**Deutscher Bundestag** **Drucksache 16/12225**

**16. Wahlperiode**

(zu Drucksache 16/11967)
12. 03. 2009

# Unterrichtung

**durch die Bundesregierung**

## Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes – Drucksache 16/11967 –

## Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung

Der Bundesrat hat in seiner 856. Sitzung am 6. März 2009 beschlossen, zu dem Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes wie folgt Stellung zu nehmen:

1. **Zu Artikel 1** (§ 3 Absatz 1 Nummer 11, Absatz 3 – neu –, § 8 Absatz 3 Satz 1, 1a – neu –, Absatz 4 – neu –, § 9 Absatz 4 Nummer 3 – neu –, § 10 Absatz 1 und 2 Satz 3 BSIG)

Artikel 1 ist wie folgt zu ändern:

a) § 3 ist wie folgt zu ändern:

aa) Absatz 1 Nummer 11 ist wie folgt zu fassen:

„11. in begründeten Ausnahmefällen die Bereitstellung von IT-Sicherheitsprodukten für Stellen des Bundes und auf Ersuchen auch für die der Länder,".

bb) Es ist folgender Absatz anzufügen:

„(3) Das Bundesamt kann den Arbeitskreis der Staatssekretäre für E-Government in Bund und Ländern oder dessen jeweilige Nachfolgeorganisation beraten und unterstützen."

b) § 8 ist wie folgt zu ändern:

aa) Absatz 3 ist wie folgt zu ändern:

aaa) Satz 1 ist wie folgt zu fassen:

„Die Bereitstellung von IT-Sicherheitsprodukten durch das Bundesamt nach § 3 Absatz 1 Satz 2 Nummer 11 erfolgt nach Durchführung von Vergabeverfahren auf Grund einer entsprechenden Bedarfsfeststellung oder durch Eigenentwicklung."

bbb) Nach Satz 1 ist folgender Satz einzufügen:

„IT-Sicherheitsprodukte können nur in begründeten Ausnahmefällen durch eine Eigenentwicklung des Bundesamtes nach § 3 Absatz 1 Satz 2 Nummer 11 bereitgestellt werden."

bb) Es ist folgender Absatz anzufügen:

„(4) Vorgaben nach den Absätzen 1 bis 3 sind, soweit sie die Kommunikationstechnik des Bundes mit den Ländern oder die Schnittstellen der Kommunikationstechnik des Bundes mit den Ländern regeln, mit dem Arbeitskreis der Staatssekretäre für E-Government in Bund und Ländern oder dessen jeweiliger Nachfolgeorganisation zu vereinbaren."

c) In § 9 Absatz 4 ist der Punkt am Ende der Nummer 2 durch ein Komma zu ersetzen und folgende Nummer anzufügen:

„3. der Arbeitskreis der Staatssekretäre für E-Government in Bund und Ländern oder dessen jeweilige Nachfolgeorganisation in Angelegenheiten, die seine Zuständigkeit betreffen, festgestellt hat, dass Länderinteressen der Erteilung nicht entgegenstehen."

d) In § 10 Absatz 1 und 2 Satz 3 sind jeweils die Wörter „ohne Zustimmung des Bundesrates" zu streichen.

Begründung

**Zu den Buchstaben a und b Doppelbuchstabe bb, den Buchstaben c und d**

Obwohl der Gesetzentwurf grundsätzlich die Sicherheit der Informationstechnik des Bundes betrifft, können sich die Regelungen in erheblichem Umfang, insbesondere im Bereich der Standardsetzung und Zertifizierung, zumindest faktisch auf die Informationstechnik in der Hoheit

der Länder und Kommunen auswirken. Dies kann im Hinblick auf die im Rahmen der Föderalismuskommission II beschlossene Grundgesetzänderung in Artikel 91c GG nicht hingenommen werden.

Mit der Ergänzung „und auf Ersuchen auch für die der Länder“ in Artikel 1 § 3 Absatz 1 Nummer 11 soll sichergestellt werden, dass auch die Länder in den Genuss der Sicherheitsprodukte kommen können.

