Adresse den Klarnamen enthält.

b) Art. 2 Abs. 1, 1 Abs. 1 GG

Verneint man einen Eingriff in das Fernmeldegeheimnis, so greift § 5 Abs. 1 und 2 BSI jedenfalls in unser Grundrecht auf informationelle Selbstbestimmung ein.

3. Mangelnde Rechtfertigung

Der in § 5 BSI liegende Eingriff in das Fernmeldegeheimnis, hilfsweise das Grundrecht auf informationelle Selbstbestimmung, ist verfassungsrechtlich nicht gerechtfertigt.

a) Verletzung des Bestimmtheitsgebots

§ 5 Abs. 1 S. 2 BSI verletzt das verfassungsrechtliche Gebot der Normenklarheit.

Nach § 5 Abs. 1 S. 2 BSI erfolgt die in Satz 1 vorgesehene automatisierte Auswertung des Kommunikationsverkehrs „unverzüglich“, also ohne schuldhaftes Zögern (§ 121 BGB). 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 BSI unausgesprochen – zu speichern, solange die Verzögerung nicht schuldhaft erfolgt, also unter Beachtung der „im Verkehr erforderlichen Sorgfalt“ (§ 276 BGB).

³⁴ BVerfGE 120, 378 (399).

³⁵ BVerfGE 100, 313 (366).

Im Zusammenhang mit § 5 Abs. 1 BSIG ist der Begriff „unverzüglich“ zu unbestimmt. Vor dem Hintergrund der hohen Eingriffsintensität der Ermächtigung hätte der Gesetzgeber festlegen müssen, ob und wie lange die auszuwertenden Daten gespeichert werden dürfen und wann ihre Löschung erfolgen muss. Die Bedeutung der Frage ist sehr groß, weil § 5 Abs. 1 S. 1 BSIG zu einer Speicherung und Auswertung der gesamten Internetkommunikation mit 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).

Im Rahmen des § 121 BGB wird als „unverzüglich“ noch ein Handeln innerhalb von zwei Wochen angesehen. Der Bundesdatenschutzbeauftragte hat es als „unverzügliche“ Löschung im Sinne des § 96 Abs. 2 TKG angesehen, wenn Verkehrsdaten erst nach siebentägiger Aufbewahrung gelöscht werden.³⁶ Der Begriff „unverzüglich“ ist im Zusammenhang mit der Regelung des § 5 BSIG nach alledem zu unbestimmt. Auf die unbestimmte Tragweite des Begriffs „unverzüglich“ ist der Gesetzgeber – ohne Erfolg – schon in der Sachverständigenanhörung hingewiesen worden.³⁷

§ 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 es versäumt, festzulegen, ob er zu einer automatisierten Auswertung in Echtzeit oder zu einer automatisierten Auswertung in bestimmten, festzulegenden Zeitabständen ermächtigen will. Dies genügt dem Gebot der Normenklarheit in Anbetracht der Eingriffsintensität des § 5 BSIG nicht. 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 präzise Regelung der Frage hat der Gesetzgeber indes verzichtet, was mit dem Gebot der Normenklarheit angesichts der Intensität des Grundrechtseingriffs nicht in Einklang zu bringen ist.

b) Verletzung des Verhältnismäßigkeitsgebots

Die in § 5 Abs. 1 S. 1 Nr. 1 BSIG vorgesehene Ermächtigung des BSI zur Erhebung und Auswertung von Verkehrs- und Nutzungsdaten verletzt das Verhältnismäßigkeitsgebot im engeren Sinne. Dieses verlangt, dass der Verlust an grundrechtlich geschützter Freiheit nicht in einem unangemessenen Verhältnis zu den Gemeinwohlzwecken stehen darf, de-

³⁶ Schaar, Antwort vom 16.03.2007, <http://www.vorratsdatenspeicherung.de/content/view/89/79/>.

³⁷ Breyer, Protokoll Nr. 16/94 der Anhörung am 11.05.2009, http://www.bundestag.de/ausschuesse/a04/anhoerungen/Anhoerung_21/Protokoll.pdf, 42.

nen die Grundrechtsbeschränkung dient.³⁸ Der Gesetzgeber muss zwischen den Allgemein- und Individualinteressen einen angemessenen Ausgleich herbeiführen.³⁹ Dabei ist eine grundsätzliche Freiheitsvermutung zu beachten.⁴⁰ Jede Grundrechtsbeschränkung muss durch überwiegende Allgemeininteressen gerechtfertigt sein.⁴¹

§ 5 Abs. 1 S. 1 Nr. 1 BSIG genügt diesen Anforderungen nicht. Das grundrechtlich geschützte Interesse der Vielzahl von Bürgern, Informationen des Bundes ohne Furcht vor Aufdeckung des Informationsverhaltens abrufen und mit Bundesbediensteten ohne Furcht vor Aufdeckung des Kommunikationsverhaltens kommunizieren zu können, überwiegt das Interesse des Bundes daran, seine Informationstechnik in 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.

bb) Verhältnismäßigkeit

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

(1) Gewicht des Eingriffsinteresses an § 5 Abs. 1 S. 1 Nr. 1 BSIG

Dass erhebliches Interesse an der Funktionsfähigkeit und Vertraulichkeit der Informationstechnik des Bundes besteht, ist bereits ausgeführt worden. Die Bestimmung des Gewichts der Rechtsgüter, deren Schutz der Grundrechtseingriff dient, darf aber 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 in den Blick zu nehmen und das Maß an Eignung zur Erreichung der verfolgten Ziele zu bestimmen. Eine kaum taugliche Maßnahme vermag nur

³⁸ BVerfGE 100, 313 (375 f.).

³⁹ BVerfGE 100, 313 (375 f.).

⁴⁰ BVerfGE 6, 55 (72); BVerfGE 32, 54 (72); BVerfGE 55, 159 (165); BVerfGE 103, 142 (153): „Derjenigen Auslegung einer Grundrechtsnorm ist der Vorrang zu geben, die ihre Wirksamkeit am stärksten entfaltet.“

⁴¹ St. Rspr. seit BVerfGE 65, 1 (44, 46); in neuerer Zeit etwa BVerfGE 100, 313 (375 f.); BVerfGE 109, 279 (376).

leichte Grundrechtseingriffe aufzuwiegen, während eine zur Abwehr schwerer Gefahren unabdingbare Maßnahme tiefere Grundrechtseingriffe rechtfertigen kann.

(2) *Gewicht des beeinträchtigten Freiheitsinteresses*

Dem vermeintlichen Interesse an einer personenbezogenen Totalprotokollierung der Internetkommunikation mit Bundesorganen steht ein tiefgreifender Grundrechtseingriff gegenüber. § 5 BSIG ermächtigt dazu, Informationen über jede dienstliche und private Kommunikation mit Behörden und Bediensteten des Bundes sowie jede Nutzung von Internetportalen des Bundes ohne Anlass oder Verdacht in personenbezogener Form aufzuzeichnen und auszuwerten. § 5 BSIG ermächtigt weiter dazu, Informationen über jede dienstliche und private Kommunikation der Bediensteten und Abgeordneten des Bundes sowie ihre gesamte Nutzung des World Wide Web ohne Anlass oder Verdacht in personenbezogener Form aufzuzeichnen und auszuwerten. Eine Kommunikation und Information ohne das Risiko einer Rückverfolgung und daran anschließender Nachteile wird dadurch unmöglich gemacht.

(a) Maßgebliche Kriterien

Das Gewicht eines Grundrechtseingriffs bemisst sich der Rechtsprechung des Bundesverfassungsgerichts zufolge danach, unter welchen Voraussetzungen Eingriffe zulässig sind, welche und wie viele Grundrechtsträger von ihnen betroffen sind und wie intensiv die Grundrechtsträger beeinträchtigt werden.⁴² Zu berücksichtigen ist auch, ob und in welcher Zahl Personen mitbetroffen werden, die für den Eingriff keinen Anlass gegeben haben.⁴³ Die Eingriffsintensität hängt bei Informationseingriffen unter anderem von Art, Umfang und denkbarer Verwendungen der erhobenen Daten sowie von der Gefahr ihres Missbrauchs ab.⁴⁴ 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.⁴⁵ 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.⁴⁶

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 Hin-

⁴² BVerfGE 109, 279 (353).

