ARD • BDZV • DJV • Deutscher Presserat

VDZ • Ver.di • VPRT • ZDF

---

8. Mai 2009

Gemeinsame Stellungnahme

zum Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BT-Drs. 16/11967)

von

Arbeitsgemeinschaft der öffentlich-rechtlichen Rundfunkanstalten (ARD)

Bundesverband Deutscher Zeitungsverleger (BDZV)

Deutscher Journalisten-Verband (DJV)

Deutscher Presserat

Verband Deutscher Zeitschriftenverleger (VDZ)

Vereinte Dienstleistungsgewerkschaft (Ver.di)

Verband Privater Rundfunk und Telekommunikation (VPRT)

Zweites Deutsches Fernsehen (ZDF)

Zusammenfassung der Stellungnahme

Nach Meinung der Stellung nehmenden Verbände ist in dem Gesetzentwurf zu beanstanden, dass die Übermittlung der personenbezogenen Daten an die Strafverfolgungsbehörden nach Absatz 4 an keine weiteren Voraussetzungen geknüpft wird und insbesondere für die in § 53 StPO geschützten Berufsgruppen kein Schutz vorgesehen ist. Vorgaben des Bundesverfassungsgerichts z.B. in seinem Urteil vom 27. Februar 2008 zur Online-Durchsuchung und in seinem Beschluss vom 11. März 2008 zum Eilantrag in Sachen Vorratsdatenspeicherung bleiben unbeachtet. Außerdem sieht zwar § 5 Abs. 6 eine sofortige Löschungspflicht für Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder Daten im Sinne von § 3 Abs. 9 BDSG vor, nicht aber für Erkenntnisse, die andere schutzwürdige Inhalte betreffen könnten,

so zum Beispiel Erkenntnisse, die eindeutig dem Bereich der Presse- und Rundfunkfreiheit zuzuordnen sind. Löschungsfristen und die Dokumentation derselben für personenbezogene Daten, die der nicht automatisierten Auswertung unterliegen, lässt der Gesetzesvorschlag gänzlich vermissen.

Sachverhalt

Mit dem **Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BT-Drs. 16/11967)** beabsichtigt die Bundesregierung, die Informations- und Kommunikationstechnologie (IKT) des Bundes besser zu schützen. Die Informations- und Kommunikationstechnologie sei elementare Voraussetzung für das Funktionieren des Gemeinwesens. Auch die Verwaltung sei auf sichere und verfügbare Kommunikationstechnik angewiesen. Die Festlegung einheitlicher und strenger Sicherheitsstandards durch eine zentrale Stelle sei notwendig. Schwachstellen in der IKT-Infrastruktur würden für Wirtschafts-, Forschungs-, Industriespionage genutzt werden. Die Sicherheit der Informationstechnik (IT) sei ein wesentlicher Bestandteil der inneren und äußeren Sicherheit der Bundesrepublik Deutschland.

Die Bundesregierung schlägt daher die Schaffung neuer Befugnisse für das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor. Das BSI soll technische Vorgaben für die Sicherung der Informationstechnik in der Bundesverwaltung machen und Maßnahmen ergreifen, um Gefahren für die Sicherheit der Informationstechnik des Bundes abzuwehren. Zudem soll das BSI als zentrale Meldestelle für IT-Sicherheit Informationen über Sicherheitslücken und neue Angriffsmuster sammeln, auswerten und Informationen und Warnungen an die betroffenen Stellen oder die Öffentlichkeit weitergeben. Das Gesetz soll für alle Arten der elektronischen Kommunikation der Bürger mit allen wesentlichen Bundesbehörden gelten, z.B. auch mit dem Bundesdatenschutz- und Informationsfreiheitsbeauftragten.