In Erwartung der Einrichtung eines IT-Planungsrats sollten in Artikel 1 § 3 Absatz 3 die Aufgaben des Bundesamtes im Verhältnis zum Arbeitskreis der Staatssekretäre für E-Government in Bund und Ländern bzw. dem IT-Planungsrat als dessen voraussichtliche Nachfolgeorganisation geregelt werden.

Die Vorgaben des Bundesamtes gemäß Artikel 1 § 8 können sich in erheblichem Umfang und mit derzeit nicht absehbaren Kostenrisiken auf die Informationstechnik in der Hoheit der Länder und Kommunen auswirken. Dies ist z. B. bei Bund-Länder-übergreifender Kommunikation oder bei Nutzung von vom Bund bereitgestellten IT-Diensten der Fall. Folge wäre etwa, dass nur noch oder sogar parallel zur bereits vorhandenen Sicherheitsinfrastruktur der Länder Netz-, Signatur- oder Verschlüsselungstechnik nach den Vorgaben des BSI gemäß Artikel 1 § 8 beschafft und eingesetzt werden müssten.

Deshalb sind Vorgaben nach Artikel 1 § 8 Absatz 1 bis 3, soweit sie die Kommunikationstechnik oder die Schnittstellen der Kommunikationstechnik des Bundes mit den Ländern regeln, mit dem Arbeitskreis der Staatssekretäre für E-Government in Bund und Ländern bzw. dessen jeweiliger Nachfolgeorganisation zu vereinbaren.

Des Weiteren sind im Rahmen der Erteilung von Sicherheitszertifikaten die Interessen der Länder zu wahren. Die Ergänzung in Artikel 1 § 9 Absatz 4 Nummer 3 trägt dem Rechnung.

In Artikel 1 § 10 Absatz 1 und 2 Satz 3 ist „ohne Zustimmung des Bundesrates“ zu streichen, da Artikel 80 Absatz 2 GG eine hinreichende Regelung trifft.

**Zu Buchstabe a Doppelbuchstabe aa und Buchstabe b Doppelbuchstabe aa**

§ 8 BSIG-E ermächtigt das BSI zu weitreichenden Eingriffen in Vergabeverfahren und gefährdet damit den Wettbewerb. Die technischen Richtlinien stellen einen Eingriff in die Auftragsvergabe anderer Behörden dar und haben unmittelbare Auswirkungen darauf, welche Informationstechnologie andere Behörden einsetzen. Daher sollte der Rat der IT-Beauftragten unmittelbaren Einfluss auf die der Vergabepraxis künftig zu Grunde liegenden technischen Richtlinien nehmen können.

Des Weiteren bestünde die Gefahr der Wettbewerbsverzerrung, wenn auf Grund von einseitig gefassten Spezifikationen der Richtlinien eine zu begrenzte Auswahl von potenziellen Anbietern in Betracht kommen würde oder wenn nur die vom BSI bereitgestellten Produkte die Standards erfüllten.

Mit der eingeräumten Befugnis zur Entwicklung und Bereitstellung eigener IT-Sicherheitsprodukte für Bundesbehörden wird dem BSI gesetzlich eine einzigartige Stellung gesichert: als Anbieter, Prüfer und Zertifizierer von IT-Sicherheitsprodukten. Eine solche Stellung und der potenzielle Interessenkonflikt erfordern zwingend Kontroll- und Beschränkungsmechanismen. Grundsätzlich müssen Eigenprodukte der Verwaltung angesichts eines hoch entwickelten privaten Anbietermarkts eine zu begründende Ausnahme bleiben. Behörden sind nur eingeschränkt in der Lage, die für die Entwicklung von IT-Systemen notwendige Qualifikation dauerhaft vorzuhalten.

Aus diesem Grund sollten dem Subsidiaritätsprinzip entsprechend nur an den Stellen Eigenentwicklungen eingesetzt werden, an denen entsprechende Systeme nicht am Markt verfügbar sind.

Als Folge ist § 3 Absatz 1 Nummer 11 neu zu fassen.

