Dr. Patrick Breyer[1]

Innenausschuss
A-Drs. 16(4)570 F

7. Mai 2009

Stellungnahme zum Entwurf eines „Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes“

Zusammenfassung

1. Bei der Behandlung des Entwurfs eines „Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes“ muss der Bundestag die bestehenden Regelungen zum Schutz der Privatsphäre von Internetnutzern erhalten (I., II.) und deutlich verbessern (III.).

2. Die vorgeschlagene Änderung des § 15 des Telemediengesetzes würde eine potenziell unbegrenzte Menge sensibler und vertraulicher Informationen über Internetnutzer Offenlegungs- und Missbrauchsrisiken aussetzen. Artikel 3 muss dringend aus dem Gesetzentwurf gestrichen werden. Dasselbe gilt für die in § 5 BSIG-RegE vorgesehene anlasslose Aufzeichnung und Vorratsspeicherung von Informationen über die Nutzung elektronischer Behördenportale.

Inhaltsübersicht

1 Der Verfasser ist Jurist und Mitglied im Arbeitskreis Vorratsdatenspeicherung. Kontakt: https://privacybox.de/pab.msg.

I. Keine Aufzeichnung des Surfverhaltens zur „Störungsbeseitigung“ (§ 15 Abs. 9 TMG-RegE)

1. Vergleichsübersicht der Vorschläge zu § 15 Abs. 9 TMG-E

	Regierungsentwurf	Innenausschuss Bundesrat	Stellungnahme Bundesrat	Eigener Kompromissvorschlag	Geltende Rechtslage
	23.01. 2009	24.02. 2009	06.03. 2009	07.05. 2009	
1. Legt fest, aus welchem Anlass Anbieter Nutzungsprotokolle erstellen dürfen; legalisiert keine permanente flächendeckende Surfprotokollierung	**NEIN**	**JA**	**JA**	**JA**	**entfällt**
2. Nutzungsprotokolle dürfen ausdrücklich nur „im Einzelfall“ erstellt werden	**NEIN**	**NEIN**	**NEIN**	**JA**	**entfällt**
3. Maximale Aufbewahrungsdauer der Nutzungsprotokolle festgelegt	**NEIN**	**JA**	**NEIN**	**JA**	**entfällt**
4. Nutzungsprotokolle dürfen nicht für andere Zwecke verwendet werden (Zweckbindung)	**NEIN**	**JA**	**JA**	**JA**	**entfällt**
5. Weitergabe von Nutzungsprotokollen ausgeschlossen; Vertraulichkeit der Internetnutzung gewährleistet	**NEIN**	**NEIN**	**JA**	**JA**	**entfällt**
6. Verstöße sind bußgeldpflichtig	**NEIN**	**JA**	**JA**	**JA**	**entfällt**
7. Legt fest, dass die Internetprotokoll-Adressen (IP-Adressen) von Internetnutzern dem Datenschutz unterliegen	**NEIN**	**NEIN**	**NEIN**	**JA**	**NEIN**
Empfehlung	– – –	– –	– –	+	+ + +

2. Nutzungsdaten

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, muss der Anbieter für die Dauer der Übertragung aus technischen Gründen unsere Internet-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.[2] 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 zurecht in besonderem Maße vor einer Erfassung geschützt.

3. Sicherheitsrisiken für Internetnutzer

In der letzten Zeit musste Deutschland zunehmend Fälle versehentlicher und absichtlicher Veröffentlichung und Zweckentfremdung von Informationen über unsere Internetnutzung erleben. So war im vergangenen Jahr plötzlich weltweit nachzulesen, wer delikate Partneranzeigen unter Chiffre aufgegeben hatte, wer ein Erotikangebot von Beate Uhse genutzt hatte und welche Kinder ein Forum des ZDF-Kinderkanals nutzten.

Diese Vorfälle haben uns in Erinnerung gerufen, dass nur nicht gespeicherte Daten sichere Daten sind. Sie haben bestätigt, dass der deutsche Ansatz einer strengen Beschränkung der Aufzeichnung von Nutzungsdaten richtig ist. Die Beschränkung der Aufzeichnung von Nutzungsdaten minimiert den Schaden aus Datenlecks und gewährleistet unsere Sicherheit vor einer missbräuchlichen Aufdeckung und Auswertung unserer Internetnutzung.

4. Datenschutz und Wirtschaftswachstum

Vor dem Hintergrund der wachsenden Zahl von Offenlegungen und Missbräuchen von Informationen über Internetnutzer müssen sich die Bürger/innen darauf verlassen können, dass die Menge der solchen Risiken ausgesetzten Daten so klein wie möglich gehalten wird. Andernfalls werden die Verbraucher/innen das Internet nicht in einem Maß nutzen, wie es erforderlich ist, um das wirtschaftliche Potenzial der Informationsgesellschaft auszuschöpfen. Dadurch würden das wirtschaftliche Wachstum und die Innovationsfähigkeit einer

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

wichtigen Zukunftsbranche in Deutschland empfindlich zurückgeworfen.

5. Das gesetzliche Protokollierungsverbot

Nach § 13 des Telemediengesetzes haben Anbieter „sicherzustellen, dass [...] die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs oder der sonstigen Nutzung unmittelbar nach deren Beendigung gelöscht [...] werden". Dieses Protokollierungsverbot stellt den Kern des deutschen Telemedien-Datenschutzrechts dar und stellt sicher, dass so wenige Daten über Internetnutzer wie möglich den vielfältigen, oben dargestellten Sicherheitsrisiken ausgesetzt werden.

6. Protokollierungsverbot nicht anwendbar auf Angriffe

Es ist wichtig, die Reichweite dieses gesetzlichen Protokollierungsverbots zu verstehen. Das Protokollierungsverbot gilt 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 Telemediums und genießt nicht den gesetzlichen Protokollierungsschutz. Im Bereich von Zugängen, über die kein Telemedium bereit gestellt wird, können Anbieter daher bereits heute nach Maßgabe des Bundesdatenschutzgesetzes Vorkehrungen zum Schutz ihrer Systeme treffen.

7. Gezielte Störungsbeseitigung bereits erlaubt

Auch personenbezogene Daten von Nutzern dürfen nach § 15 Abs. 1 TMG erhoben und verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen. Kann ein Telemedium wegen einer Störung nicht mehr in Anspruch genommen werden und sollte es im Einzelfall erforderlich werden, zur Wiederherstellung der Verfügbarkeit personenbezogene Daten zu erheben, so ermöglicht dies das geltende Recht.

8. Protokollierungsverbot nicht anwendbar auf anonyme Daten

Das Protokollierungsverbot gilt nur für Daten, die die Bestimmung der Person des Nutzers zulassen (§ 3 BDSG). Anhand anonymer Daten können demgegenüber ohne Einschränkungen der Netzwerkverkehr beobachtet, Störungen erkannt und statistische Auswertungen vorgenommen werden.

9. Einwilligung bleibt möglich

Eine personenbezogene Erfassung des Nutzungsverhaltens ist darüber hinaus zulässig, wenn ein Nutzer in freier Entscheidung einwilligt. Eine Einwilligung kann grundsätzlich auch von allen Nutzern eines Dienstes gefordert werden, was insbesondere bei anmelde- und kostenpflichtigen Diensten in Betracht kommt.