⁴³ BVerfGE 109, 279 (353).

⁴⁴ BVerfGE 65, 1 (46).

⁴⁵ BVerfGE 100, 313 (376).

⁴⁶ BVerfGE 65, 1 (45).

tergrund 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 Missbrauchs, 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“.⁴⁷ Eine reale Missbrauchsgefahr ist im Rahmen der Abwägung demgegenüber durchaus zu berücksichtigen.⁴⁸ Die Grundrechte schützen den Einzelnen nämlich auch „vor fehlerhafter, missbräuchlicher oder exzessiver Verwertung von Kommunikationsdaten durch [...] staatliche Stellen“.⁴⁹ Die „in der Gesprächsbeobachtung liegende Gefahr einer Grundrechtsverletzung der [...] Gesprächsteilnehmer wie auch die Gefahr der Sammlung, Verwertung und Weitergabe der Informationen zu anderen Zwecken“ als den gesetzlich vorgesehenen darf daher nicht aus den Augen verloren werden.⁵⁰ Wenn das Grundgesetz das unbefangene Gebrauchmachen von Grundrechten 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 Grundrechtsträgern konkret aufgrund der Überwachungsmaßnahmen drohen. Ebenso zu berücksichtigen sind entferntere Risiken, deren Eintritt von den Bürgern nicht ohne Grund befürchtet wird.⁵¹ 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.

Auch eine nur kurzfristige Speicherung von Verkehrsdaten berührt das Interesse des Betroffenen an der Wahrung seines Fernmeldegeheimnisses in nicht ganz unerheblichem Ausmaß.⁵² Aufgrund der Speicherung kann der Bund diese Daten zu eigenen Zwecken verwenden.⁵³ Auch das Risiko eines Missbrauchs der Verkehrsdaten durch den Bund oder

⁴⁷ BVerfGE 30, 1 (27).

⁴⁸ BVerfGE 65, 1 (45 f.).

⁴⁹ BVerfGE 85, 386 (397).

⁵⁰ BVerfGE 85, 386 (400).

⁵¹ BVerfGE 100, 313 (376).

⁵² BVerfG, 1 BvR 1811/99 vom 27.10.2006, Absatz-Nr. 16.

⁵³ Vgl. BVerfG, 1 BvR 1811/99 vom 27.10.2006, Absatz-Nr. 17.

durch Dritte, die sich unbefugt Zugang zu ihnen verschaffen, ist nicht völlig auszuschließen.⁵⁴

Auf die Frage, inwieweit von einer gesetzlichen Eingriffsermächtigung tatsächlich Gebrauch gemacht wird, kann es bei der Beurteilung der Eingriffsintensität richtigerweise nicht ankommen,⁵⁵ weil eine Vollzugspraxis jederzeit geändert werden kann⁵⁶ 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.⁵⁷ 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.⁵⁸

(b) Tragweite des § 5 Abs. 1 und 2 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 pauschal⁵⁹ – ermächtigt. Es erfolgt eine flächendeckende Erfassung⁶⁰ des computergestützten Kommunikations- und Informationsverhaltens im Verhältnis der Bürger zu 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 uneinträchtigte computergestützte Kommunikation mit Behörden, Mitarbeitern und Abgeordneten des Bundes und keine uneinträchtigte 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 keine Angriffe auf die Informationstechnik des Bundes ausgehen. Zu schätzungsweise über 99,9% sind daher unschuldige und ungefährliche Bürger betroffen und ist eine Aufzeichnung von vornherein überflüssig. Die Ermächtigung setzt keine Verantwort-

⁵⁴ Vgl. BVerfG, 1 BvR 1811/99 vom 27.10.2006, Absatz-Nr. 17.

⁵⁵ MVVerfG, LKV 2000, 149 (154); AK-GG-Bizer, Art. 10, Rn. 86; a.A. wohl BVerfGE 100, 313 (376 ff.).

⁵⁶ Vgl. BVerfGE 100, 313 (380).

⁵⁷ EGMR, Khan-GB (2000), Decisions and Reports 2000-V, Abs. 27.

⁵⁸ Vgl. BVerfGE 100, 313 (384 f.).

⁵⁹ Vgl. BVerfGE 313, 100 (376 und 383).

⁶⁰ Vgl. dazu BVerfGE 313, 100 (377).

lichkeit oder wenigstens Gefahrennähe der Betroffenen voraus. Der bloße informationstechnische Kontakt oder Informationsabruf führt zur Aufzeichnung.

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.

Als weiteres Kriterium für die Bestimmung der Eingriffsintensität fragt das Bundesverfassungsgericht nach der 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. § 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.⁶¹ Dem Bürger wird nicht mitgeteilt, ob und inwieweit das Bundesamt von seinen Befugnissen nach § 5 Abs. 1 BSiG Gebrauch macht.

Die verdachtslose Totalregistrierung des Kommunikationsverhaltens zwischen Bürger und Staat oder dessen Mitarbeitern ist ein tiefgreifender Grundrechtseingriff. Zur Vermeidung von Wiederholungen wird vollumfassend auf den Vortrag zur Verfassungsbeschwerde gegen § 113a TKG im Verfahren 1 BvR 256/08 Bezug genommen, weil auch § 113a TKG eine Totalprotokollierung des Kommunikationsverfahrens zum Gegenstand hatte.

Während § 113a Abs. 8 TKG dies noch im Einklang mit zwingendem Verfassungsrecht⁶² ausschloss, ermächtigt § 5 BSiG nun erstmals auch zur Protokollierung des Nutzungsverhaltens von Telemedien 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 be-

⁶¹ Bundesrat, BT-Drs. 16/12225, 3.

⁶² BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 218.

trachtet 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 gehobenen⁶³ Grundsatz der §§ 13, 15 TMG, demzufolge Nutzungsdaten nicht über die Dauer des Nutzungsvorgangs hinaus aufbewahrt werden dürfen, bedeutungslos. Sie ist nicht auf eine Erfassung „im Einzelfall“ bei Vorliegen einer konkreten Störung beschränkt, sondern erlaubt eine anlasslose, globale und pauschale Aufzeichnung unserer Internetnutzung.

(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 Verwendungsmöglichkeit zu berücksichtigen ist.

Die Individualkommunikation mit Bundesorganen kann in hohem Maße Aufschluss auf das Privatleben von Personen und Geschäftsgeheimnisse von Unternehmern geben. Dies gilt etwa für die private Kommunikation der etwa 500.000 Bundesbediensteten,⁶⁴ die mit dienstlicher Erlaubnis über ihren dienstlichen Internetanschluss zum Beispiel mit Fachärzten, Psychologen, Beratungsstellen (z.B. Eheberatung, Schwangerschaftsberatung), Gewerkschaften oder Presseangehörigen kommunizieren können. Auch dienstliche Kommunikation kann besonders vertraulich sein, etwa die Anzeige von Straftaten, Steuerdelikten oder sonstigen Vergehen, aber auch die gesetzlich vorgeschriebene Übermittlung personenbezogener Daten etwa durch Arbeitgeber oder Steuerpflichtige. An Bundesbehörden werden etwa 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 werden regelmäßig hochsensible Sachverhalte anvertraut.

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

⁶³ BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 270.

⁶⁴ Statistisches Bundesamt, Pressemitteilung Nr.417 vom 30.09.2005, <http://www.destatis.de..>

geben, reflektieren Informationsdaten 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.⁶⁵ 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.

(d) Sicherheitsrisiken 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.⁶⁶ Das mit Discretion werbende Erotikunternehmen Beate Uhse veröffentlichte die E-Mail-Adressen Tau-

⁶⁵ Bundesregierung, Begründung zum TDDSG, BT-Drs. 13/7385, 25.