2. **Zu Artikel 1** (§ 5 Absatz 1 BSIG)

Der Bundesrat bittet, im weiteren Verlauf des Gesetzgebungsverfahrens zu prüfen, ob die in § 5 Absatz 1 des Gesetzentwurfs vorgesehene Befugnis des Bundesamtes für Sicherheit in der Informationstechnik, ohne jeden Anlass „Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen“, zu erheben und automatisiert auszuwerten sowie „die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten“ einschließlich der Kommunikationsinhalte automatisiert auszuwerten,

– die hohen verfassungsrechtlichen Anforderungen an die Rechtfertigung von Eingriffen in das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung erfüllt, insbesondere

– einen verhältnismäßigen Ausgleich zwischen dem gravierenden Grundrechtseingriff und der Schutzgutgefährdung herbeiführt und

– die Gefahr von allgemeinen Einschüchterungseffekten bei den Nutzern dieser Kommunikationstechnik vermeidet.

Begründung

Die Regelung in § 5 BSIG-E soll dem Bundesamt für Sicherheit in der Informationstechnik die Befugnis verschaffen, zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes die in Absatz 1 genannten Daten automatisiert auszuwerten. Es begegnet erheblichen Bedenken, ob der hiermit verbundene Eingriff in das Fernmeldegeheimnis nach Artikel 10 des Grundgesetzes (siehe auch § 11 BSIG-E) auf der Grundlage der in § 5 BSIG-E vorgesehenen Regelungen verfassungsrechtlich zu rechtfertigen ist.

Nach § 5 Absatz 1 Satz 1 Nummer 1 BSIG-E darf das BSI „Protokolldaten“ erheben und auswerten. Diese haben nach der Legaldefinition in § 2 Absatz 8 BSIG-E keinen Bezug zu Kommunikationsinhalten. Nach § 5 Absatz 1 Satz 1 Nummer 2 BSIG-E darf das BSI aber auch „die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auswerten“. Dieser Begriff der Daten ist im Gesetz selbst nicht definiert, so dass er grundsätzlich auch Kommunikationsinhalte erfasst. Diesen Eindruck stützt die Entwurfsbegründung (Bundesratsdrucksache 62/09, Seite 18), wenn es dort heißt: „Gemäß Nummer 2 kann das BSI auch automatisiert auf („technische“) Telekommunikationsinhalte zu-

greifen, um diese auf Schadprogramme zu untersuchen oder auf Links zu Internetseiten, die ihrerseits Schadsoftware enthalten, die sich beim Aufruf versucht 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.“ 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 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).

Auf dieser Grundlage und der vom Bundesverfassungsgericht für das Gewicht eines Grundrechtseingriffs als maßgebend entwickelten Kriterien erweist sich der Eingriff in die dargestellte Grundrechtsposition als gravierend:

– Bei erfassten Kommunikationsinhalten ist die Persönlichkeitsrelevanz der Informationen, die von der informationsbezogenen Maßnahme erfasst werden (vgl. BVerfG, Beschluss vom 4. April 2006, 1 BvR 518/02, BVerfGE 115, 320 <347>) als sehr hoch einzuschätzen.

– § 5 Absatz 1 BSIG-E gestattet zunächst die anlasslose Auswertung aller genannten Daten (vgl. BVerfG, Urteil vom 27. Juli 2005, 1 BvR 668/04, BVerfGE 113, 348 <383>; Beschluss vom 4. April 2006, a. a. O., BVerfGE 115, 320 <354>) und begrenzt nur deren Speicherung und weitere Verwendung.

– Die von § 5 Absatz 1 Satz 1 Nummer 2 BSIG-E gestattete Auswertung aller an Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten kann zu allgemeinen Einschüchterungseffekten bei den Nutzern dieser Kommunikationstechnik führen und Beeinträchtigungen bei der Ausübung von Grundrechten bedingen (vgl. BVerfG, Urteil vom 15. Dezember 1983, 1 BvR 209/83 u. a., BVerfGE 65, 1 <42>; Beschluss vom 12. April 2005, 2 BvR 1027/02, BVerfGE 113, 29 <46>).