Nach dem Art. 1[1] § 5 Abs. 3 bis Abs. 5 des Entwurfs soll das BSI verwendete personenbezogenen Daten, die sich auf ein Schadprogramm nach § 2 Abs. 5 beziehen, an die Strafverfolgungsbehörden zur Verfolgung einer Straftat von erheblicher Bedeutung oder einer mittels Telekommunikation begangenen Straftat übermitteln dürfen. Schließlich soll das BSI "für

[1] Art. 1 des Entwurfs betrifft die Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)

sonstige Zwecke" die Daten übermitteln dürfen 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, sowie, unter bestimmten, in § 3 des BVerfSchG festgelegten Voraussetzungen, an die Verfassungsschutzbehörden des Bundes und der Länder. Nur die Übermittlung an die Polizeien zum Zweck der Gefahrenabwehr bedarf der gerichtlichen Zustimmung. Für die Übermittlung an die Verfassungsschutzbehörden sollen die §§ 9 bis 16 des Artikel 10-Gesetzes entsprechend gelten. Zu anderen Zwecken soll eine Datenweitergabe unzulässig sein.

Stellungnahme

Aus Sicht der Stellung nehmenden Verbände bedarf der Gesetzesentwurf einer verfassungsrechtlichen begründeten Prüfung und Korrektur:

1) Es fehlt in § 5 Abs. 4 und Abs. 5 des Entwurfs gänzlich an einer die nach § 53 StPO Zeugnisverweigerungsberechtigten schützenden Einschränkung der Weitergabe von persönlichen Daten an die Strafverfolgungsbehörden oder die Polizeien.
2) In § 5 Absatz 4 BSIG-E fehlt es zudem an dem Richtervorbehalt.
3) Darüber hinaus ist nicht eindeutig geregelt, wann welche Daten einer Löschungspflicht unterliegen.

Hierzu im Einzelnen:

zu 1)

a) Unter Kommunikationstechnik versteht der Entwurf nach § 2 Abs. 3 BSIG-E allgemein die Informationstechnik, die der Kommunikation oder dem Datenaustausch von Bundesbehörden untereinander oder mit Dritten dient. Informationstechnik sind nach § 2 Abs. 1 BSIG-E alle technischen Mittel zur Verarbeitung oder Übertragung von Informationen.
b) Nach § 5 Abs. 1 Nr. 1 BSIG-E darf das Bundesamt zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes **Protokolldaten** erheben und automatisiert auswerten. **Protokolldaten** sind nach § 2 Abs. 8 BSIG-E Steuerdaten, Verkehrsdaten (nach § 3 Nr. 30 TKG) und Nutzungsdaten (§ 15 Abs. 1 TMG).

c) Nach § 5 Abs. 1 Nr. 2 BSIG-E darf das Bundesamt zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes, „an den **Schnittstellen** der Kommunikationstechnik des Bundes anfallende **Daten** automatisiert auswerten, soweit dies für die Erkennung und Abwehr von Schadprogrammen erforderlich ist."

d) Der Begriff „*Daten*" in § 5 Abs. 1 Nr. 2 ist im Gegensatz zu den Protokolldaten in § 5 Abs. 1 Nr. 1 nicht näher definiert. Legal definiert wird hingegen der Begriff „*Datenverkehr*" in § 2 Abs. 9 BSIG-E. Danach umfasst *Datenverkehr* auch Telekommunikationsinhalte nach § 88 Absatz 1 TKG und Nutzungsdaten nach § 15 Abs. 1 TMG[2]. Das lässt zum einen darauf schließen, dass *Daten* im Sinne des § 5 Abs. 1 Nr. 2 BSIG-E auch Kommunikationsinhalte umfassen – entsprechend dem *Datenverkehr* nach § 2 Abs. 9 des Entwurfs. Zudem wurde in der ersten Lesung des Entwurfs ausdrücklich darauf hingewiesen, dass "wer die Seiten des Bundesverwaltungsamts, des BKA, des BMI oder anderer Behörden des Bundes im Internet aufruft, dessen Eingaben, Klicks und Verweildauer auf den Seiten werden gespeichert und ausgewertet, und zwar ohne Anonymisierung und ohne Pseudonymisierung, nämlich im Klartext. Damit kann das BSI die gesamte Kommunikation der Bürgerinnen und Bürger mit Behörden abhören und auswerten, den Besuch von Internetseiten, E-Mails, Internet-Telefonie und Chats."[3] Hier wird die Erhebung und Auswertung von Inhaltsdaten beschrieben.