⁶⁶ Spiegel 43/2008 vom 20.10.2008, Seite 70.

sender von Personen, die sich Sexfilme im Internet angesehen hatten.⁶⁷ In einem Forum des ZDF-Kinderkanals konnten sich beliebige Personen Klarnamen, Adresse, Telefonnummer und Geburtsdatum aller 1.000 registrierten Kinder verschaffen.⁶⁸

Wegen der vielen Fälle von Datenmissbrauch sind inzwischen 80% der Bundesbürger „sehr besorgt“ um die Sicherheit ihrer Daten.⁶⁹ Eine deutliche Mehrheit der Bevölkerung fordert eine gesetzliche Stärkung des Datenschutzes.⁷⁰ Einer Umfrage aus dem Jahr 2007⁷¹ 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.

Diese Vorfälle zeigen eindeutig, dass nur nicht gespeicherte Daten sichere Daten sind. Sie haben bestätigt, dass der deutsche Ansatz einer strengen Beschränkung der Aufzeichnung von Kommunikationsspuren richtig ist. Die bisherigen gesetzlichen Beschränkungen der Aufzeichnung von Verkehrs- und Nutzungsdaten minimieren den Schaden aus Datenlecks und gewährleisten Sicherheit vor einer missbräuchlichen Aufdeckung und Auswertung unserer Internetnutzung.

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.⁷² 60% sorgen sich, dass ihre Daten in die Hände Dritter gelangen könnten.⁷³ Jeder vierte Internet-Nutzer ist zum Schutz seiner Daten inzwischen immer oder vorwiegend unter Fantasienamen im Netz unterwegs.⁷⁴ Auf diese Weise wollen die Bürger einen Missbrauch ihrer Daten verhindern, Internetangebote anonym nutzen und sich dagegen wehren, dass unangemessen viele Daten abgefragt werden.⁷⁵ Dieser Selbstschutz wird durch die Aufzeichnung von Protokolldaten unterlaufen, weil diese unbemerkt erfolgt und nicht verhindert

⁶⁷ 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.

⁶⁸ 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>.

⁶⁹ Unisys-Umfrage vom 01.10.2008, <http://www.unisyssecurityindex.com/resources/reports/-Germany%20security%20index%20Oct%201-08.pdf>.

⁷⁰ Emnid-Umfrage vom 02.06.2008, <http://www.presseportal.de/pm/13399/1204206/n24/rss>.

⁷¹ Institut Allensbach, Sicher im Netz?, http://www.ifd-allensbach.de/news/prd_0717.html.

⁷² Microsoft, Umfrage vom Februar 2008, <http://www.daten-speicherung.de/?p=267>.

⁷³ Microsoft, Umfrage vom Februar 2008, <http://www.daten-speicherung.de/?p=267>.

⁷⁴ Fittkau und Maaß, Umfrage unter 121.233 deutschsprachigen Internet-Nutzern im Frühjahr 2009, <http://www.w3b.org/nutzerverhalten/furcht-vor-datenmissbrauch-beeinflusst-nutzerverhalten.html>.

⁷⁵ Fittkau und Maaß, Umfrage unter 121.233 deutschsprachigen Internet-Nutzern im Frühjahr 2009, <http://www.w3b.org/nutzerverhalten/furcht-vor-datenmissbrauch-beeinflusst-nutzerverhalten.html>.

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.

(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 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 Bedrohlichkeiten 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 das Fernmeldegeheimnis (Art. 10 GG) setzt. Es schreckt unzumutbar von der Kommunikation mit Bundesbehörden und ihren Angehörigen sowie von der Nutzung ihrer Telemedien ab, wenn Informationen über das gesamte Information- 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.⁷⁶ 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 Grundrechtseingriffe rechtfertigen, nicht aber derart schwerwiegende Eingriffe in Fernmeldegeheimnis und Informationsfreiheit wie sie hier zur Diskussion stehen. 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) *Unverhältnismäßiges Erkennen und Beseitigen von Störungen und Fehlern (§ 5 Abs. 1 S. 1 Nr. 1 Var. 1 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 Störungen und Fehler zu erkennen und zu beseitigen. Dies betrifft namentlich Verkehrsdaten über die computergestützte Kommunikation mit Bundesbehörden (z.B. per E-Mail, Internettelefonie oder Instant Messaging) 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 Beseitigung der meisten Störungen ungeeignet, weil aus der Maßnahme gewonnene Erkenntnisse über Störungen oder Fehler 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 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). In-

⁷⁶ Helmbrecht, INA-Protokoll Nr. 16/94, 23.

soweit ist § 5 Abs. 1 S. 1 Nr. 1 BSIG von vornherein zur Erreichung seiner Ziele ungeeignet.

(a) Verkehrsdaten

Nach der bisherigen Rechtslage war dem BSI die Aufzeichnung der näheren Umstände von Individualkommunikation mit Bundesbehörden und Bundesangehörigen nicht erlaubt.⁷⁷ 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 ist nach § 13 Abs. 1 BDSG unzulässig gewesen, 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.⁷⁸ 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.⁷⁹

Erkennen lassen sich Störungen anhand von Verkehrsdaten nicht, außer vielleicht das Ausbleiben von Verbindungen. Um solche Verfügbarkeitsstörungen zu erkennen, ist es

⁷⁷ Helmbrecht, INA-Drs. 16(4)570 A, 6: „bislang nur nach ausdrücklicher Einwilligung der betroffenen Bundesbediensteten zulässig“.

⁷⁸ Bundesregierung, BT-Drs. 16/11967, 14.

⁷⁹ 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.“

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 Störungen und Fehlern. Es würde also genügen, wenn die Behörde eigene Testverbindungen herstellt oder herstellen lässt und deren nähere Umstände aufgezeichnet und ausgewertet, 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.

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 an-

arbeitern hergestellten Verbindungen zu erheben. Die von § 5 Abs. 1 BStG gestattete anlasslose grundrechtseingreifende Erhebung und Auswertung aller Daten „ins Blaue hinein“ lässt die Verfassung nicht zu.⁸⁰ Das Bundesverfassungsgericht hat bereits 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.⁸¹ Eine allgemeine Bedrohungslage, deren Realisierung „praktisch nie ausgeschlossen“ ist, genügt dem nicht.⁸² Zur Begründung führte das Gericht aus, die Befugnis zur Rasterfahndung gleiche den zu Zwecken der strategischen Kontrolle vorgenommenen Eingriffen in das Fernmeldegeheimnis insofern, als auch sie verdachtslos erfolgende Grundrechtseingriffe in großer Streubreite vorsehe.⁸³ Auch § 5 BStG sieht Grundrechtseingriffe in großer Streubreite vor, die ohne jeden Verdacht vorgenommen werden. Die Erfassung der grundrechtlich besonders geschützten (Art. 10 GG) näheren Umstände jeglicher Kommunikation mit Bundesbehörden 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.

(b) Telemedien-Nutzungsdaten

Soweit § 5 Abs. 1 S. 1 Nr. 1 BStG 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 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

⁸⁰ Bundesrat, BT-Drs. 16/12225, 3.

⁸¹ BVerfGE 115, 320 (320), Ls. 1.

⁸² BVerfGE 115, 320 (364).

⁸³ BVerfGE 115, 320 (359).

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“.⁸⁴ Der Bundesgerichtshof hat dementsprechend jüngst ein „Recht des Internetnutzers auf Anonymität“ anerkannt.⁸⁵

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 – aufgezeichnet 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.

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.

⁸⁴ So ausdrücklich BVerfG, 1 BvR 518/02 vom 4.4.2006, Abs.-Nr. 105 - Rasterfahndung.

⁸⁵ BGH, NJW 2009, 2888 (2893), Abs. 42.

§ 5 BSIG ist auch deshalb nicht erforderlich, weil schon die frühere Rechtslage 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.⁸⁶

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.