– Nach § 5 Absatz 3 Satz 4 und 5 BSIG-E erfolgt die Auswertung der Daten bis zum Erkennen des Schadprogramms oder anderer Gefahr heimlich. Dies führt zu einer weiteren Erhöhung des Gewichts der gesetzgeberischen Freiheitsbeeinträchtigung (vgl. BVerfG, Urteil vom 12. März 2003, 1 BvR 330/96, 1 BvR 328/99, BVerfGE 107, 299 <321>; Urteil vom 2. März 2006, 2 BvR 2099/04, BVerfGE, 115, 166 <194>; Beschluss vom 4. April 2006, a. a. O., BVerfGE 115, 320 <353>). Dem Betroffenen wird durch die Heimlichkeit des Eingriffs vorheriger Rechtsschutz faktisch verwehrt und nachträglicher Rechtsschutz kann zumindest erschwert werden (vgl. BVerfG, Urteil vom 15. Dezember 1983, a. a. O., BVerfGE 113, 348 <383 f.>; Beschluss vom 13. Juni 2007, 1 BvR 1550/03, 1 BvR 2357/04, 1 BvR 603/05, NJW 2007, S. 2464 <2470 f.>).

Vor diesem Hintergrund ist es erheblichen Zweifeln ausgesetzt, ob die in § 5 BSIG-E formulierten Eingriffsschwellen einen verhältnismäßigen Ausgleich zwischen dem hier gravierenden Grundrechtseingriff und der Schutzgutgefährdung herbeiführen. Insbesondere die von § 5 Absatz 1 des Gesetzentwurfs gestattete anlasslose grundrechtseingreifende Auswertung aller Daten „ins Blaue hinein“ lässt die Verfassung nicht zu.

3. **Zu Artikel 1** (§ 5 Absatz 5 Satz 2 BSIG)

In Artikel 1 § 5 Absatz 5 Satz 2 ist nach dem Wort „der“ das Wort „vorherigen“ einzufügen.

Begründung

Die Änderung dient der Klarstellung. Der Rechtsbegriff der Zustimmung umfasst im bürgerlichen Recht sowohl die Einwilligung (vorherige Zustimmung) als auch die Genehmigung (nachträgliche Zustimmung), vgl. Legaldefinitionen in § 183 Satz 1 und § 184 Absatz 1 BGB. Von diesem Begriffsverständnis geht offenbar auch der Gesetzentwurf aus. Für den in § 5 Absatz 5 Satz 5 geregelten Zustimmungsvorbehalt bei einer Datenübermittlung an die Verfassungsschutzbehörden wird durch den Wortlaut („nach Zustimmung des Bundesministeriums des Innern“) hinreichend deutlich, dass eine vorherige Zustimmung erforderlich sein soll. Die in § 5 Absatz 5 Satz 2 enthaltene Formulierung „bedarf der gerichtlichen Zustimmung“ kann hingegen – auch im Hinblick auf die von § 5 Absatz 5 Satz 5 abweichende Formulierung – dahingehend verstanden werden, dass die für eine Datenübermittlung nach § 5 Absatz 5 Satz 1 Nummer 1 erforderliche gerichtliche Zustimmung auch nachträglich erteilt werden kann. Damit würde aber – bei denkbarer Verweigerung der Zustimmung – der Schutzzweck des Zustimmungsvorbehaltes unterlaufen.

4. **Zu Artikel 1** (§ 7 Absatz 1 Satz 1a – neu – BSIG)

In Artikel 1 ist in § 7 Absatz 1 nach Satz 1 folgender Satz einzufügen:

„Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung der Warnung über diese zu informieren.“

Begründung

Bei der Identifizierung von Sicherheitslücken in Programmen sollte deren Behebung erstes Ziel sein. Um das Risiko der Ausnutzung von Sicherheitslücken in gefährdeten Programmen nicht zu erhöhen, ist es zwingend erforderlich, die betroffenen Anbieter vor der Öffentlichkeit zu informieren und ihnen Gelegenheit zu geben, geeignete Gegenmaßnahmen vorzubereiten und umzusetzen. Warnungen ohne vorherige Information der Programmanbieter hätten massive Auswirkungen auf den jeweiligen Anbieter und könnten dessen Geschäftsmodelle gefährden.