   Die Erfassung von Kommunikationsinhalten nach § 2 ergibt sich auch aus der systematischen Stellung zu Nr. 1, der eben nur die Steuerdaten eines Protokolls erfasst, sowie schließlich auch aus der Begründung zu § 5 Abs. 1 Nr. 2 BSIG-E.[4] Der Bundesrat hat in seiner Stellungnahme zu Recht daraus abgeleitet, dass "Der letzte Satz der Entwurfsbegründung verdeutlicht, dass eine Erfassung und Speicherung auch von Kommunikationsinhalten gestattet werden soll. Gerade an der Nahtstelle zwischen Bund und Unternehmen/ Bürger (§ 5 Absatz 1 Satz 1 Nummer 2 BSIG-E) dürfen danach – zweckbegrenzt – Kommunikationsinhalte erfasst und ausgewertet werden. Die Zweckbegrenzung (§ 5 Absatz 3

---

2 In der Begründung, S. 12, wird darauf hingewiesen, dass der Datenverkehr kann auch Telekommunikationsinhalte umfassen könne.

3 Protokoll der 211. Sitzung des BT am 19.03.2009, S. 22869, MdB Gisela Piltz (FDP)

4 Begründung S. 14: " Gemäß Nummer 2 kann das BSI auch automatisiert auf (technische) Telekommunikationsinhalte zugreifen, um diese auf Schadprogramme zu untersuchen oder auf Links zu Internetseiten, die ihrerseits Schadsoftware enthalten, die beim Aufruf versucht, sich automatisch auf dem Rechner des Benutzers zu installieren. Dies betrifft den Einsatz von Virenscannern und ähnlichen Detektionstools, der bislang nur mit Einwilligung der Betroffenen möglich ist.

   Die automatisierte Auswertung gestattet nicht die Speicherung der Inhalte über den für die technische Abwicklung des Kommunikations- und Erkennungsvorgangs ohnehin notwendigen Umfang hinaus.

BSIG-E) ist dabei so formuliert, dass der begrenzende Charakter zweifelhaft ist (siehe insbesondere § 5 Absatz 3 Satz 1 Nummer 3 a. E. BSIG-E)."[5]

Dies bedeutet, dass auch die Speicherung von Kommunikationsinhalten gestattet werden soll.

e) Eine nicht automatisierte Auswertung und Verwendung der in § 5 Absatz 1 BSIG-E genannten personenbezogenen Daten, d.h. Protokoll- und Telekommunikationsinhalte sowie Nutzungsdaten (s.o.), ist nach Absatz 2 Satz 3 BSIG-E – wie oben dargelegt – unter den Voraussetzungen der Absätzen 3 bis 5 zulässig.

f) Die Weitergabe der Daten nach § 5 Abs. 4 und Abs. 5 berührt den Kommunikationsbereich von Zeugnisverweigerungsberechtigten, die mit den Mitarbeitern der Bundesbehörden in elektronischen Datenaustausch treten. Das gilt insbesondere auch für Journalistinnen und Journalisten, die Anfragen an Bundesbehörden richten oder mit Informanten sprechen etc.

g) Die Befugnisse, die dem BSI eingeräumt werden sollen, insbesondere die Auswertung der erhobenen Daten und deren Weitergabe an Strafverfolgungsbehörden und Polizeien, ihre Rechte aus Art. 5 Abs. 1 Satz 2 GG, müssen das Zeugnisverweigerungsrecht der nach Art. 5 Abs. 1 Satz 2 GG geschützten Personen berücksichtigen.

h) Die Gewährleistungsbereiche der Presse- und Rundfunkfreiheit schließen diejenigen Voraussetzungen und Hilfstätigkeiten mit ein, ohne welche die Medien ihre Funktion nicht in angemessener Weise erfüllen können. Geschützt sind namentlich die Geheimhaltung der Informationsquellen und das Vertrauensverhältnis zwischen Presse beziehungsweise Rundfunk und den Informanten.[6] Dieser Schutz ist unentbehrlich, weil die Medien auf private Mitteilungen nicht verzichten können, diese Informationsquelle aber nur dann ergiebig fließt, wenn sich der Informant grundsätzlich auf die Wahrung des Redaktionsgeheimnisses verlassen kann.[7] Werden die Datenerhebungs- und Weiterleitungsbefugnisse des BSI, wie von der Bundesregierung vorgeschlagen, umgesetzt, bleibt kein Raum mehr für den Schutz der Informanten, der gerade im Bereich der Politik besonders wichtig ist.