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.⁸⁷ Das Bundesjustizministerium musste seine Praxis anpassen und stellt sein Internet-

⁸⁶ Rechtsausschuss, BT-Drs. 16/13259, 8.

⁸⁷ AG Berlin, Urt. v. 27.03.2007, 5 C 314/06.

portal 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 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“ lässt die Verfassung nicht zu.⁸⁸ Das Hohe Gericht hat bereits 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.⁸⁹ Eine allgemeine Bedrohungslage, deren Realisierung „praktisch nie ausgeschlossen“ ist, genügt nicht.⁹⁰ Zur Begründung führte das Gericht aus, die Befugnis zur Rasterfahndung gleiche den zu Zwecken der strategischen Kontrolle vorgenommenen Eingriffen in das Fernmeldegeheimnis insofern, als auch sie vollständig verdachtslos erfolgende Grundrechtseingriffe in großer Streubreite vorsehe.⁹¹ Auch § 5 BSIG sieht vollständig verdachtslos erfolgende Grundrechtseingriffe in großer Streubreite vor. Die Erfassung des grundrechtlich besonders geschützten (Art. 5 GG) Informationsverhaltens einschließlich der Inhalte der abgerufenen Informationen (z.B. abgerufene URLs und darin enthaltene Suchworte) 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 Störungen oder Fehler in einer beliebigen informationstechnischen Anlage des Bundes – etwa einem Webserver – stellt offenkundig kein wichtiges Rechtsgut dar, welches eine allgemeine Kommunikationsdatenerfassung rechtfertigen könnte.

(5) 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 Kommu-

⁸⁸ Bundesrat, BT-Drs. 16/12225, 3.

⁸⁹ BVerfGE 115, 320 (320), Ls. 1.

⁹⁰ BVerfGE 115, 320 (364).

⁹¹ BVerfGE 115, 320 (359).

nikation 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 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.⁹² 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.“⁹³ 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.⁹⁴ Damit dürften sog. „Einbruchserkennungsvorrichtungen“ („Intrusion Detection Systems“) gemeint sein. Es handelt sich dabei um eine

⁹² Bundesregierung, BT-Drs. 16/11967, 14.

⁹³ Bundesregierung, BT-Drs. 16/11967, 14.

⁹⁴ Helmbrecht, INA-Drs. 16(4)570 A, 6.

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.“⁹⁵

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 Kommunikations- und Informationsprotokollen ist denkbar schlecht geeignet, unbekannte Angriffswege aufzudecken. Fox führt dazu aus:⁹⁶ 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-Attacken, bemerke man auch ohne personenbezogene Protokollierung. Insgesamt bleibe der Einsatz von „Einbruchserkennungsvorrichtungen“ „ohne einen erkennbaren Sicherheitsgewinn“.⁹⁷

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 Aussa-

⁹⁵ <http://www.datenschutz.hessen.de/k76.htm#entry2919>.

⁹⁶ Fox, DuD 2005, 422.

⁹⁷ Fox, DuD 2005, 422.

gen 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.*⁹⁸

Im Leitfaden des BSI für die Einführung von Intrusion-Detection-Systemen⁹⁹ 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.“

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:¹⁰⁰

„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 über-

⁹⁸ https://www.bsi.bund.de/cln_136/ContentBSI/Themen/sinet/Uebersicht/angriff.html.

⁹⁹ https://www.bsi.bund.de/cae/servlet/contentblob/486992/publicationFile/30698/Leitfadenv10_pdf.pdf.

¹⁰⁰ Pohl, Protokoll Nr. 16/94 der Anhörung am 11.05.2009, http://www.bundestag.de/ausschuesse/a04/anhoerungen/Anhoerung_21/Protokoll.pdf, 15 f.

flüssig. 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.“

Es ist nochmals darauf hinzuweisen, dass die Systeme des Bundes über Jahre hinweg ohne personenbezogene Totalprotokollierung funktionierten 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 personenbezogenen, vollkommen anlasslosen und flächendeckenden 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 BSI-G vorgesehenen 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 („Virens Scanner“). Es ist nicht erkennbar, dass eine Bundesbehörde jemals mithilfe von Verkehrsdaten Schadprogramme aufgefunden habe, die nicht schon durch den Einsatz eines Virens Scanners 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 („Virens Scanner“) 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 mildereren 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 Gesetzesentwurfs 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 – 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 Verfügbarkeitsstörungen. Es würde also genügen, wenn die Behörde 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) Einbruchversuche

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 Einbruchversuchen 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 Einbruchversuchen.

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 Einbruchversuchen 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 flächendeckend 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 beeinträchtigt 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:¹⁰¹

- 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 ist bereits oben gezeigt worden, dass § 15 Abs. 1 TMG die Erhebung und Verarbeitung personenbezogener Nutzungsdaten zulässt, 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 erforderlich 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 Nut-

¹⁰¹ https://www.bsi.bund.de/cln_136/ContentBSI/Themen/sinet/Gefahrenungen/DDoSAngriffe/ddos.html.

zungsdaten 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 BSI nach Maßgabe des Bundesdatenschutzgesetzes angemessene Vorkehrungen zum Schutz ihrer Systeme treffen. § 5 BSI 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 milderer 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 BSI vorgesehene Erfassung der Nutzung sämtlicher öffentlich zugänglicher Telemedien. Im Übrigen liegt für Authentifizierungsformulare ein milderer 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.

(6) Unverhältnismäßige Abwehr von Schadprogrammen (§ 5 Abs. 1 S. 1 Nr. 2 BSI)

§ 5 Abs. 1 S. 1 Nr. 2 BSI 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,¹⁰² 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 („Virens Scanner“) und Maßnahmen 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.¹⁰³

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

¹⁰² Seite 39 ff.

¹⁰³ Seite 27 ff.

Verhältnis zu dem damit erhofften, nicht nachweisbaren Sicherheitsgewinn im Vergleich zu den auch ohne § 5 BSIG verfügbaren und erforderlichen Schutzmöglichkeiten.

(7) 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, um Schadprogramme zu erkennen und abzuwehren. 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 geeignet oder erforderlich sind. Zur Vermeidung von Wiederholungen wird auf die obigen Ausführungen Bezug genommen.¹⁰⁴

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 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.¹⁰⁵ 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

¹⁰⁴ Seite 39.

¹⁰⁵ Seite 39.

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:¹⁰⁶

„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.¹⁰⁷ 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 mildereren Mitteln.

(8) Die Rechtsprechung des Bundesverfassungsgerichts

§ 5 BSIG wird den verfassungsrechtlichen Mindestanforderungen und dem Verhältnismäßigkeitsgebot nicht gerecht. Nach der Rechtsprechung des Bundesverfassungsgerichts darf eine automatisierte Datenerfassung „nicht anlasslos erfolgen oder flächendeckend durchgeführt werden“.¹⁰⁸ Begriffe wie „erforderlich“ oder „sachdienlich“ stellen keine hinreichende Eingrenzung dar.¹⁰⁹ Das „strikte Verbot der Sammlung personenbezogener Daten auf Vorrat“ ist zu gewährleisten.¹¹⁰

¹⁰⁶ Helmbrecht, INA-Drs. 16(4)570 A, 7.

¹⁰⁷ Seite 39 ff.

¹⁰⁸ BVerfGE 120, 378 (378); BVerfG, NVwZ 2007, 688 (691).

¹⁰⁹ BVerfG, MMR 2007, 93 (94); BVerfG, NVwZ 2007, 688 (691).

¹¹⁰ BVerfGE 115, 320 (350).

Die Anlehnung an § 100 TKG, der seinerseits mit der Verfassung nicht im Einklang steht¹¹¹ und von den Gerichten notdürftig einschränkend ausgelegt und angewandt wird,¹¹² übersieht, dass Nutzungsdaten nicht nur über die näheren Umstände von Individualkommunikation, sondern über den Inhalt der abgerufenen und eingegebenen Informationen (z.B. Internetseiten, Suchwörter) Aufschluss geben und damit weit reichende Rückschlüsse auf die Persönlichkeit des Nutzers zulassen, wie sie bei sonstigen Medien undenkbar wären.