10. Aufzeichnung des Surfverhaltens nicht erforderlich zum "Erkennen, Eingrenzen oder Beseitigen von Störungen"

Zur Beseitigung von Störungen brauchen Anbieter von Telemedien im Internet wie Google, eBay oder StudiVZ 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 Protokolle.

Den fehlenden Bedarf für personenbezogenen Protokolle belegt die erfolgreiche Anwendung des Telemedienrechts in den letzten Jahren. Bei der letzten Novellierung im Jahre 2007 hat der Gesetzgeber zu Recht keine Aufgabe dieses Schutzes für erforderlich gehalten.

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 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 AG Berlin, dass die „Störungsbeseitigung“ keine generelle Sammlung von IP-Adressen oder anderer personenbezogener Informationen über

Nutzer rechtfertigt.[3] Das Bundesjustizministerium musste seine Praxis anpassen und stellt sein Internetportal seither sicher und zuverlässig ohne Sammlung personenbezogener Daten zur Verfügung.

11. Der Regierungsentwurf eines § 15 Abs. 9 TMG

Während der Bundestag bei Erlass des Telemediengesetzes im Jahr 2007 den bewährten Schutz von Internetnutzern beibehalten wollte, schlägt das insoweit unzuständige Bundesinnenministerium nun zur Aushebelung der vorgenannten Rechtsprechung eine Abänderung vor.

Der als „besonders eilbedürftig" vorgelegte Entwurf eines „Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes"[4] betrifft mit der „Informationstechnik des Bundes" eigentlich ganz andere Fragen. Mit Artikel 3 soll jedoch als neuer § 15 Abs. 9 die folgende Bestimmung in das Telemediengesetz eingefügt werden:

> „*Soweit erforderlich, darf der Diensteanbieter Nutzungsdaten zum Erkennen, Eingrenzen oder Beseitigen von Störungen seiner für Zwecke seines Dienstes genutzten technischen Einrichtungen erheben und verwenden. Absatz 8 Satz 2 und Satz 3 gilt entsprechend.*" Absatz 8 Satz 2 und Satz 3 lauten: „*Der Diensteanbieter hat die Daten unverzüglich zu löschen, wenn die Voraussetzungen nach Satz 1 nicht mehr vorliegen oder die Daten für die Rechtsverfolgung nicht mehr benötigt werden. Der betroffene Nutzer ist zu unterrichten, sobald dies ohne Gefährdung des mit der Maßnahme verfolgten Zweckes möglich ist.*"

Zur Begründung des Vorstoßes führt das Bundesinnenministerium aus, eine § 100 Abs. 1 TKG entsprechende Bestimmung benötigten auch Telemedienanbieter, „beispielsweise um Angriffe (Denial of Service, Schadprogramme, Veränderung ihrer Webangebote von außerhalb) abwehren zu können". Zur „Erkennung und Abwehr bestimmter Angriffe" sei eine „kurzfristige Speicherung und Auswertung der Nutzungsdaten erforderlich". Der Begriff der Störung sei „umfassend zu verstehen als jede vom Diensteanbieter nicht gewollte Veränderung der von ihm für sein Telemedienangebot genutzten technischen Einrichtungen".

---

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

4 BR-Drs. 62/09.

12. Vorschlag des Innenausschusses des Bundesrats

Am 24. Februar 2009 haben der Innen- und Rechtsausschuss des Bundesrats demgegenüber die folgende Fassung des geplanten § 15 Abs. 9 TMG vorgeschlagen:[5]

> *„Liegen dem Diensteanbieter **im Einzelfall zu dokumentierende tatsächliche Anhaltspunkte** vor, dass **bestimmte Nutzer** seine zur Bereitstellung des Dienstes genutzten technischen Einrichtungen **stören**, darf er die **personenbezogenen Daten dieser Nutzer** über das Ende des Nutzungsvorgangs sowie die in Absatz 7 genannte Speicherfrist hinaus verwenden, soweit dies zum Erkennen, Eingrenzen oder Beseitigen der Störung erforderlich ist; **eine Verwendung der Daten für andere Zwecke ist unzulässig. Die Maßnahme kann auch durchgeführt werden, wenn Dritte unvermeidbar mitbetroffen werden.** Der Diensteanbieter hat die Daten unverzüglich zu löschen, wenn die Voraussetzungen nach Satz 1 nicht mehr vorliegen oder die Daten zur Störungseingrenzung oder -beseitigung nicht mehr benötigt werden. **Nach Satz 2 gespeicherte Daten sind spätestens nach 24 Stunden zu löschen.** Der betroffene Nutzer ist zu unterrichten, soweit und sobald dies ohne Gefährdung des mit der Maßnahme verfolgten Zwecks möglich ist.“*

Zur Begründung führten die Ausschüsse aus, mit den Grundrechten unvereinbar seien „anlasslose oder flächendeckend durchgeführte Speicherungen sämtlicher Nutzungsdaten; es müssen vielmehr Anhaltspunkte für eine konkrete Störung vorliegen“. Darüber hinaus sei eine „konkrete Zweckbindung bei der Datenverwertung“ vorzusehen. Sei es aus technischen Gründen unvermeidbar, neben den mutmaßlichen Störern auch andere Nutzer zu erfassen, so seien die Daten spätestens nach 24 Stunden zu löschen.

13. Stellungnahme des Bundesrats

Auf Initiative der Länder Hessen und Baden-Württemberg[6] schlug der Bundesrat schließlich am 6. März 2009 die folgende Fassung des geplanten § 15 Abs. 9 TMG vor:[7]

> *„Liegen dem Diensteanbieter **zu dokumentierende tatsächliche Anhaltspunkte** vor, dass **bestimmte***

5 BR-Drs. 62/1/09, 9.

6 BR-Drs. 62/2/09.

7 BR-Drs. 62/09 (Beschluss), 8.

> ***Nutzer*** *seine zur Bereitstellung seines Dienstes genutzten technischen Einrichtungen* ***stören****, darf er die* ***personenbezogenen Daten*** *dieser Nutzer über das Ende des Nutzungsvorgangs sowie die in Absatz 7 genannte Speicherfrist hinaus* ***nur erheben, speichern und nutzen****, soweit dies für den* ***Zweck der Eingrenzung oder Beseitigung der Störung*** *erforderlich ist;* ***eine Verwendung der Daten für andere Zwecke ist unzulässig. Die Maßnahme kann auch durchgeführt werden, wenn Dritte unvermeidbar mitbetroffen werden.*** *Der Diensteanbieter hat die Daten unverzüglich zu löschen, wenn die Voraussetzungen nach Satz 1 nicht mehr vorliegen oder die Daten zur Störungseingrenzung oder -beseitigung nicht mehr benötigt werden. Der betroffene Nutzer ist zu unterrichten, soweit und sobald dies ohne Gefährdung des mit der Maßnahme verfolgten Zwecks möglich ist.“*

Zur Begründung führten die Länder an, Nutzungsprotokolle dürften nur anlassbezogen und nicht permanent zum rein vorsorglichen „Erkennen“ von Störungen erstellt werden.[8]