i) Zwar handelt es sich bei der Sicherung von Kommunikationssystemen aus den in der Begründung aufgeführten Erwägungen (Funktionieren des Gemeinwesens, IKT-Infrastruktur

---

5 Stellungnahme des BR, BT-Drs. 16/12225, S. 3

6 BVerfGE 117, 244 (259); BVerfGE 100, 313 (365) m.w.N.

7 BVerfGE 117, 244 (259); vgl. BVerfGE 20, 162 (176, 187); 36, 193 (204).

als Bestandteil der Sicherheit Deutschlands) um einen legitimen Zweck und zweifelsohne ist das Mittel auch geeignet, diesen Zweck zumindest zu fördern. Diese Zwecke werden jedoch auch ohne insbesondere die Weitergabe nach § 5 Abs. 5 erreicht. Im Übrigen wäre klarzustellen, dass jedenfalls Inhaltsdaten nicht erhoben oder weitergegeben werden dürfen, wenn ein Zeugnisverweigerungsrecht in Rede steht. Werden Daten trotzdem erhoben, sind sie zu löschen oder jedenfalls mit einem Verwertungsverbot zu belegen, sobald das Zeugnisverweigerungsrecht bekannt wird.

zu 2)

a) Nur die Übermittlung nach § 5 Abs. 5 Satz 1 Nr. 1 bedarf der gerichtlichen Zustimmung. Der Gesetzesbegründung zufolge handelt es sich bei den nach Absatz 5 zu übermittelnden Daten um mögliche Zufallsfunde. Da das eigentliche Ziel die Suche nach Schadprogrammen sei, also die Suche nach technischen Inhalten, sei sonst kein Richtervorbehalt erforderlich[8].

b) Eine Übermittlung von Protokoll- und Telekommunikationsinhalten sowie Nutzungsdaten an verschiedene Strafverfolgungsbehörden und Polizeien ist demnach entweder ohne weitere Voraussetzungen an den Begriff der Schadprogramme geknüpft (Absatz 4) bzw. für sonstige Zwecke an einen Richtervorbehalt.

   Gemäß § 2 Abs. 5 BSIG-E sind Schadprogramme „Programme und sonstige informationstechnische Routinen und Verfahren, die dem Zweck dienen, unbefugt Daten zu nutzen oder zu löschen oder die dem Zweck dienen, unbefugt auf sonstige informationstechnische Abläufe einzuwirken." Die Gesetzesbegründung führt dazu weiter aus, dass Schadprogramme typischerweise Schäden verursachen, dies aber keine zwingende Voraussetzung ist und dass auch der Versand von Spam und so genannte DoS-Angriffe – Massenanfragen, um Server durch Überlastung lahm zulegen – unter den Begriff des Schadprogramms fallen sollen (BR-Drs 62/09, S. 14).

c) Besonders problematisch erscheint aus Sicht der Stellung nehmenden Verbände, dass die nach § 5 Abs. 3 erhobenen Daten nach Absatz 4 ohne weitere Einschränkungen zur Verfolgung einer Straftat von erheblicher Bedeutung oder einer mittels Telekommunikation begangenen Straftat an die Strafverfolgungsbehörden weitergeleitet werden können. Da-

[8] Begründung S. 15, BT-Drs. 16/11967: verwiesen wird insoweit auf die vergleichbaren Vorschriften des § 64 Abs. 1 TKG oder § 14 Abs. 7 des Gesetzes über die elektromagnetische Verträglichkeit von Betriebsmitteln (EMVG)

durch besteht die tatsächliche Gefahr, dass z.B. Inhalte einer E-Mail, die als „Zufallsfund" kategorisiert werden, vom Bundesamt für Sicherheit in der Informationstechnik direkt an eine Strafverfolgungsbehörde weitergeleitet werden, ohne dass für diesen grundrechtsintensiven Eingriff eine richterliche Kontrollinstanz einzuschalten wäre.