5. **Zu Artikel 3** (§ 15 Absatz 3 und 9, § 16 Absatz 2 Nummer 5 TMG)

Artikel 3 ist wie folgt zu fassen:

‚Artikel 3
Änderung des Telemediengesetzes

Das Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 2 des Gesetzes vom 25. Dezember 2008 (BGBl. I S. 3083) geändert worden ist, wird wie folgt geändert:

1. § 15 wird wie folgt geändert:
   a) Absatz 3 wird wie folgt geändert:
      aa) In Satz 1 werden die Wörter „dem nicht widerspricht“ durch die Wörter „darin einwilligt“ ersetzt.
      bb) Nach Satz 1 wird folgender Satz eingefügt:
      „Der Nutzer kann seine Einwilligung jederzeit widerrufen.“
   b) Folgender Absatz 9 wird angefügt:
      „(9) Liegen dem Diensteanbieter zu dokumentierende tatsächliche Anhaltspunkte vor, dass bestimmte 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 sind. 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.“
2. In § 16 Absatz 2 Nummer 5 werden nach den Wörtern „§ 15 Absatz 1 Satz 1“ das Wort „oder“ durch ein Komma ersetzt und nach den Wörtern „Absatz 8 Satz 1 oder 2“ die Wörter „oder Absatz 9 Satz 1 bis 3“ eingefügt.‘

Begründung

**Zu Nummer 1**

**Zu Buchstabe a**

Im Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes (Bundesratsdrucksache 4/09) ist vorgesehen, die Weitergabe personenbezogener Daten zu Werbezwecken nach § 28 Absatz 3 BDSG künftig grundsätzlich von der Einwilligung des Betroffenen abhängig zu machen. Die Erstellung von Nutzungsprofilen durch Diensteanbieter sowie deren Nutzung zu Werbezwecken nach § 15 Absatz 3 TMG berührt in gleicher Weise das Recht auf informationelle Selbstbestimmung der betroffenen Kunden. Daher erscheint es zur Schaffung eines medienunabhängigen hohen Datenschutzniveaus im Sinne eines Gleichlaufs mit der beabsichtigten Änderung von § 28 Absatz 3 BDSG geboten, auch die Erstellung von Nutzungsprofilen nach dem Telemediengesetz von der Einwilligung des Dienstenutzers abhängig zu machen.

**Zu Buchstabe b**

Der Bundesrat anerkennt das grundsätzliche Bedürfnis nach einer ausdrücklichen Befugnis für Telemedienanbieter, zur Eingrenzung und Beseitigung von Störungen Nutzungsdaten zu verwenden. Mit Blick auf die verfassungsrechtlichen Anforderungen aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG (Grundrecht auf informationelle Selbstbestimmung) ist die Ermächtigungsgrundlage jedoch zu konkretisieren und durch eine eindeutige Zweckbindung zu flankieren.

Telemedienanbieter und deren Nutzer sind angesichts der aktuellen Bedrohung durch Angriffe auf Webanwendungen vergleichbar schwerwiegenden Eingriffen ausgesetzt wie Anbieter von Telekommunikationsdienstleistungen; für diese sieht § 100 Absatz 1 des Telekommunikationsgesetzes (TKG) eine entsprechende Regelung vor. Für eine strukturelle Angleichung der beiden Regelungsregimes in diesem Punkt spricht insbesondere, dass trotz § 1 Absatz 1 TMG eine trennscharfe Unterscheidung zwischen technischer Übertragungsleistung und Übertragungsdienst in der Praxis kaum möglich ist. Internetprovider bieten ihren Kunden häufig integrierte Leistungspakete an, die sowohl Elemente von Telekommunikation, Telemedien und vielfach auch Inhaltsleistungen haben. Für Telemedien, die überwiegend in der Übertragung von Signalen über die Telekommunikationsnetze bestehen (Access-Providing, E-Mail-Dienste), ordnet § 11 Absatz 3 TMG dementsprechend an, dass nur bestimmte datenschutzrechtliche Normen des Telemediengesetzes Anwendung finden; im Übrigen gelten die entsprechenden Bestimmungen des Telekommunikationsgesetzes.