14. Katastrophale Auswirkungen des Vorschlags

Die Annahme des § 15 Abs. 9 TMG-E in der Fassung des Regierungsentwurfs hätte katastrophale Auswirkungen:

- Der Regierungsentwurf legt fest nicht, aus welchem Anlass Anbieter Nutzungsprotokolle erstellen dürfen. Der unbestimmte Wortlaut des § 15 Abs. 9 TMG-RegE leistet einer Auslegung Vorschub, wonach sämtliche Anbieter von Internetdiensten wie Google, Amazon oder StudiVZ künftig berechtigt wären, das Surfverhalten ihrer Besucher ohne Anlass aufzuzeichnen. Es dürfte nämlich nie auszuschließen sein, dass diese Daten einmal zum „Erkennen“ denkbarer zukünftiger „Störungen“ „erforderlich“ sein könnten. Damit würde zur potenziell unbegrenzten und unbefristeten Speicherung jeder Eingabe und jedes Mausklicks beim Lesen, Schreiben und Diskutieren im Internet ermächtigt, zur Vorratsdatenspeicherung im Internet. Der Vorschlag würde den Grundsatz der §§ 13, 15 TMG, demzufolge Nutzungsdaten nicht über die Dauer des Nutzungsvorgangs hinaus aufbewahrt werden dürfen, bedeutungslos machen. Der Vorschlag ist nicht auf eine Erfassung „im Einzelfall“

8 BR-Drs. 62/2/09, 2.

bei Vorliegen einer konkreten Störung beschränkt, sondern würde eine anlasslose, globale und pauschale Aufzeichnung unserer Internetnutzung erlauben.

- Auch dem Formulierungsvorschlag des Bundesrats fehlt eine ausdrückliche Beschränkung auf den Einzelfall. Der Vorschlag des Bundesrates bestimmt zudem nicht, nach welcher Zeitdauer Protokolle über unbeteiligte, rechtschaffene Nutzer spätestens zu löschen sind. Schließlich spricht der Vorschlag des Bundesrats pauschal von „personenbezogenen Daten", während im Regierungsentwurf immerhin präziser von „Nutzungsdaten" die Rede ist.
- § 15 Abs. 9 TMG-RegE schließt eine Verwendung der gesammelten Informationen zu ganz anderen Zwecken nicht aus. Die Verwendung der Surfprotokolle wird „zum Erkennen, Eingrenzen oder Beseitigen von Störungen" gestattet, aber eben nicht „nur" dazu (vgl. hingegen § 15 Abs. 1 TMG). Die Surfprotokolle dürften daher beispielsweise an Polizei, Bundeskriminalamt, Geheimdienste sowie an die Unterhaltungsindustrie herausgegeben werden (§§ 15 Abs. 5 S. 4, 14 Abs. 2 TMG). Eine richterliche Anordnung ist nicht vorgeschrieben, eine Beschränkung auf schwere Straftaten oder wenigstens eine Abwägung (vgl. § 28 Abs. 3 BDSG) nicht vorgesehen. In weitem Umfang bestünden sogar Herausgabepflichten (z.B. §§ 95 StPO, 20m BKA-G, 8a BVerfSchG, 101 UrhG).
- Der Regierungsentwurf gewährleistet die Vertraulichkeit der Mediennutzung nicht. Die vorgeschlagene Ermächtigung der Anbieter zum „Verarbeiten" von Nutzungsdaten würde auch deren Übermittlung abdecken (§ 3 Abs. 4 BDSG). Der Regierungsentwurf würde daher zur Offenlegung unserer Internet-Nutzungsdaten gegenüber Dritten ermächtigen.

Der Vorschlag der Bundesregierung 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".[9] Begriffe wie „erforderlich" oder „sachdienlich" stellen keine hinreichende Eingrenzung dar.[10] Das „strikte Verbot der Sammlung

9 BVerfG, MMR 2008, 308, 308; BVerfG, NVwZ 2007, 688, 691.

10 BVerfG, MMR 2007, 93, 94; BVerfG, NVwZ 2007, 688, 691.

personenbezogener Daten auf Vorrat“ ist zu gewährleisten.[11] Eine „enge und konkrete Zweckbindung“ muss gesetzlich angeordnet werden.[12]

Die Anlehnung an § 100 TKG, der seinerseits mit der Verfassung nicht im Einklang steht[13] und von den Gerichten notdürftig einschränkend ausgelegt werden muss,[14] 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.

15. Position der Zivilgesellschaft und der Datenschutzbeauftragten

Am 29.10.2008 kritisierten 11 Bürgerrechts-, Presse-, Anwalts- und Verbraucherschutzorganisationen einen mit der „Netz- und Informationssicherheit“ begründeten Vorschlag des Europäischen Parlaments.[15] Dieser würde den Anbietern einen „Blankoscheck“ zur zeitlich unbegrenzten Vorratsspeicherung von Kommunikationsdaten geben. Dies würde „sensible Informationen über unsere Kommunikation und unsere Bewegungen Missbrauchsrisiken aussetzen“.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erklärte am 06./07.11.2008 zum selben Entwurf, es sei „nicht erforderlich, zur Gewährleistung der Netz- und Informationssicherheit einzelfallunabhängig personenbezogene Verkehrsdaten zu speichern. Die Anbieter [...] sind aufgefordert, ihre Systeme so sicher zu gestalten, dass Angriffe von vornherein erfolglos bleiben.“[16]

Am 20.01.2009 kritisierte die Gesellschaft für Informatik, angesichts der aktuellen und auch zukünftig zu erwartenden Unsicherheit des Internet begründe § 15 Abs. 9 TMG-RegE „ein vorbehaltsloses Recht zur Überwachung von Nutzungsdaten der

11 BVerfG, MMR 2006, 531.
12 BVerfGE 100, 313, 385 f.
13 Breyer, RDV 2004, 147.
14 LG Darmstadt, MMR 2006, 330.
15 http://www.vorratsdatenspeicherung.de/images/brief_esecurity_bmwi_publi.pdf.
16 http://www.datenschutz-bayern.de/dsbk-ent/DSK_76-ElektronischeKommunikation.html.

Sprach- und Datenkommunikation aller Kunden/Benutzer wie Unternehmen und Bürger".[17]

Am gleichen Tag meldete der Arbeitskreis Vorratsdatenspeicherung, die geplante „verdachtslose Aufzeichnung des Surfverhaltens im Internet" gehe „gewaltig über die bisherige Vorratsdatenspeicherung hinaus".[18] Der Vorstoß würde die unbegrenzte und unbefristete Speicherung jeder Eingabe und jedes Mausklicks beim Lesen, Schreiben und Diskutieren im Internet legalisieren. Die Surfprotokolle dürften an Polizei, Bundeskriminalamt, Geheimdienste sowie an die Unterhaltungsindustrie herausgegeben werden.