Das Bundesverfassungsgericht hat bereits zu einer anderen automatisierten Datenerhebung und -verwendung entschieden, dass die automatisierte Erfassung personenbezogener Lebenssachverhalte nicht anlasslos erfolgen oder flächendeckend durchgeführt werden darf.¹¹³ Der Grundsatz der Verhältnismäßigkeit im engeren Sinne ist nicht gewahrt, wenn die gesetzliche Ermächtigung die automatisierte Erfassung und Auswertung personenbezogener Lebenssachverhalte ermöglicht, ohne dass konkrete Gefahrenlagen oder allgemein gesteigerte Risiken von Rechtsgutgefährdungen oder -verletzungen einen Anlass zur Einrichtung der Erfassung geben.¹¹⁴ Im Vergleich zu dieser Entscheidung, die zum Abgleich von Kfz-Kennzeichen mit dem Fahndungsbestand ergangen ist, ist zu beachten, dass die Eingriffsintensität der hier in Rede stehenden Maßnahmen weit höher ist. § 5 BStG sieht keinen sofortigen Abgleich mit einer Fahndungsdatenbank und im Nichttrefferfall eine sofortige und spurlose Löschung vor; vielmehr soll die Löschung der erfassten Verkehrsdaten nur „unverzüglich“ oder sogar erst nach drei Monaten erfolgen. Im vorliegenden Zusammenhang geht es zudem um die grundrechtlich in Artikel 10 GG besonders geschützte Vertraulichkeit der Telekommunikation.

Insgesamt ist § 5 BStG vor dem Hintergrund einer Aufweichung des strikten Verbots der Sammlung personenbezogener Daten auf Vorrat durch den Gesetzgeber zu sehen. Anders als die europarechtlich vorgegebene Vorratsspeicherung von Verbindungs- und Bestandsdaten stellt § 5 BStG einen vom Deutschen Bundestag in freiem Willen beschlossenen Dammbruch dar, der eine Flut anlassloser Erfassungen unseres täglichen Lebens nach sich ziehen wird, wenn ihm nicht durch Aufhebung des § 5 BStG 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. Eine solche globale und pauschale Aufzeichnung des Verhaltens vollkommen unbescholtener Bürger widerspricht dem Menschenbild des Grundgesetzes. Auch im Hinblick auf seine Präcedenzwirkung hinsichtlich der Zukunft des Datenschutzes muss § 5 BStG folglich aufgehoben werden.

¹¹¹ Breyer, RDV 2004, 147; vgl. auch Bundesrat, BR-Drs. 62/09, 10.

¹¹² LG Darmstadt, MMR 2006, 330.

¹¹³ BVerfGE 120, 378 (378), Ls. 4.

¹¹⁴ BVerfGE 120, 378 (378), Ls. 4.

Rechtfertigen lässt sich § 5 BSIG auch nicht mit der Erwägung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung, wonach es hinsichtlich der Telekommunikationsdaten mangels öffentlicher Wahrnehmbarkeit kein gesellschaftliches Gedächtnis gebe, das es wie in anderen Bereichen erlaubte, zurückliegende Vorgänge auf der Grundlage zufälliger Erinnerung zu rekonstruieren.¹¹⁵ Soweit § 5 BSIG zur Erfassung und Auswertung von Telekommunikationsinhalten und -umständen ermächtigt, gibt es kein gesellschaftliches Gedächtnis, das es in anderen Bereichen erlaubte, zurückliegende vergleichbare Kommunikationsvorgänge auf der Grundlage zufälliger Erinnerung zu rekonstruieren. Der E-Mail-Kommunikation mit Behördenmitarbeitern ist 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 erinnerte – mit Ausnahme des Empfängers, dem aber auch im Fall einer E-Mail alle Inhalte und Verkehrsdaten vorliegen.

Soweit § 5 BSIG zur Erfassung und Auswertung von Internet-Nutzungsdaten ermächtigt, gibt es ebenfalls kein gesellschaftliches Gedächtnis, das es in anderen Bereichen erlaubte, zurückliegende vergleichbare Vorgänge auf der Grundlage zufälliger Erinnerung zu rekonstruieren. Die Nutzung der Telemedien von Bundesorganen ist mit der Abholung ausliegender Formulare und Informationsschriften aus einer Behörde vergleichbar. Angriffe auf Internetserver können mit Beschädigungen von Behördenräumen verglichen werden. Dass jemand – etwa der Pförtner einer Filiale der Arbeitsagentur – frühere Besucher der Behörde erinnerte, ist unwahrscheinlich. Anders mag dies im Fall einer Videoaufzeichnung für die Dauer weniger Tage sein. § 5 BSIG unterscheidet sich aber schon dadurch grundlegend von einer Videoaufzeichnung, dass sich Internet-Nutzungsdaten automatisiert auswerten und analysieren lassen, was bei Videobildern derzeit nur sehr eingeschränkt möglich ist. Im Übrigen kann auch eine Videoaufzeichnung nur verfassungsgemäß sein, wenn für sie ein hinreichender Anlass besteht und sie in räumlicher und zeitlicher Hinsicht das Übermaßverbot wahrt.¹¹⁶ § 5 BSIG setzt demgegenüber weder einen hinreichenden Anlass voraus, noch ist er zeitlich auf diesen beschränkt. Bereits der Bundesrat hat zutreffend ausgeführt:¹¹⁷ „Die Ermächtigungsgrundlage muss daneben hinreichend normenklar und -bestimmt sein sowie dem verfassungsrechtlichen Gebot der Verhältnismäßigkeit genügen. Hiermit nicht vereinbar sind anlasslose oder flächendeckend durchgeführte Speicherungen sämtlicher Nutzungsdaten; es müssen vielmehr Anhaltspunkte für eine konkrete Störung vorliegen (vgl. BVerfG, Urteil vom 11.03.2008 - 1 BvR 2074/05 u. a. -, MMR 2008, 308).“ §

¹¹⁵ So BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 217.

¹¹⁶ BVerfG, 1 BvR 2368/06 vom 23.2.2007, Absatz-Nr. 56.

¹¹⁷ BR-Drs. 62/09, 9 f.

5 BSIG macht Anhaltspunkte für ein konkrete, gegenwärtige Störung nicht zur Voraussetzung der dort vorgesehenen Erfassungen.

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 2.3.2010 betont, dass die Zulässigkeit der vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten aufgrund der EG-Richtlinie zur Vorratsdatenspeicherung eine Ausnahme bleiben muss.¹¹⁸ Maßgeblich für ihre Rechtfertigungsfähigkeit sei insbesondere, dass sie nicht direkt durch staatliche Stellen erfolge, dass sie nicht auch die Kommunikationsinhalte erfasse und dass auch die Speicherung der aufgerufenen Internetseiten grundsätzlich untersagt sei.¹¹⁹ Diese Rechtfertigungsvoraussetzungen erfüllt § 5 BSIG nicht: Die dort vorgesehene Speicherung erfolgt direkt durch staatliche Stellen und umfasst gerade auch die Speicherung jeder aufgerufenen Internetseite. In seiner Entscheidung vom 2.3.2010 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.¹²⁰ Im Bereich der vielen Telemedien des Bundes beseitigt § 5 BSIG diese Löschungspflichten des TMG und zielt umgekehrt darauf ab, dass die Nutzung dieser Internetangebote inhaltlich festgehalten wird und damit rekonstruierbar gemacht wird. Dies entspricht dem Grundgesetz nicht.