d) De facto werden damit Regelungen in der Strafprozessordnung umgangen, die für ähnlich gelagerte Fälle entwickelt worden sind. Möchte die Staatsanwaltschaft z.B. Verkehrsdaten erheben und nach § 100g StPO ein Auskunftsersuchen nach § 113b TKG an die nach § 113a TKG zur Vorratsdatenspeicherung verpflichteten Unternehmen richten, bedarf es einer gerichtlichen Anordnung nach §§ 100g Abs. 2 Satz 1, 100b Abs. 1 StPO.

e) Nicht berücksichtigt wird in § 5 Abs. 4 BSIG-E insoweit auch der Beschluss des Bundesverfassungsgerichts vom 11. März 2008 im Eilverfahren gegen die Vorratsdatenspeicherung[9], wonach die angeforderten Daten den Strafverfolgungsbehörden nur dann zu übermitteln sind, wenn Gegenstand des Ermittlungsverfahrens eine schwere Straftat im Sinne des § 100a Abs. 2 StPO ist, die auch im Einzelfall schwer wiegt, der Verdacht durch bestimmte Tatsachen begründet ist und die Erforschung des Sachverhalts auf andere Weise wesentlich erschwert oder aussichtslos wäre (§ 100a Abs. 1 StPO).

f) Nach § 5 Abs. 4 BSIG-E können nicht nur Verkehrsdaten im Sinne des § 96 TKG, sondern auch Telekommunikationsinhalte im Sinne von § 88 Abs. 1 TKG an die Strafverfolgungsbehörden weitergeleitet werden – ohne dass ein Richter eine solche Erhebung überhaupt anordnet, ohne dass die Strafverfolgungsbehörden überhaupt bereits mit einem Ermittlungsverfahren in der Größenordnung des § 100a Abs. 2 StPO befasst wären. Damit stellt § 5 Abs. 4 BSIG-E die Systematik von Anfangsverdacht, Ermittlungsverfahren und Ermittlungsmaßnahme auf den Kopf. § 5 Abs. 4 BSIG-E erlaubt nämlich eine verdachtslose Überwachung jedweder Kommunikation an den Schnittstellen der Kommunikationstechnik des Bundes. Die Überwachung ist geeignet, Verdachtsmomente für ein breit gefächertes Spektrum möglicher Straftaten aufgrund „zufälliger" Kenntnisnahme von Kommunikationsinhalten zu erheben, die dann konsequenterweise an die Strafverfolgungsbehörden weitergeleitet werden, welche auf diese Informationen einen Anfangsverdacht gründen und infolgedessen Ermittlungsmaßnahmen begründen können, denen sonst jegliche Grundlage gefehlt hätte.

g) Da die Frage, ob personenbezogene Daten an die Strafverfolgungsbehörden weitergege-

[9] BVerfG, 1 BvR 256/08 vom 11.3.2008, Absatz-Nr. (164), *http://www.bverfg.de/entscheidungen/rs20080311_1bvr025608.html*

ben werden dürfen oder nicht, einen Bereich berührt, der vom Gesetzgeber in anderen Verfahren dem Richter oder bei Gefahr im Verzug immerhin dem Staatsanwalt (§§ 100g Abs. 2 Satz 1, 100b Abs. 1 Satz 2 StPO) zugewiesen wird, ist eine solche Einschränkung auch für § 5 Abs. 4 BSIG-E notwendig.

h) Die vom Entwurf vorgesehene Herangehensweise, in § 5 Abs. 4 BSI-G keinen Richtervorbehalt vorzusehen, ist wohl schwerlich mit dem Grundgesetz vereinbar. Verfahrensprinzipien sind Ausfluss der Grundrechte der Verfahrensbeteiligten, insbesondere Art. 20 Absatz 3 und Art. 2 Absatz 1 GG.[10] Grundrechtsschutz ist weitgehend auch durch die Gestaltung von Verfahren zu bewirken und Grundrechte beeinflussen demgemäß nicht nur das gesamte materielle, sondern auch das Verfahrensrecht, soweit dieses für einen effektiven Grundrechtsschutz von Bedeutung ist.[11] Diesem Anspruch entspricht Absatz 4 nicht.