Am 18.02.2009 warnte auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, § 15 Abs. 9 TMG-RegE sehe eine „umfassende Protokollierung des Surfverhaltens" vor. Der Gesetzgeber müsse unmissverständlich klarstellen, „dass die Erhebung und Auswertung personenbezogener Daten ultima ratio ist".[19]

Der Bundestagsabgeordnete Frank Hofmann (SPD) sagte bei der ersten Lesung des Gesetzentwurfs am 19.03.2009: „Weshalb man im Zusammenhang mit diesem Gesetzesentwurf in Art. 3 auch noch das Telemediengesetz ändern will, ist für mich nicht nachvollziehbar."[20]

In seinem am 21.04.2009 vorgelegten Tätigkeitsbericht kritisierte der Bundesbeauftragte für den Datenschutz Peter Schaar den § 15 Abs. 9 TMG-RegE mit den Worten, er sei „von der Notwendigkeit einer zusätzlichen Speicherung nicht überzeugt." Vielmehr sei zu prüfen, „ob nicht bereits verwendete, erforderlichenfalls zu optimierende Mittel (Firewalls) zur Verhinderung und Abwehr von Angriffen genügen."[21]

Das Europäische Parlament nahm am 06.05.2009 in zweiter Lesung von seinem ursprünglichen Vorstoß Abstand, wonach Anbietern im Rahmen des „Telekom-Pakets" eine Aufzeichnung von Kommunikationsdaten zur Gewährleistung der „Netz- und Informationssicherheit" erlaubt werden sollte.[22]

---

17 GI, Pressemitteilung vom 20.01.2009, www.gi-ev.de.

18 Arbeitskreis Vorratsdatenspeicherung, Pressemitteilung vom 20.01.2009, www.vorratsdatenspeicherung.de.

19 Entschließung vom 18.02.2009, www.bfdi.bund.de.

20 BT-Prot. 16/211, 22942.

21 Bundesdatenschutzbeauftragter, Tätigkeitsbericht 2007/2008, BT-Drs. 16/12600, 96.

22 Beschluss T6-0360/2009 vom 06.05.2009.

16. Eigener Kompromissvorschlag

In einer öffentlichen Stellungnahme nach Bekanntwerden des Regierungsentwurfs teilte das Bundesinnenministerium am 20.01.2009 mit, eine „unbegrenzte oder anlassbezogene [gemeint wohl: anlasslose] Speicherung“ sollte „durch die vorgeschlagene Regelung nicht gestattet“ werden; es sollte eine „Zweckbindung“ bestehen. Auch sei zur „Erkennung und Abwehr“ von „Angriffen“ nur eine „kurzfristige Speicherung [...] erforderlich“.

Wie oben dargestellt, hat diese Absicht keinen Niederschlag im Regelungsentwurf gefunden. Dieser sieht keine Beschränkung auf besondere Anlässe, keine Zweckbindung und keine Beschränkung auf eine „kurzzeitige“ Speicherung vor.

Wollte man zumindest die öffentlich mitgeteilte Intention des Bundesinnenministeriums verfassungskonform umsetzen, dann müsste § 15 Abs. 9 TMG-E wie folgt umformuliert werden:

> „***Liegen dem Diensteanbieter im Einzelfall zu dokumentierende tatsächliche Anhaltspunkte vor, dass bestimmte Nutzer seine zur Bereitstellung seines Dienstes genutzten technischen Einrichtungen stören, darf er die Internetprotokoll-Adressen und die sonstigen Nutzungsdaten dieser Nutzer über das Ende des Nutzungsvorgangs sowie die in Absatz 7 genannte Speicherfrist hinaus nur erheben, speichern und nutzen, soweit dies zur Beseitigung der Störung erforderlich ist; eine Verwendung der Daten für andere Zwecke ist unzulässig. Die Maßnahme kann auch durchgeführt werden, wenn Dritte unvermeidbar mitbetroffen werden.*** *Der Diensteanbieter hat die Daten unverzüglich zu löschen, wenn die Voraussetzungen nach Satz 1 nicht mehr vorliegen oder die Daten zur Störungsbeseitigung nicht mehr benötigt werden.* ***Nach Satz 3 erhobene Daten sind spätestens am Folgetag zu löschen.*** *Der betroffene Nutzer ist zu unterrichten, sobald dies ohne Gefährdung des mit der Maßnahme verfolgten Zweckes möglich ist.*“

Diese Formulierung lehnt sich an § 15 Abs. 8 TMG an, welcher der besonderen Sensibilität von Internet-Nutzungsdaten Rechnung trägt. Die Formulierung würde die öffentlich geäußerte Absicht des Ministeriums umsetzen, eine Protokollierung nicht permanent, generell und ohne Anlass zu gestatten, sondern nur wenn „im Einzelfall“ tatsächlich konkrete Anhaltspunkte für eine Störung durch bestimmte Nutzer eines

Dienstes vorliegen. Die Weitergabe der Daten an Dritte wäre ausgeschlossen.

Die hier vorgeschlagene Formulierung schafft ferner im ersten Satz Klarheit, dass Internetprotokoll-Adressen, über welche unsere Internetnutzung nachverfolgt werden kann (vgl. § 113 TKG, § 101 UrhG), als Nutzungsdaten den Schutz des Telemediengesetzes genießen. Ohne diese Klarstellung bestünde die Gefahr, dass die restriktiven Vorgaben des Gesetzgebers in § 15 Abs. 9 TMG-E mit dem Argument unterlaufen werden, Internet-Nutzungsprotokolle („Logfiles") seien nicht personenbezogen und die Regelung daher nicht anwendbar. Es besteht ein Klarstellungsbedürfnis, weil ein Amtsgericht[23] und ein Teil der Literatur[24] neuerdings die einhellige Meinung der Aufsichtsbehörden[25] und der Rechtsprechung[26] in Frage gestellt haben, wonach Internetnutzer anhand ihrer IP-Adresse „bestimmbar" im Sinne des § 3 Abs. 1 BDSG sind und Internet-Nutzungsprotokolle daher dem gesetzlichen Datenschutz unterliegen.[27]

Satz 2 des hier unterbreiteten Formulierungsvorschlags würde die vom Innenministerium beabsichtigte Zweckbindung auch tatsächlich anordnen. Satz 3 würde dem Umstand Rechnung tragen, dass es aus technischen Gründen unvermeidbar sein kann, neben den mutmaßlichen Störern auch andere Nutzer mitzuerfassen. Jedoch müssen die Daten der mutmaßlichen Störer dann unverzüglich ermittelt und die übrigen Aufzeichnungen spätestens nach 24 Stunden gelöscht werden (Satz 5). Dies dient dem Schutz der überwältigenden Mehrheit rechtstreuer Nutzer, die keinen Anlass für eine Aufzeichnung ihrer Internetnutzung gegeben haben.

---

23 AG München, MMR 2008, 860 – nicht rechtskräftig.

24 Eckhardt, K&R 2007, 602; dagegen zutr. Pahlen-Brandt, K&R 2008, 288.

25 Artikel 29-Gruppe der Datenschutzbeauftragten der Europäischen Union, Stellungnahmen WP37 vom 21.11.2000, 17, WP58 vom 30.05.2002, 3 und WP136 vom 20.06.2007, 19; Bundesdatenschutzbeauftragter, Tätigkeitsbericht 2007/2008, BT-Drs. 16/12600, 96; Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe zum Umgang mit personenbezogenen Daten bei Internetdiensten, Punkt 3.1; Bundesamt für Sicherheit in der Informationstechnik (BSI), Handlungsempfehlungen für E-Government-Angebote, 13.