II. Verletzung des Art. 5 Abs. 1 S. 1 GG

1. Schutzbereich der Meinungsfreiheit

Art. 5 Abs. 1 S. 1 Hs. 1 GG gewährleistet das Recht, Meinungen in Wort, Schrift und Bild äußern und verbreiten zu dürfen. Dies umfasst auch Meinungsäußerungen unter Benutzung der Medien Telefon („Wort“), Telefax („Schrift und Bild“) und Internet („Wort, Schrift und Bild“).¹²¹ Geschützt sind Meinungsäußerungen sowohl im Wege der Individual- wie auch der Massenkommunikation.¹²² Die Äußerung und Verbreitung von Tatsachenbehauptungen ist dann geschützt, wenn die Kenntnis der Tatsachenbehauptungen Voraussetzung für die Meinungsbildung ist.¹²³ Weil die Kenntnis einer Tatsachenbehauptung stets unabdingbare Voraussetzung dafür ist, sich darüber eine Meinung bilden zu können, ist die Äußerung und Verbreitung von Tatsachen und Tatsachenbehauptungen umfassend geschützt.

¹¹⁸ BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 218.

¹¹⁹ BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 218.

¹²⁰ BVerfG, 1 BvR 256/08 vom 2.3.2010, Absatz-Nr. 270.

¹²¹ BVerfG EuGRZ 1997, 446 (446) für das Internet.

¹²² Für Meinungsäußerungen in der Presse BVerfGE 85, 1 (11 f.); BVerfGE 86, 122 (128).

¹²³ BVerfGE 94, 1 (7); BVerfGE 65, 1 (41); BVerfGE 61, 1 (8).

Demnach ist das Recht auf Verbreitung von Tatsachenbehauptungen und Werturteilen mittels Telekommunikation durch Art. 5 Abs. 1 S. 1 Hs. 1 GG umfassend gewährleistet. Im Bereich des Internet können alle Dienste zur Verbreitung von Tatsachen und Werturteilen genutzt werden (insbesondere WWW, FTP, Usenet und E-Mail). Allerdings werden das Internet und die genannten Dienste nicht stets zur Verbreitung von Tatsachenbehauptungen oder Werturteilen genutzt. Werden sonstige Arten von Daten über das Internet ausgetauscht, so handelt es sich lediglich um eine Transaktion, die mit dem Austausch materieller Gegenstände vergleichbar ist. Insoweit ist die Meinungsfreiheit nicht einschlägig. So wird es sich etwa regelmäßig bei dem Angebot von Software oder Computerspielen über das Internet verhalten.

Die Meinungsfreiheit gewährleistet auch das Recht, die Umstände – also etwa die Zeit und den Ort – der Meinungskundgabe frei zu bestimmen.¹²⁴ Daraus ergibt sich, dass auch das Recht der Inanspruchnahme Dritter zur Verbreitung eigener Tatsachenbehauptungen oder Meinungen gewährleistet ist.

Fraglich ist, ob Art. 10 GG gegenüber der Meinungsfreiheit speziell ist und sie verdrängt.¹²⁵ Dass Art. 10 GG nicht in jedem Fall das speziellere Grundrecht ist, ergibt sich daraus, dass Art. 10 GG die Übermittlung aller Arten von Informationen schützt und nicht nur die Verbreitung von Tatsachenbehauptungen und Meinungen. Aber auch in Fällen, in denen sowohl ein Grundrecht aus Art. 10 GG als auch die Meinungsfreiheit einschlägig ist, weisen die Grundrechte unterschiedliche Schutzrichtungen auf: Während das Fernmelde- und das Briefgeheimnis die Vertraulichkeit der Kommunikation schützen sollen, schützt die Meinungsfreiheit das Recht, Tatsachenbehauptungen und Meinungen überhaupt frei äußern und verbreiten zu dürfen. Es ist nicht gerechtfertigt, durch die Annahme eines Spezialitätsverhältnisses die Meinungsfreiheit auf dem Gebiet der räumlich distanzierten Kommunikation quasi aufzuheben, zumal Art. 5 Abs. 1 S. 1 Hs. 1 GG die freie Wahl des für eine Meinungsäußerung eingesetzten Mediums gewährleistet. In Anbetracht der unterschiedlichen Schutzzwecke müssen die Grundrechte aus Art. 10 GG einerseits und die Meinungsfreiheit andererseits daher nebeneinander anwendbar sein (Idealkonkurrenz).

2. Schutzbereich der Informationsfreiheit

Art. 5 Abs. 1 S. 1 Hs. 2 GG gewährleistet das Recht, sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Erfasst ist sowohl die Unterrichtung über Meinungen als auch über Tatsachenbehauptungen.¹²⁶ Das Recht auf freie Unterrichtung über Tatsa-

¹²⁴ Pieroth/Schlink, Grundrechte (17. Aufl.), Rn. 556 m.w.N.

¹²⁵ So Jarass/Pieroth, Grundgesetz (7. Aufl.), Art. 10, Rn. 2; Maunz/Dürig, Grundgesetz (Stand: Juni 2002), Art. 10, Rn. 29; Brenner, Die strafprozessuale Überwachung des Fernmeldeverkehrs mit Verteidigern, 33.

¹²⁶ Dreier-Schulze-Fielitz, Art. 5 I, II, Rn. 57; Jarass/Pieroth, Grundgesetz (6. Aufl.), Art. 5, Rn. 15 m.w.N.

chen ist Funktionsbedingung einer Demokratie,¹²⁷ die von der Mitwirkung bei und der Kontrolle von staatlichen Entscheidungen durch die Öffentlichkeit lebt. Kann eine Informationsquelle nur mit Hilfe von technischen Vorrichtungen genutzt werden, dann gewährleistet die Informationsfreiheit auch das Recht zur Anschaffung und Nutzung der erforderlichen Vorrichtungen.¹²⁸

Allgemein zugänglich ist eine Informationsquelle jedenfalls dann, wenn sie technisch dazu geeignet und bestimmt ist, einem individuell nicht bestimmbar Personenkreis Informationen zu verschaffen.¹²⁹ Diese Definition ist allerdings insoweit unglücklich, als es statt „individuell bestimmbar“ „individuell bestimmt“ heißen muss: Einschlägig ist die Informationsfreiheit nur dann nicht, wenn der Adressatenkreis einer Quelle nach dem Willen ihres Inhabers abschließend feststeht und nicht erweiterbar ist.¹³⁰ Demgegenüber ist es für den Schutzzweck der Informationsfreiheit unerheblich, ob eine Informationsquelle nach dem Willen ihres Inhabers nur einem bestimmten, nach allgemeinen Merkmalen abgegrenzten Adressatenkreis offen stehen soll oder der Allgemeinheit. Beispielsweise soll eine Zeitung regelmäßig nur an zahlende Käufer abgegeben werden und jugendgefährdende Schriften nur an Volljährige. In derartigen Fällen müssen sich all diejenigen Personen auf das Grundrecht der Informationsfreiheit berufen können, welche die von dem Inhaber der Informationsquelle geforderten Merkmale erfüllen. Das Wort „zugänglich“ in Art. 5 Abs. 1 S. 1 Hs. 2 GG bezieht sich nach allgemeinem Sprachverständnis allein auf die faktische oder technische Erreichbarkeit, so dass auch nur diese „allgemein“, also für jedermann, gegeben sein muss. Nicht erforderlich ist, dass der Inhaber einer Informationsquelle diese voraussetzungslos für jedermann eröffnet.

Art. 5 Abs. 1 S. 1 Hs. 2 GG ist hinsichtlich Internetdiensten regelmäßig einschlägig. Dies gilt sowohl im Bereich des World Wide Web¹³¹, soweit Informationen nicht nur an einen im Voraus abschließend bestimmten Adressatenkreis gerichtet sind (z.B. individuelle elektronische Grußkarten), als auch für die Dienste FTP (File Transfer Protocol) und Usenet (Newsgroups). E-Mails werden oft an einen abschließend bestimmten Adressatenkreis gerichtet sein mit der Folge, dass Art. 5 Abs. 1 S. 1 Hs. 2 GG keine Anwendung findet. Der Versand von E-Mails kann aber auch als Informationsdienst ausgestaltet sein, dessen Inanspruchnahme jedermann oder jedenfalls bestimmten Personenkreisen offen steht (z.B. so genannte Newsletter). In diesem Fall ist die Informationsfreiheit einschlägig.