Die bisherigen Befugnisse der Telemedienanbieter zur Erhebung und Verwendung von Nutzungsdaten reichen zur Schließung der Schutzlücken nicht aus; insbesondere scheidet ein Rückgriff auf § 15 Absatz 1 TMG aus (vgl. AG Berlin-Mitte, Urteil vom 27. März 2007 – 5 C 314/06, RDV 2007, 257). Eine Einwilligung zur Datenspeicherung nach § 12 Absatz 1 Variante 2 TMG kommt bei den in Rede stehenden Sachverhalten regelmäßig nicht in Betracht.

Die Verwendung personenbezogener Nutzungsdaten durch den Diensteanbieter berührt den Gewährleistungsgehalt des Grundrechts auf informationelle Selbstbestimmung, das die Befugnis des Einzelnen umfasst, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen (vgl. BVerfG, Urteil vom 15. Dezember 1983, 1 BvR 209/83 u. a., BVerfGE 65, 1 – „Volkszählungsurteil“). Dieses Recht entfaltet als Norm des objektiven Rechts seinen Rechtsgehalt auch im Verhältnis von Privaten zueinander. Grundsätzlich obliegt es zwar dem Einzelnen selbst, seine Kommunikationsbeziehungen zu gestalten und in diesem Rahmen zu entscheiden, ob er bestimmte Informationen preisgibt oder zurückhält. Ist ihm allerdings ein informationeller Selbstschutz tatsächlich nicht möglich oder zumutbar, so besteht eine staatliche Verantwortung, die Voraussetzungen selbstbestimmter Kommunikationsteilhabe zu gewähr-

leisten (vgl. BVerfG, Beschluss vom 23. Oktober 2006 – 1 BvR 2027/02 –, DVBl 2007, 111).

Bei der Schaffung von Befugnissen für Telemedienanbieter zur Datenspeicherung hat der Gesetzgeber deshalb die sich aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG ergebenden Anforderungen zu beachten. Notwendig ist nicht nur ein verfassungsrechtlich anerkennenswertes Interesse an der Datenspeicherung, welches hier in der Wahrung der Funktionsfähigkeit der zur Bereitstellung von Telemediendiensten genutzten technischen Einrichtungen liegt. 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. März 2008 – 1 BvR 2074/05 u. a., MMR 2008, 308). Darüber hinaus sind eine konkrete Zweckbindung bei der Datenverwertung sowie verfahrensrechtliche Schutzvorkehrungen, die einen effektiven Schutz des Grundrechts gewährleisten, vorzusehen. Die oben genannte Fassung von § 15 Absatz 9 TMG trägt diesen Erfordernissen Rechnung. Satz 1 Halbsatz 1 verdeutlicht den Einzelfall- und Anlassbezug der weiteren Datenverwendung, um Auslegungsschwierigkeiten bei der Normanwendung vorzubeugen. Dies erscheint insbesondere deshalb veranlasst, weil die zu § 100 Absatz 1 TKG ergangene Rechtsprechung in verfassungsrechtlich bedenklicher Weise die vorbeugende Speicherung von IP-Adressen zur Störungseingrenzung und -beseitigung zulässt, ohne dass tatsächliche Anhaltspunkte bei einem bestimmten Nutzer vorliegen (vgl. LG Darmstadt, Urteil vom 6. Juni 2007 – 10 O 562/03, CR 2007, 574). Satz 1 Halbsatz 2 sichert die Zweckbindung bei der Datenverwertung.

Die Einschränkung „nur“ in Satz 1 stellt klar, dass der Verwendungszweck sich auf die Eingrenzung und Beseitigung der Störung beschränkt. Das Wort „Erkennen“ ist zu streichen, denn mit der Dokumentationspflicht und der Begrifflichkeit „tatsächliche Anhaltspunkte“ ist bereits sichergestellt, dass nur anlassbezogen und nicht verdachtsunabhängig personenbezogene Daten erhoben, gespeichert und genutzt werden können. Die Anlassbezogenheit der Maßnahme ist insbesondere von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder herausgestellt worden (vgl. deren Entschließung vom 18. Februar 2009; Erhebung und Auswertung als Ultima Ratio).