26 AG Berlin, 5 C 314/06 vom 27.03.2007, ZUM 2008, 83; LG Berlin, 27 O 616/05 vom 10.11.2005, CR 2006, 418; AG Wuppertal, NStZ 2008, 161.

27 Vgl. auch Erwägungsgrund 26 der RiL 95/46/EG.

Damit Verstöße gegen die gesetzlichen Schutzbestimmungen nicht gänzlich folgenlos blieben, müsste zudem die Bußgeldandrohung in § 16 Abs. 2 Nr. 5 TMG entsprechend dem Vorschlag des Bundesrats angepasst werden.

17. Die beste Lösung: Beibehaltung der bestehenden Rechtslage

Ungeachtet dieser Ausführungen bleibt es dabei, dass bereits das geltende Recht die zuverlässige Bereitstellung von Telemedien und die gezielte Beseitigung von Störungen ermöglicht, eine Änderung der bewährten und ausgewogenen Regelungen mithin nicht erforderlich ist. Umgekehrt begründet jede Ermächtigung zur personenbezogenen Erfassung von Nutzungsdaten die Gefahr, dass hochsensible Informationen über unsere Internetnutzung versehentlich abhanden kommen, veröffentlicht werden oder absichtlich zweckentfremdet werden.

Da die vorgeschlagene Änderung des § 15 TMG eine potenziell unbegrenzte Menge äußerst sensibler Daten über unsere Internetnutzung Offenlegungs- und Missbrauchsrisiken aussetzen würde, muss sie dringend aus dem Gesetzentwurf gestrichen werden. Die geltenden Schutzbestimmungen des Telemediengesetzes stellen erwiesenermaßen die beste Garantie für unsere Sicherheit in der Informationsgesellschaft dar und müssen erhalten bleiben.

II. Keine Aufzeichnung des Surfverhaltens durch das BSI (§ 5 BSIG-RegE)

1. „Protokolldaten“ bei der Nutzung öffentlicher Internetportale

Wenn wir heute bei dem Finanzamt eine Broschüre lesen oder ein Formular abholen, brauchen wir nicht zu befürchten, dass uns jemand über die Schulter schauen oder mitschreiben könnte. Wenn wir uns dagegen auf der Internetseite einer Bundesbehörde informieren, muss die Behörde für die Dauer der Übertragung aus technischen Gründen unsere Internet-Adresse kennen. Anhand dieser Adresse oder anderer Nutzerkennungen kann jede Eingabe und jeder Mausklick beim Lesen, Schreiben und Diskutieren behördlicher Internetangebote erfasst, aufgezeichnet, ausgewertet, weiter gemeldet und offen gelegt werden.

Was wir auf Behördenseiten lesen, suchen und schreiben, spiegelt unsere Persönlichkeit, unsere Vorlieben und Schwächen, unser Privatleben und unsere Geschäftsgeheimnisse

in großer Deutlichkeit wider. Der Gesetzgeber hat unsere Nutzung auch von eGovernment-Informationsangeboten daher zurecht gesetzlich vor einer Aufzeichnung und Erfassung geschützt (§ 15 TMG).

Behörden können schon nach geltendem Recht ihre Internetserver mithilfe von „Firewalls“ vor Angriffen schützen, ohne dass dazu eine personenbezogene Aufzeichnung des Surfverhaltens erforderlich wäre. Zudem unterliegen unautorisierte Zugriffe bereits nach geltendem Recht nicht dem Löschungsgebot des Telemediengesetzes.[28] Eine Änderung der bestehenden Rechtslage ist daher nicht erforderlich.

2. „Protokolldaten“ bei der Kommunikation mit Behörden

Wer sich per E-Mail an seinen Abgeordneten oder an eine Bundesbehörde wendet, weiß, dass seine Nachricht und seine Absenderkennung bei dem Empfänger gespeichert werden. Bei einer Bundesbehörde eingegangene dienstliche E-Mails oder Daten unterliegen schon nach geltendem Recht nicht dem Fernmeldegeheimnis, weil dieses nur den vertraulichen Übermittlungsvorgang bis zum Empfänger gewährleistet (§ 88 TKG).

Bundesbehörden dürfen daher schon jetzt eingegangene E-Mails und eingehende Internetdaten nach Maßgabe des Bundesdatenschutzgesetzes und der Mitbestimmungsregelungen auf schädliche Inhalte filtern und ähnliche Sicherheitsmaßnahmen vornehmen. Bundesbehörden können mit solchen Maßnahmen auch das Bundesamt für Sicherheit in der Informationstechnik beauftragen (§ 9 BDSG); sie behalten dann die Kontrolle über und die Verantwortung für den Umgang mit ihren Daten bei dem BSI.

3. Auswirkungen des § 5 BSIG-RegE

Mit § 5 BSIG-E sieht der Regierungsentwurf weitreichende Änderungen dieser Rechtslage vor:

- Künftig soll die Abwehr von Gefahren für die Kommunikationstechnik von Bundesbehörden nicht mehr der jeweiligen Behörde als Betreiber obliegen, sondern das BSI soll Eingriffe zentral und in eigener Verantwortung vornehmen dürfen. Diese wären von den betroffenen Behörden, ihren Mitarbeitern und Personalvertretungen nicht mehr kontrollierbar. Dies gilt insbesondere für die

28 Näher Seite 4 oben.

Filterung eingehender E-Mail-Nachrichten (§ 5 Abs. 1 Nr. 2 BSIG-RegE).

- In Abweichung von dem geltenden Telemediengesetz soll der Staat zudem künftig das Recht erhalten, die Nutzung seiner Internet-Informationsportale ohne Anlass in personenbezogener Form festzuhalten und aufzuzeichnen (§ 5 Abs. 1 Nr. 1 BSIG-RegE). Dies ist nicht nur einer Filmaufzeichnung unser Lektüre öffentlicher Druckwerke vergleichbar. Vielmehr können uns Internet-Nutzungsdaten – anders als Videoaufzeichnungen – maschinell zugeordnet und ausgewertet werden und weisen daher eine besonders „hohe Sensitivität“ auf.

4. Nachteile einer zentralen Sicherheitsarchitektur

Schon der Grundkonzeption des Vorschlags, die gesamte Informationstechnik des Bundes künftig durch eine zentrale Behörde schützen zu lassen, ist zu kritisieren. Unter Fachleuten ist 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 haben. Dezentrale Sicherheitslösungen sind daher aus Sicherheitsgründen vorzuziehen.

Zudem ist eine zentrale Sicherheitsarchitektur anfälliger für internen Missbrauch und weckt Begehrlichkeiten für ihre spätere Nutzung zu weiteren Zwecken. 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. Der zentralen Speicherung wohnt ein Missbrauchspotenzial inne, welches von der elektronischen Kontaktaufnahme zu Bundesbehörden abschrecken kann.