¹²⁷ Hornung, MMR 2004, 3 (5) m.w.N.

¹²⁸ BVerfGE 90, 27 (32).

¹²⁹ BVerfGE 27, 71 (83); BVerfGE 33, 52 (65).

¹³⁰ Für die Anwendung dieses Kriteriums im Bereich der Rundfunkfreiheit plädiert Jarass/Pieroth, Grundgesetz (6. Aufl.), Art. 5, Rn. 36.

¹³¹ Vgl. Hornung, MMR 2004, 3 (5).

Entsprechend den Ausführungen zur Meinungsfreiheit erfasst auch die Informationsfreiheit nicht den Bezug bloßer Daten, in denen weder Tatsachen noch Werturteile zum Ausdruck kommen. Zwischen der Informationsfreiheit einerseits und dem Fernmeldegeheimnis andererseits besteht Idealkonkurrenz.

3. § 5 BSIG als Eingriff in diese Grundrechte

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-Meinungsforen¹³² oder Kontaktformulare anbietet. Über diese Kanäle kann man seine Meinung wegen § 5 BSIG nicht mehr ohne das Risiko einer Identifikation anonym äußern.

Die in § 5 BSIG vorgesehene Informationserfassung und -auswertung kann von dem unbefangenen Gebrauch der Meinungs- und Informationsfreiheit abschrecken.¹³³ 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.¹³⁴ 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 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 abrufen. Die entsprechenden Nutzer wurden anhand ihrer IP-Adresse über § 113 TKG identifiziert und mit verschiedenen Datenbanken abgeglichen. Die aufgezeigte Verfahrensweise hat die Bundesregierung auf parlamentarische Anfragen öffentlich bestätigt.¹³⁵ Identifizierung und Datenbankabgleich wurden nach unbestrittenen Presseinformationen bei einer dreistelligen Anzahl von Perso-

¹³² 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.

¹³³ Vgl. BGH, NJW 2009, 2888.

¹³⁴ Vgl. BGH, NJW 2009, 2888.

¹³⁵ BT-Prot. 16/117, 22; BT-Drs. 16/6938.

nen durchgeführt, die in keinerlei Verbindung mit einer Straftat standen. In dem Pressebericht heißt es:¹³⁶

„Ursprünglich hatte das BKA die Identität von 417 Personen feststellen wollen. Dabei handelte es sich nicht um Tatverdächtige, 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. Das Hohe Gericht hat entschieden, dass eine Abschreckungswirkung schon dann in die Abwägung einzubeziehen ist, wenn die Betroffenen Nachteile „nicht ohne Grund befürchten“.¹³⁷ 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.¹³⁸ 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.

¹³⁶ Tagesspiegel vom 30.09.2007, <http://www.tagesspiegel.de/politik/deutschland/BKA-Datenschutz;art122,2390884>.

¹³⁷ BVerfGE 100, 313 (376).

¹³⁸ Vgl. BVerfGE 27, 71 (81).

Dem Risiko einer Identifizierung kann nicht durch Möglichkeiten anonymer Telekommunikationsnutzung begegnet werden, weil die Nutzung dieser Möglichkeiten zusätzliche 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.

4. Mangelnde Rechtfertigung

Der Eingriff des § 5 BSIG in Art. 5 GG ist nicht gerechtfertigt, weil § 5 BSIG das Gebot der Normenklarheit und das Verhältnismäßigkeitsgebot verletzt. Zur Vermeidung von Wiederholungen wird auf die diesbezüglichen Ausführungen zu Art. 10 GG und zu den Art. 2 Abs. 1, 1 Abs. 1 GG Bezug genommen, die für Art. 5 GG entsprechend gelten.¹³⁹

III. Verletzung des allgemeinen Gleichheitssatzes (Artikel 3 Abs. 1 GG)

1. Eingriff in den Schutzbereich des Art. 3 Abs. 1 GG

Art. 3 Abs. 1 GG gewährleistet, dass der Staat Sachverhalte, die im Wesentlichen gleich sind, auch gleich behandelt.¹⁴⁰ Diese Pflicht trifft nach Art. 1 Abs. 3 GG auch den Gesetzgeber.¹⁴¹ Im Wesentlichen gleich sind zwei Sachverhalte dann, wenn sie sich einem gemeinsamen Oberbegriff zuordnen lassen.¹⁴² Der Oberbegriff muss die Sachverhalte vollständig erfassen.¹⁴³ Nicht erforderlich ist dagegen, dass der Oberbegriff ausschließlich die beiden zu vergleichenden Sachverhalte umfasst. Die Vergleichbarkeit zweier Sachverhalte, die sich einem gemeinsamen Oberbegriff zuordnen lassen, kann allenfalls dann verneint werden, wenn die Sachverhalte unterschiedlichen rechtlichen Ordnungsbereichen angehören und in anderen systematischen und sozialgeschichtlichen Zusammenhängen stehen.¹⁴⁴

§ 5 BSIG führt zur unterschiedlichen Behandlung des Informationsaustausches mit Bundesorganen einerseits und des Informationsaustauschs mit sonstigen Personen andererseits. Während § 5 Abs. 1 S. 1 Nr. 1 und Abs. 2 BSIG den Bund dazu ermächtigt, Informationen über das Telekommunikations- und Mediennutzungsverhalten der Bürger

¹³⁹ Seite 17 ff.

¹⁴⁰ St. Rspr. seit BVerfGE 1, 14 (52).

¹⁴¹ BVerfGE 1, 14 (52).

¹⁴² Pieroth/Schlink, Grundrechte (17. Aufl.), Rn. 431 ff.

¹⁴³ Pieroth/Schlink, Grundrechte (17. Aufl.), Rn. 435.

¹⁴⁴ Jarass/Pieroth, Grundgesetz (6. Aufl.), Art. 3, Rn. 4 m.w.N.

global und pauschal aufzuzeichnen, sind Privatpersonen 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.

Beide Sachverhalte unterscheiden sich dadurch, dass ein Kommunikationsvorgang im einen Fall mit einem Bundesorgan oder Bundesbediensteten stattfindet, im anderen Fall mit einer Privatperson. Dieser Unterschied ändert jedoch nichts daran, dass es sich in beiden Fällen um menschliche Kommunikation handelt, und zwar um Individual- oder um Massenkommunikation (Telemedien). Gemeinsamer Oberbegriff ist daher die menschliche Kommunikation. Die Kommunikation mit Bundesorganen einerseits und Privatpersonen andererseits gehören nicht etwa ganz unterschiedlichen rechtlichen Ordnungsbereichen an, sondern sind vergleichbar. Der Schutzbereich des Art. 3 Abs. 1 GG ist durch eine generelle Erfassung des Kommunikationsverhaltens allein mit Bundesorganen und -angehörigen demnach betroffen.

Ein Eingriff in Art. 3 Abs. 1 GG liegt vor, wenn eine Person durch eine Ungleichbehandlung von wesentlich Gleichem nachteilig betroffen ist.¹⁴⁵ Dies ist im Fall von § 5 BSIG bei denjenigen Menschen der Fall, die mit Bundesorganen und -bediensteten kommunizieren und deren Kommunikation dabei durchgängig registriert wird, während dies bei ihrer Kommunikation mit sonstigen natürlichen und juristischen Personen nicht geschieht. Damit stellt § 5 BSIG einen rechtfertigungsbedürftigen Eingriff in das Grundrecht der Internetnutzer aus Art. 3 Abs. 1 GG dar.