zu 3)

a) Für Erkenntnisse, die den Kernbereich privater Lebensgestaltung oder Daten im Sinne von § 3 Abs. 9 BDSG[12] betreffen, sieht § 5 Abs. 6 S. 2 BSIG-E ein Verwendungsverbot sowie eine Löschungspflicht vor. Bestehen Zweifel daran, ob die Daten dem Kernbereich privater Lebensgestaltung zuzuordnen sind, sind die Daten zu löschen oder unverzüglich dem Bundesministerium des Inneren zur Entscheidung über Verwertung oder Löschung vorzulegen. Die so begründete Zuständigkeit des Bundesministeriums des Inneren und nicht eines Gerichts, ob Erkenntnisse zum Kernbereich privater Lebensgestaltung gehören, ist nach der Rechtsprechung des Bundesverfassungsgerichts im Zusammenhang mit dem Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht mit der Verfassung vereinbar. Danach ist bei einem Grundrechtseingriff von besonders hohem Gewicht wie z. B. dem heimlichen Zugriff auf ein informationstechnisches System grundsätzlich die Kontrolle durch einen Richter vorzusehen. Der Gesetzgeber darf eine andere Stelle nur dann mit der Kontrolle betrauen, wenn diese gleiche Gewähr für ihre Unabhängigkeit und Neutralität bietet wie ein Richter[13]. Es ist äußerst

---

10 BVerfGE 63, 131 (143); 53, 30 (65); Beulke, Strafprozessrecht, 9. Aufl., Rz. 454; Maunz-Dürig, GG-Kommentar, Art. 2 Abs. 1, Rz. 137.

11 BVerfGE 53, 30 (65)

12 Besondere Daten i.S.d. § 3 Abs. 9 BDSG sind personenbezogene Daten als Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

13 BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (259f), h*ttp://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html*

fraglich, ob das BMI als für Sicherheitsfragen zuständiges Ministerium diese Unabhängigkeit gewährleisten kann.

b) Bezüglich der Löschung von personenbezogenen Daten spricht § 6 BSIG-E lediglich von einer unverzüglichen Löschung, „sobald sie für die Erfüllung der Aufgaben für die sie erhoben worden sind, oder für eine etwaige gerichtliche Überprüfung nicht mehr benötigt werden." Eine Speicherungs-Höchstdauer ist damit nicht festgelegt.

   Die Anforderungen an die *Bestimmtheit* von Normen, die das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG einschränken, „soll sicherstellen, dass die gesetzesausführende Verwaltung für ihr Verhalten steuernde und begrenzende Handlungsmaßstäbe vorfindet", und nicht dazu führen, dass sich die Verwaltung bei Zweifeln an die Verwaltung wendet[14].

   Diese Zweifel hinsichtlich der Speicherungs-Höchstdauer von Inhaltsdaten werden durch den Vergleich der die Löschungsfristen regelnden Normen nicht beseitigt. Im Gegenteil: In § 5 Abs. 1 Satz 2 BSIG-E wird eine sofortige Löschungspflicht für Daten, die der *automatisierten* Auswertung unterliegen, festgeschrieben. Nach § 5 Abs. 2 Satz 1 dürfen Protokolldaten nach § 5 Abs. 1 Satz 1 Nr. 1 BSIG-E über den für die automatische Auswertung erforderlichen Zeitraum hinaus höchstens für drei Monate gespeichert werden, wenn der Verdacht besteht, dass diese für die Datenverarbeitung nach § 5 Abs. 3 Satz 2[15] erforderlich sind. So gespeicherte Daten dürfen aber nach § 5 Abs. 2 Satz 2 nur automatisiert ausgewertet werden.

   Für die viel interessantere Frage, wie lange personenbezogenen Daten, die nicht Protokolldaten im Sinne von § 5 Abs. 1 Satz 1 Nr. 1 sind, sondern Kommunikationsinhalte betreffen und *nicht automatisiert* ausgewertet werden und gespeichert werden dürfen, schweigt das Gesetz.

c) Für den Umgang mit Kommunikationsinhalte betreffenden Daten und mit sonstigen Daten – denn auch nach Auffassung des Bundesverfassungsgerichts gibt es „unter den Bedingungen der elektronischen Datenverarbeitung (...) kein schlechthin, also ungeachtet des Verwendungskontextes, belangloses personenbezogenes Datum"[16] – ist ein sensiblerer Umgang wünschenswert. Zu denken ist dabei an eine Ergänzung des § 6 Satz 1 BSIG-E

---

14 BVerfGE 118, 168 [186]

15 Danach ist die weitere Datenverarbeitung erforderlich, um Schadprogramm selbst oder Gefahren die davon ausgehen, abzuwehren oder um andere Schadprogramme zu erkennen oder abzuwehren.