5. Katastrophale Auswirkungen der vorgeschlagenen Surfprotokollierung (§ 5 Abs. 1 Nr. 1 und Abs. 2 BSIG-RegE)

§ 5 Abs. 1 Nr. 1 BSIG-RegE sieht vor, global und pauschal personenbezogen aufzuzeichnen, welcher Bürger wann welches öffentliche Internetangebot genutzt hat. Ausweislich der Gesetzesbegründung sollen die Surfprotokolle auf Hinweise auf „bevorstehende IT-Angriffe“ überprüft werden.

Diesem Ansinnen ist bereits entgegen gehalten worden, dass sich IT-Angriffe nicht durch die Aufzeichnung personenbezogener

Daten verhindern lassen. Verhindern lassen sich Angriffe nur durch den Einsatz von Schutzsoftware („Firewalls“) und durch die fortlaufende Schließung von Sicherheitslücken („Patches“).

Dass eine Aufzeichnung des Surfverhaltens aller Nutzer öffentlicher Internetportale nicht erforderlich ist, beweist die Verwaltung schon dadurch, dass sie selbst mehrere Portale ohne personenbeziehbare Aufzeichnungen anbietet, ohne dass diese Angebote häufiger gestört oder sonst beeinträchtigt wären als ihre sonstigen Portale. Dazu gehören etwa die Portale www.bmj.bund.de, www.bmbf.de, www.bfdi.bund.de, www.bundesrechnungshof.de und sogar www.bundeskriminalamt.de.

Nach § 5 Abs. 2 BSIG-RegE sollen die Surfprotokolle drei Monate lang aufbewahrt werden, um gegebenenfalls Behörden benachrichtigen zu können, die von Schadsoftware betroffen sind. Diese rein vorsorgliche Vorratsdatenspeicherung ins Blaue hinein ist nicht verhältnismäßig: Bei Einsatz der üblichen technischen Schutzmaßnahmen kann es nur selten zu einem Befall mit Schadsoftware kommen. Noch seltener ermöglichen Protokolldaten die Feststellung der befallenen Systeme. Es ist vollkommen unverhältnismäßig, für diese seltenen Ausnahmefälle das Informationsverhalten aller Nutzer von Bundesportalen auf Vorrat aufzuzeichnen.

Aus fachlicher Sicht wäre es ohnehin verfehlt, nach Auffinden von Schadsoftware nur bereits betroffene Behörden zu informieren. Vielmehr müssen alle Behörden informiert werden und ihre Schutzsoftware (z.B. „Virenscanner“) aktualisieren. Diese Software entfernt dann etwa vorhandene Schadsoftware automatisch und verhindert einen neuen Befall. Die Aufzeichnung personenbezogener Nutzungsprotokolle ist zu alledem nicht erforderlich.

Selbst wenn man entgegen der technischen Gegebenheiten unterstellen wollte, aus Surfprotokollen ließen sich „Hinweise auf bevorstehende IT-Angriffe“ oder auf vorhandene Schadprogramme gewinnen, ist die Umsetzung der Aufzeichnungsermächtigung in § 5 BSIG-RegE misslungen:

- Der Regierungsentwurf bestimmt nicht, welche Anlässe eine Aufzeichnung des Surfverhaltens rechtfertigen sollen. Der Vorschlag des Bundesinnenministeriums ist so weit und unbestimmt gefasst, dass das BSI potenziell jede Nutzung der Internetangebote des Bundes auf unbegrenzte Zeit personenbeziehbar aufzeichnen könnte mit der bloßen

Behauptung, die Daten seien „zum Erkennen, Eingrenzen oder Beseitigen von Störungen“ erforderlich. Der Vorschlag würde den Grundsatz der §§ 13, 15 TMG, demzufolge Nutzungsdaten nicht über die Dauer des Nutzungsvorgangs hinaus aufbewahrt werden dürfen, bedeutungslos machen. Das BSI würde einen Blankoscheck zur Überwachung der Nutzer öffentlicher Internetangebote erhalten. Der Vorschlag ist nicht auf eine Erfassung „im Einzelfall“ bei Vorliegen einer Störung beschränkt, sondern würde eine generelle Aufzeichnung von Informationen über unsere Nutzung öffentlicher Internetportale erlauben.

- Der Regelungsvorschlag des Innenministeriums sieht in großem Umfang eine Verwendung der gesammelten Informationen zu ganz anderen Zwecken vor (§ 5 Abs. 4 und 5 BSIG-RegE). Eine Beschränkung schwere Straftaten oder wenigstens eine Abwägung ist nicht vorgesehen. Eine Weitergabe personenbezogener Surfprotokolle wird nicht nur „im Einzelfall“ gestattet, sondern systematisch und in großem Umfang.

§ 5 BSIG-RegE wird damit den verfassungsrechtlichen Mindestanforderungen und dem Verhältnismäßigkeitsgebot nicht gerecht. Insbesondere die von § 5 BSIG-RegE gestattete anlasslose grundrechtseingreifende Aufzeichnung und Auswertung aller Daten „ins Blaue hinein" lässt die Verfassung nicht zu.[29] Nach der Rechtsprechung des Bundesverfassungsgerichts darf eine automatisierte Datenerfassung „nicht anlasslos erfolgen oder flächendeckend durchgeführt werden“.[30] Begriffe wie „erforderlich“ oder „sachdienlich“ stellen keine hinreichende Eingrenzung dar.[31] Das „strikte Verbot der Sammlung personenbezogener Daten auf Vorrat“ ist zu gewährleisten.[32] Eine „enge und konkrete Zweckbindung“ muss gesetzlich angeordnet werden.[33] § 5 Abs. 1 Nr. 1 BSIG-RegE trägt alledem keine Rechnung und ist daher verfassungswidrig.

4. Position der Zivilgesellschaft und der Datenschutzbeauftragten

Am 20.01.2009 kommentierte die Gesellschaft für Informatik, der Gesetzentwurf sehe in § 5 die ständige verdachtslose und

29 Bundesrat, BR-Drs. 62/09 (Beschluss), 6.

30 BVerfG, MMR 2008, 308, 308; BVerfG, NVwZ 2007, 688, 691.

31 BVerfG, MMR 2007, 93, 94; BVerfG, NVwZ 2007, 688, 691.

32 BVerfG, MMR 2006, 531.

33 BVerfGE 100, 313, 385 f.

sogar anlasslose vollständige Überwachung der gesamten Sprach- und Datenkommunikation aller Unternehmen und Bürger vor, die mit Bundesbehörden kommunizieren.[34] Die vollständige Überwachung jeglicher Kommunikation mit der Bundesverwaltung sei jedoch „eine untaugliche Sicherheitsmaßnahme."

Am 05.03.2009 kritisierte der Wirtschaftsverband BITKOM in einem Positionspapier, § 5 BSIG-RegE setze „keinen konkreten Verdacht voraus".[35] Dies käme „einer Generalermächtigung zur Speicherung gleich". Durch die Vorschrift werde „faktisch die Zweckbindung der Datenerfassung durch das BSI nachträglich aufgehoben." Der Vorschlag gehe weit „über das Ziel der Sicherung der Kommunikationstechnik des Bundes hinaus."