2. Rechtfertigungsmaßstab

Unter welchen Umständen eine Ungleichbehandlung verfassungsrechtlich gerechtfertigt ist, hängt nach der Rechtsprechung des Bundesverfassungsgerichts von dem jeweiligen Regelungsgegenstand und Differenzierungsmerkmal ab.¹⁴⁶ In manchen Fällen lässt das Bundesverfassungsgericht jeden sachlichen Grund als Rechtfertigung genügen.¹⁴⁷ Für eine bloße Willkürprüfung spricht es etwa, wenn eine Ungleichbehandlung von Sachverhalten ohne engen menschlichen Bezug vorliegt,¹⁴⁸ wenn der Bereich der gewährenden Staatstätigkeit betroffen ist,¹⁴⁹ es sich um wirtschaftsordnende Maßnahmen handelt¹⁵⁰ oder wenn eine Differenzierung bereits im Grundgesetz angelegt ist.¹⁵¹

¹⁴⁵ Vgl. BVerfGE 67, 239 (244).

¹⁴⁶ BVerfGE 88, 87 (96); BVerfGE 95, 267 (316).

¹⁴⁷ BVerfGE 88, 87 (96); BVerfGE 95, 267 (316).

¹⁴⁸ Etwa BVerfGE 38, 225 (229).

¹⁴⁹ Etwa BVerfGE 49, 280 (282).

¹⁵⁰ Etwa BVerfGE 18, 315 (331).

¹⁵¹ Jarass/Pieroth, Grundgesetz (6. Aufl.), Art. 3, Rn. 23; vgl. etwa BVerfGE 52, 303 (346) für Beamte.

Dasselbe soll im Bereich vielgestaltiger Sachverhalte gelten, die im Einzelnen noch nicht bekannt sind.¹⁵² Richtigerweise handelt es sich hierbei allerdings um eine Erscheinungsform des allgemeinen Problems der Behandlung unbekannter Tatsachen im Rahmen der verfassungsrechtlichen Prüfung, das differenziert zu lösen ist. Tatsächliche Unsicherheiten rechtfertigen einen Einschätzungsspielraum des Gesetzgebers nur hinsichtlich der Einschätzung der unbekannten Tatsachen. Auswirkungen auf den generellen Kontrollmaßstab können sie dagegen nicht haben.¹⁵³

In anderen Fallgruppen wendet das Bundesverfassungsgericht einen strengeren Prüfungsmaßstab an, dem zufolge zu untersuchen ist, ob ein sachlicher Grund von solcher Art und solchem Gewicht vorliegt, dass er die Ungleichbehandlung rechtfertigt.¹⁵⁴ Im Kern handelt es sich um eine Prüfung der Verhältnismäßigkeit.¹⁵⁵ Für die Vornahme einer Verhältnismäßigkeitsprüfung spricht es etwa, wenn die diskriminierende Maßnahme in ein Freiheitsgrundrecht eingreift¹⁵⁶ oder wenn die Diskriminierten keinen Einfluss auf ihre Behandlung nehmen können.¹⁵⁷ Insgesamt wird die Verhältnismäßigkeit insbesondere in denjenigen Fällen zu prüfen sein, in denen von einer Ungleichbehandlung erhebliche Belastungen für die Betroffenen ausgehen.

Misst man § 5 BSIG an den genannten Kriterien, so fragt sich zunächst, ob die Vorschrift lediglich eine Ungleichbehandlung von Sachverhalten ohne engen menschlichen Bezug darstellt, was für eine bloße Willkürprüfung sprechen würde. Für diese Annahme könnte man anführen, dass die meisten Menschen nicht nur mit Bundesbehörden, sondern auch mit vielen Dritten kommunizieren. Ein strikter Personenbezug in dem Sinn, dass ein Sachverhalt ausschließlich eine bestimmte Gruppe von Menschen und der andere Sachverhalt ausschließlich eine andere Menschengruppe betrifft, liegt nicht vor. Fraglich ist aber, ob dies Voraussetzung für die Annahme eines „engen menschlichen Bezugs“ ist oder ob es nicht auch genügt, dass bestimmte Personengruppen von der Ungleichbehandlung typischerweise stärker betroffen sind als andere. Von § 5 BSIG sind etwa Bundesangehörige stärker betroffen als andere Personengruppen, die nicht im gleichen Maße auf die Nutzung der Telekommunikationsvorrichtungen des Bundes angewiesen sind.

Die von § 5 BSIG Betroffenen haben in vielen Fällen keine zumutbare Ausweichmöglichkeit. Wer dienstlich mit Bundesbehörden in Kontakt tritt, ist regelmäßig dazu gezwungen, etwa um gesetzlichen Verpflichtungen nachzukommen. Dass in der heutigen Informationsgesellschaft Kommunikation ohne Telekommunikationsnetze kaum noch denkbar ist, liegt

¹⁵² BVerfGE 33, 171 (189 f.); BVerfGE 78, 249 (288).

¹⁵³ Chrysogonos, Verfassungsgerichtsbarkeit und Gesetzgebung, 189.

¹⁵⁴ Vgl. allgemein BVerfGE 87, 234 (255); BVerfGE 91, 389 (401); BVerfGE 95, 267 (317).

¹⁵⁵ Vgl. nur BVerfGE 82, 126 (146) und Jarass/Pieroth, Grundgesetz (7. Aufl.), Art. 3, Rn. 27.

¹⁵⁶ Für das allgemeine Persönlichkeitsrecht BVerfGE 60, 123 (134); BVerfGE 88, 87 (97).

¹⁵⁷ Vgl. BVerfGE 88, 87 (96); BVerfGE 97, 169 (181).

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.

Festzuhalten ist somit, dass vielen Menschen in weiten Bereichen keine zumutbare Alternative zur Internetkommunikation mit Bundesorganen zur Verfügung steht und dass dies zumeist nicht auf einer freien Willensentscheidung beruht. Dies spricht nach den Kriterien des Bundesverfassungsgerichts für die Vornahme einer Verhältnismäßigkeitsprüfung. Zudem stellt eine globale und pauschale Erfassung, Rasterung und Vorratsspeicherung des Informations- und Kommunikationsverhaltens einen schwerwiegenden Eingriff in verschiedene Freiheitsgrundrechte dar (Fernmeldegeheimnis oder Recht auf informationelle Selbstbestimmung, Meinungsfreiheit, Informationsfreiheit). Unabhängig davon, ob man einen engen menschlichen Bezug der Ungleichbehandlung annimmt oder nicht, überwiegen damit jedenfalls die Gesichtspunkte, die für eine Verhältnismäßigkeitsprüfung sprechen. Prüfungsmaßstab ist daher, ob ein sachlicher Grund von solcher Art und solchem Gewicht existiert, dass er es rechtfertigt, den Bund zu einer anlasslosen und flächendeckenden Erfassung, Rasterung und Vorratsspeicherung der näheren Umstände der Kommunikation über seine Server zu ermächtigen, Privatpersonen dagegen nicht.

3. Unterschiedliche Schutzwürdigkeit als Rechtfertigungsgrund?

Als Rechtfertigungsgrund könnte angeführt werden, dass die Funktionsfähigkeit der Informationstechnik des Bundes schutzwürdiger sei als die Informationstechnik Privater. Dagegen spricht jedoch erstens, 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.¹⁵⁸ Zweitens könnte selbst eine unterstellt höhere Schutzwürdigkeit nur solche Maßnahmen rechtfertigen, die tatsächlich geeignet, erforderlich und verhältnismäßig sind, um die Verfügbarkeit der Informationstechnik des Bundes zu verbessern. Dass dies bei § 5 BSIG nicht der Fall ist, ist oben bereits umfassend erläutert worden.¹⁵⁹ Aus demselben Grund kann zur Rechtfertigung nicht angeführt werden, dass die Informationstechnik des Bundes überdurchschnittlich häufig angegriffen werde, was im Übrigen empirisch nicht zu belegen ist.

¹⁵⁸ BMI: Nationaler Plan zum Schutz der Informationsinfrastrukturen, http://www.bmi.bund.de/cae/servlet/contentblob/121734/publicationFile/13577/Nationaler_Plan_Schutz_Informationsinfrastrukturen.pdf, 21.

¹⁵⁹ Seite 18 ff.

4. Ergebnis

Festzuhalten ist, dass es nicht zu rechtfertigen 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. § 5 BSIG ist folglich auch mit Art. 3 Abs.1 GG unvereinbar.

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