16 BVerfGE 118, 168 [185]

um eine Formulierung, wie sie sich z.B. im § 4 Absatz 1 Satz 2 und 3 G-10 oder § 101 Abs. 8 StPO findet: Die Löschung der Daten erfolgt unter Aufsicht eines Bediensteten zum Richteramt, bzw. die Löschung ist zumindest zu protokollieren, bzw. aktenkundig zu machen.

d) Die durch § 5 BSIG-E zu schaffenden Befugnisse für das Bundesamt für Sicherheit in der Informationstechnik, insbesondere im Hinblick auf den weiten Spielraum des § 5 Abs. 1 Nr. 2, der sich auf alle *an den Schnittstellen der Kommunikationstechnik anfallenden Daten* bezieht, ist ein eklatanter Eingriff in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, denn „auch der Umgang mit personenbezogenen Daten, die für sich genommenen nur geringen Informationsgehalt haben, kann (...) grundrechtserhebliche Auswirkungen auf die Privatheit und Verhaltensfreiheit des Betroffenen haben."[17]

e) Auch der Bundesrat äußert in seiner Stellungnahme[18] erhebliche Zweifel an der Vereinbarkeit des Gesetzesentwurfs der Bundesregierung mit verfassungsrechtlichen Vorgaben. Im Mittelpunkt der Kritik steht insbesondere die Eingriffsintensität, die durch die Heimlichkeit des Eingriffs und mangelnde Rechtsschutzmöglichkeiten intensiviert wird und einen allgemeinen Einschüchterungseffekt bei Nutzern befürchten lässt.

Die Erwiderung[19] der Bundesregierung auf die Stellungnahme des Bundesrats vermag die oben dargestellten, verfassungsrechtlichen Zweifel an dem Gesetzesentwurf nicht zu entkräften.

Nach Ansicht der Bundesregierung ist die Eingriffsschwelle – auch nach Maßgabe der Rechtsprechung des Bundesverfassungsgerichts – gar nicht überschritten, "soweit die Daten unverzüglich ausgewertet und danach sofort und spurenlos wieder gelöscht werden, wie es der Gesetzesentwurf vorsieht." Damit bezieht sich die Bundesregierung auf die Entscheidung des Bundesverfassungsgerichts zur automatisierten Kennzeichenerfassung, die nach Ansicht des Gerichts dann nicht in das Recht auf informationelle Selbstbestimmung eingreift, wenn das Kennzeichen unverzüglich mit dem Fahndungsbestand abgeglichen und ohne weitere Auswertung sofort wieder gelöscht wird.[20]

---

17 BVerfGE 118, 168 [185]

18 BR-Drs. 62/1/09; BT Drs. 16/12225 (S. 1-5).

19 BT-Drs. 16/12225 (S. 7)

20 BVerfGE 120, 378 (397)

Damit verweigert die Bundesregierung nicht nur eine Auseinandersetzung mit den vom Bundesrat vorgebrachten Kritikpunkten, sondern bedient sich darüber hinaus auch noch einer ungeeigneten höchstrichterlichen Referenz. Angesichts der Vielzahl von Entscheidungen, die das Bundesverfassungsgericht in den letzten Jahren zum Datenschutz in Zeiten des Internets getroffen hat, ist es völlig unvertretbar, die Speicherung von Protokoll- und Inhaltsdaten von Kommunikationsvorgängen mit einer Entscheidung zum automatisierten Abgleich von Kfz-Kennzeichnen zu rechtfertigen.

Diese Argumentationsweise zeigt nur, dass sich auch die Bundesregierung darüber im Klaren ist, dass ihr Vorschlag in dieser Form nicht mit der neuesten Rechtsprechung des Bundesverfassungsgerichts vereinbar ist.