In seiner Stellungnahme vom 06.03.2009 äußerte der Bundesrat „erheblichen Bedenken", ob der mit § 5 BSIG-RegE verbundene Eingriff in das Fernmeldegeheimnis „verfassungsrechtlich zu rechtfertigen ist."[36] Die Maßnahme könne „zu allgemeinen Einschüchterungseffekten bei den Nutzern dieser Kommunikationstechnik führen und Beeinträchtigungen bei der Ausübung von Grundrechten bedingen". Die Heimlichkeit erschwere nachträglichen Rechtsschutz. Insbesondere die von § 5 Absatz 1 des Gesetzentwurfs gestattete anlasslose grundrechtseingreifende Auswertung aller Daten „ins Blaue hinein" sei mit der Verfassung nicht vereinbar.

Im April 2009 kritisierte der Deutsche Anwaltverein, § 5 BSIG-RegE fehle es an der verfassungsrechtlich gebotenen Anlassbezogenheit der Überwachung.[37] Die vollständige Überwachung sei „der falsche Ansatz zur Erhöhung der IT-Sicherheit". Stattdessen seien Sicherheitslücken in der eingesetzten IT-Infrastruktur und Software zu schließen, „welche Schadprogrammen das Eindringen erst ermöglichen." Die informationelle Selbstbestimmung der Nutzer sei „ein höheres Schutzgut als die technische Unversehrtheit von IT-Infrastrukturen." Wörtlich schreibt der Verein weiter:

> *„Die Erhöhung der IT-Sicherheit darf sodann nicht um den Preis der anlasslosen und permanenten Verletzung des Fernmeldegeheimnisses erfolgen. Nach § 5 soll eine ständige verdachts- und anlasslose vollständige Überwachung von Verbindungsdaten und Inhalten*

34 GI, Pressemitteilung vom 20.01.2009, www.gi-ev.de.

35 BITKOM, Positionspapier vom 05.03.2009, 6.

36 BR-Drs. 62/09 (Beschluss), 5.

37 DAV, Stellungnahme 2009-31 vom April 2009, 3.

erfolgen, die mit Bundesbehörden in Verbindung treten. Unabhängig davon, ob die Mittel zur vollständigen Überwachung überhaupt tauglich sind, ist eine solche vollständige Überwachung jeglicher Kommunikation unter Sicherheitsaspekten nicht angezeigt (s. dazu oben 1. a) und damit im Hinblick auf die Grundrechte auf informationelle Selbstbestimmung und das Fernmeldegeheimnis nicht verfassungsmäßig."

5. Eigener Kompromissvorschlag

In erster Linie ist zu fordern, § 5 BSIG-RegE ersatzlos zu streichen, weil die personenbezogene Aufzeichnung des Surfverhaltens zur Abwehr von Angriffen schlicht ungeeignet und zur Entfernung von Schadprogrammen nicht erforderlich ist; auch die in § 5 Abs. 1 Nr. 2 BSIG-RegE vorgesehene Filterung eingehender Daten auf Schadsoftware („Virenscanner") kann bereits nach geltendem Recht bei der jeweiligen Behörde vorgenommen werden.

Wollte man § 5 BSIG-RegE hingegen im Grundsatz akzeptieren und verfassungskonform umgestalten, so müsste die darin vorgesehene Aufzeichnung des Nutzungsverhaltens anlassbezogen ausgestaltet werden. Das BSI kann die laut Entwurfsbegründung geplante Sichtung von Datenvolumen und angeforderten URLs bereits anhand anonymer Protokolle vornehmen. Nur wenn diese Sichtung überhaupt Anhaltspunkte für einen Angriff ergibt, kann im Einzelfall eine personenbezogene Aufzeichnung verhältnismäßig sein. Gleichfalls kann eine Überprüfung auf Schadsoftware anlassbezogen nach der Feststellung einer konkreten Infektion vorgenommen werden. Mit den Grundrechten vereinbar ist indes auch eine anlassbezogene Ermächtigung zur Vornahme personenbezogener Aufzeichnungen nur, wenn eine enge Zweckbindung und eine konkrete Höchstspeicherfrist festgelegt werden.

§ 5 BSIG-RegE könnte dazu wie folgt verfassungskonform umformuliert werden:

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

(1) Das Bundesamt darf zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes ***die an den Schnittstellen*** *der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auswerten, soweit dies für die Erkennung und Abwehr von Schadprogrammen*

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

(2) Das Bundesamt darf zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen, ***in anonymisierter Form*** *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.* ***Liegen dem Bundesamt im Einzelfall zu dokumentierende tatsächliche Anhaltspunkte für eine Störung oder einen Fehler bei der Kommunikationstechnik des Bundes oder einen Angriff auf die Informationstechnik des Bundes vor, so darf es Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen, in personenbezogener Form erheben und automatisiert auswerten, soweit dies zur Beseitigung der Störung oder zur Abwehr des Angriffs erforderlich ist. Unbeschadet des Absatzes 3 hat das Bundesamt die nach Satz 2 erhobenen Daten unverzüglich, spätestens aber an dem auf ihre Erhebung folgenden Tag, zu löschen.***

(3) Eine über die Absätze 1 und 2 hinausgehende ***Speicherung und Nutzung von nach Absatz 1 oder 2 erhobenen 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. Im Falle der Bestätigung ist die weitere Verarbeitung personenbezogene 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.

Ein Schadprogramm kann beseitigt oder in seiner Funktionsweise gehindert werden. Die nicht automatisierte Verwendung der Daten nach den Sätzen 1 und 2 darf nur durch einen Bediensteten des Bundesamts mit der Befähigung zum Richteramt angeordnet werden. Die Beteiligten des Kommunikationsvorgangs sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder von Gefahren, die von einem Schadprogramm ausgehen, zu benachrichtigen, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange Dritter entgegenstehen. Die Unterrichtung kann unterbleiben, wenn die Person nur unerheblich betroffen wurde und anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat. In den Fällen der Absätze 4 und 5 erfolgt die Benachrichtigung durch die dort genannten Behörden in entsprechender Anwendung der für diese Behörden geltenden Vorschriften. Enthalten diese keine Bestimmungen zu Benachrichtigungspflichten, sind die Vorschriften der Strafprozessordnung entsprechend anzuwenden.

(4) Das Bundesamt kann die nach Absatz 3 verwendeten personenbezogenen Daten ***im Einzelfall*** *an die Strafverfolgungsbehörden zur Verfolgung einer Straftat von erheblicher Bedeutung oder einer mittels Telekommunikation begangenen Straftat übermitteln. Es kann diese Daten ferner* ***im Einzelfall*** *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.

(5) Für sonstige Zwecke kann das Bundesamt die ***nach Absatz 1 oder 2 erhobenen*** *Daten* ***im Einzelfall*** *übermitteln*

1. 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,

2. 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.