Auch der Einwand der Bundesregierung, ein etwaiger Grundrechtseingriff sei deshalb verhältnismäßig, weil die Absätze 2 bis 7 "umfangreiche materielle und verfahrenssichernde Vorkehrungen" träfen, "um mögliche Beeinträchtigungen des dann betroffenen Fernmeldegeheimnisses so gering wie möglich zu halten", vermag ebenso wenig zu überzeugen wie der Einwand, "dass – anders als z. B. bei der Telekommunikationsüberwachung – die Maßnahme niemals darauf" abzielten, "Inhalte der Kommunikation zu erfassen".

In seiner Entscheidung zur Online-Durchsuchung hat das Bundesverfassungsgericht noch einmal hervorgehoben, dass eine Norm, die heimliche Ermittlungstätigkeiten des Staates vorsieht, die besonders geschützte Zonen der Privatheit berühren oder eine besonders hohe Eingriffsintensität aufweisen, wie z.B. hinsichtlich von Zeugnisverweigerungsrechten, dem Gewicht des Grundrechtseingriffs durch geeignete Verfahrensvorkehrungen Rechnung zu tragen hat. Insbesondere sei der Zugriff grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen.[21]

Dies ist hier, wie oben dargestellt, nicht erfolgt. Im Gegensatz zur Auffassung der Bundesregierung enthalten § 5 Absätze 2 bis 7 keinesfalls materielle wie verfahrenssichernde Vorkehrungen, um Grundrechtseingriffe gering zu halten. Die Absätze 2 bis 7 erweitern vielmehr die

[21] BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (257ff.), *http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html*; vgl. BVerfG, Beschluss vom 13. Juni 2007 - 1 BvR 1550/03 u.a. -, NJW 2007, S. 2464 (2471), m.w.N

in Absatz 1 begründeten Eingriffsbefugnisse des BSI und lassen eine richterliche Kontrolle der Weitergabe der Daten vermissen.

Die Bundesregierung erklärt, der Einsatz von vergleichbar arbeitenden Programmen bei Dienstanbietern, Unternehmern und Privatpersonen habe nicht zu einem Einschüchterungseffekt bei den Nutzern der Kommunikationstechnik geführt und möchte damit wohl den Schluss nahe legen, dass folglich der Einsatz von Virenscannern durch das BSI auch keinen negativen Einfluss auf das Kommunikationsverhalten der Bürger haben werde. Es ist nicht ausgeschlossen, dass hier „Äpfel mit Birnen verglichen“ werden. Nicht nur wird in der Gegenäußerung der Bundesregierung vernachlässigt, dass die Kritik an dem Gesetzesentwurf nicht allein auf den Einsatz von Virenscanner abzielt, sondern vielmehr und im Besonderen die weitergehende Datenverarbeitung im Blick hat. Auch die Tatsache, dass es ein elementarer Unterschied ist, ob ein Dienstanbieter bzw. eine Privatperson oder der Staat mit seinen Sanktionsmöglichkeiten Daten protokolliert, Zugriff auf Inhalte hat und sich die Möglichkeit vorbehält, den Inhalt von Kommunikationsvorgängen an Strafverfolgungsbehörden weiterzuleiten, wird in der Gegenäußerung nicht richtig gewichtet. Damit bleibt die zu Recht geäußerte Befürchtung des Bundesrats bestehen, die so auch das Bundesverfassungsgericht vertritt: "Soweit Daten erhoben werden, die Aufschluss über die Kommunikation des Betroffenen mit Dritten geben, wird die Intensität des Grundrechtseingriffs dadurch weiter erhöht, dass die – auch im Allgemeinwohl liegende – Möglichkeit der Bürger beschränkt wird, an einer unbeobachteten Fernkommunikation teilzunehmen. Eine Erhebung solcher Daten beeinträchtigt mittelbar die Freiheit der Bürger, weil die Furcht vor Überwachung, auch wenn diese erst nachträglich einsetzt, eine unbefangene Individualkommunikation verhindern kann."[22] Nichts anderes kann hinsichtlich der Kommunikation von zeugnisverweigerungsberechtigten Personen gelten.

Benno H. Pöppelmann
- DJV-Justiziar -

[22] BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (233), *http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html*; vgl. zur Erhebung von Verbindungsdaten BVerfGE 115, 166 (187 ff.)