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

(6) Eine über die vorstehenden Absätze hinausgehende ***Verwendung von Protokolldaten oder*** *inhaltliche Auswertung* ***des Fernmeldeverkehrs*** *zu anderen Zwecken und die Weitergabe von personenbezogenen Daten an Dritte sind unzulässig. Werden aufgrund der Maßnahmen der Absätze 1 bis 3 Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder Daten im Sinne des § 3 Absatz 9 des Bundesdatenschutzgesetzes erlangt, dürfen diese nicht verwendet werden. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung sind unverzüglich zu löschen. Bestehen Zweifel, ob Erkenntnisse dem Kernbereich privater Lebensgestaltung zuzurechnen sind, sind diese entweder ebenfalls zu löschen oder unverzüglich* ***dem Amtsgericht, in dessen Bezirk das***

Bundesamt seinen Sitz hat, *zur Entscheidung über ihre Verwertbarkeit oder Löschung vorzulegen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.*

(7) Vor Aufnahme der Datenerhebung und -verwendung hat das Bundesamt ein Datenerhebungs- und -verwendungskonzept zu erstellen und für Kontrollen durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit bereitzuhalten. Das Konzept hat dem besonderen Schutzbedürfnis der Regierungskommunikation Rechnung zu tragen. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit teilt das Ergebnis seiner Kontrollen nach § 24 des Bundesdatenschutzgesetzes auch dem Rat der IT-Beauftragten der Bundesregierung mit.“

6. Die beste Lösung: Streichung des § 5 BSIG-RegE

Ungeachtet dieses Kompromissvorschlags bleibt es dabei, dass bereits das geltende Recht die zuverlässige Bereitstellung von Telemedien und die gezielte Beseitigung von Schadprogrammen ermöglicht, eine Datenspeicherung und -durchsicht durch das BSI mithin nicht erforderlich ist. Umgekehrt begründet jede Ermächtigung zur personenbezogenen Erfassung von Nutzungsdaten die Gefahr, dass hochsensible Informationen über unsere Internetnutzung versehentlich abhanden kommen, veröffentlicht werden oder absichtlich zweckentfremdet werden.

Da der vorgeschlagene § 5 BSIG-RegE eine potenziell unbegrenzte Menge äußerst sensibler Daten über unsere Internetnutzung Offenlegungs- und Missbrauchsrisiken aussetzen würde, sollte er insgesamt aus dem Gesetzentwurf gestrichen werden. Persönliche Daten nicht anzusammeln, stellt erwiesenermaßen die beste Garantie für unsere Sicherheit in der Informationsgesellschaft dar.

III. Sicherheit von Internetnutzern vor Datenlecks, Spionage und Datenhandel stärken

1. Sicherheit von Internetnutzern in Gefahr

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.[38] Das mit Diskretion werbende Erotikunternehmen Beate Uhse veröffentlichte die E-Mail-Adressen Tausender von Personen, die sich Sexfilme im Internet angesehen hatten.[39] In einem Forum des ZDF-Kinderkanals konnten sich beliebige Personen Klarnamen, Adresse, Telefonnummer und Geburtsdatum aller 1.000 registrierten Kinder verschaffen.[40]

2. Schwindendes Vertrauen

Wegen der vielen Fällen von Datenmissbrauch im Jahr 2008 sind inzwischen 80% der Bundesbürger „sehr besorgt“ um die Sicherheit ihrer Daten.[41] Eine deutliche Mehrheit der Bevölkerung fordert eine gesetzliche Stärkung des Datenschutzes.[42] Einer Umfrage aus dem Jahr 2007[43] 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.

3. Lösungsmöglichkeiten

Den besten und einzig wirksamen Schutz vor Datendiebstahl und Datenmissbrauch im Internet stellt es dar, wenn von vornherein möglichst wenige persönliche Daten erhoben und

38 Spiegel 43/2008 vom 20.10.2008, Seite 70.

39 Die Welt vom 04.09.2008: Beate Uhse verschlampt E-Mail-Adressen im Web.

40 Spiegel Online vom 16.10.2008: Kika stellt Daten von Kindern ungeschützt ins Web.

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

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

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

gespeichert werden. Internetnutzer erwarten daher, dass sie im virtuellen Leben ebenso anonym und überwachungsfrei handeln können wie es im wirklichen Leben weitgehend noch der Fall ist. Zur Stärkung der Privatsphäre und des Nutzervertrauens ist es dringend erforderlich, durchzusetzen, dass Telemediendienste so wenige persönliche Daten wie möglich verarbeiten und dass Nutzer über den Umgang mit ihren Daten wirklich frei entscheiden können.

4. Forderungen

Unter anderem sind dazu die folgenden Maßnahmen erforderlich:

- Erstreckung des Fernmeldegeheimnisses auf die Nutzung von Telemedien,
- Weitergabe von Nutzerdaten an Dritte nur unter den Voraussetzungen, die für die Offenlegung von Telekommunikationsinhalten gelten,
- Schaffung von Rechtssicherheit durch Klarstellung, dass Internetprotokoll-Adressen Nutzungsdaten im Sinne des § 15 TMG darstellen,
- Verbot der Erstellung von Nutzerprofilen ohne Einwilligung des Nutzers (§ 15 Abs. 3 TMG),
- Information der Nutzer über die Dauer der Aufbewahrung ihrer Daten (§ 13 Abs. 1 TMG),
- Stärkung des Rechts auf Anonymität durch ein wirkungsvolleres Koppelungsverbot als in § 12 Abs. 3 und § 13 Abs. 6 TMG vorgesehen,
- Schutz der Nutzer vor Ausspionieren durch „Spyware“, „Web-Bugs“ usw., indem Art. 5 Abs. 3 RiL 2002/58/EG endlich umgesetzt wird,
- Schutz der Nutzer vor unangemessenen Einwilligungsklauseln, indem klargestellt wird, dass derartige Klauseln der AGB-Kontrolle unterfallen und von Verbraucherverbänden erforderlichenfalls abgemahnt werden können.

Konkrete Formulierungsvorschläge zu diesen Punkten liegen dem Bundestag bereits vor.[44]

44 Breyer, Stellungnahme an den Wirtschaftsausschuss des Deutschen Bundestages vom 27.02.2009, Ausschussdrucksache 16(9)1419, http://www.bundestag.de/ausschuesse/a09/anhoerungen/Archiv/20_Anhoerung/Stellungnahmen/A-Drs_16-9-1419.pdf.

5. Fazit

Der Gesetzgeber muss den zunehmenden Datenskandalen mutig gegensteuern und die Anhäufung privater Informationen über Internetnutzer wirksam unterbinden. In einer Informationsgesellschaft sind die persönlichen Daten, die wir dem Internet anvertrauen, Schlüssel zu unserem Privatleben. Diese Daten dürfen nicht länger endlos gehortet und dem Zugriff von Datendieben und Betrügern ausgesetzt werden.

Wenn wir uns im Internet ebenso anonym wie sonst auch politisch informieren, über religiöse Fragen oder unsere Krankheiten erkundigen und Erotikangebote nutzen können, gewährleistet dies nicht nur unsere Sicherheit vor Datenpannen und Missbrauch. Auch die wirtschaftliche Entwicklung einer wichtigen Zukunftsbranche in Deutschland hängt davon ab, ob der Gesetzgeber aus den Datenskandalen, Datenpannen und Datenlecks der jüngsten Vergangenheit die richtigen Schlüsse zu ziehen vermag.

Dazu müssen die bestehenden Regelungen zum Schutz der Privatsphäre von Internetnutzern nicht nur erhalten bleiben, sondern deutlich ausgebaut werden. Der BSIG-Regierungsentwurf droht indes das genaue Gegenteil zu bewirken, wenn der Bundestag nicht noch entschieden nachbessert.