Ferner ist klarzustellen, was unter „Verwendung“ zu verstehen ist. Im Sinne der Einheit der Rechtsordnung wird auf die in den Datenschutzgesetzen des Bundes und der Länder gleichlautenden Begriffe Erheben, Speichern und Verarbeiten abgehoben (vgl. § 3 BDSG).

Satz 2 trägt dem Umstand Rechnung, dass es aus technischen Gründen unvermeidbar sein kann, neben den Nutzungsdaten mutmaßlicher Störer auch diejenigen anderer Nutzer zu erfassen. Satz 4 ist § 15 Absatz 8 Satz 3 TMG nachgebildet.

**Zu Nummer 2**

§ 16 Absatz 2 Nummer 5 TMG ist zu ergänzen, damit Verstöße gegen § 15 Absatz 9 Satz 1 bis 3 TMG nicht sanktionslos bleiben.

6. **Zu Artikel 3** (§ 19 Absatz 9 TMG)

Der Bundesrat bittet, im weiteren Verlauf des Gesetzgebungsverfahrens zu prüfen, ob der Gesetzentwurf aufgrund der Regelung des Artikels 3 des Gesetzentwurfs der Kommission der Europäischen Gemeinschaften nach Artikel 8 der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 204 vom 21. Juli 1998, S. 37) in der Fassung der Richtlinie 2006/96/EG des Rates vom 20. November 2006 (ABl. L 363 vom 20. Dezember 2006, S. 81) zu übermitteln ist.

Begründung

Der Gesetzentwurf sieht derzeit vor, Diensteanbieter nach dem Telemediengesetz zu ermächtigen, Nutzungsdaten für Zwecke der Sicherheit ihrer technischen Einrichtungen zu erheben und zu verwenden. Diese Regelung könnte der oben genannten Notifizierungsrichtlinie 98/34/EG unterfallen. Nach Artikel 8 Absatz 1 Unterabsatz 1 dieser Richtlinie übermitteln die Mitgliedstaaten (vorbehaltlich des Artikels 10) der EU-Kommission unverzüglich jeden Entwurf einer technischen Vorschrift, sofern es sich nicht um eine vollständige Übertragung einer internationalen oder nationalen Norm handelt. Der Begriff des Entwurfs einer technischen Vorschrift ist in Artikel 1 Nummer 12 der Richtlinie legaldefiniert und meint den Wortlaut einer technischen Spezifikation oder einer sonstigen Vorschrift oder einer Vorschrift betreffend Dienste einschließlich Verwaltungsvorschriften, der ausgearbeitet worden ist, um diese als technische Vorschrift festzuschreiben oder letztlich festschreiben zu lassen, und der sich im Stadium der Ausarbeitung befindet, in dem noch wesentliche Änderungen möglich sind. Der Begriff der Vorschrift betreffend Dienste ist weit gefasst und betrifft insbesondere auch Regelungen über die Betreibung von Dienstleistungen der Informationsgesellschaft (vgl. Artikel 1 Nummer 5 in Verbindung mit Nummer 2 der Richtlinie).

## Gegenäußerung der Bundesregierung

**Vorbemerkung**

Der Regierungsentwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes ist dringend erforderlich, um den zunehmenden Gefahren für die Sicherheit in der Informationstechnik zu begegnen. Die Bundesregierung beobachtet eine stetige Zunahme von Angriffen sowohl auf die Verfügbarkeit von Kommunikationseinrichtungen als auch auf sensible Daten.

Das Bundesamt für Sicherheit in der Informationstechnik muss daher auch rechtlich in die Lage versetzt werden, an zentraler Stelle die Kommunikationsnetze der Bundesverwaltung insbesondere vor Schadprogrammen zu schützen. Hierzu ist es notwendig, den Datenverkehr der Bundesverwaltung zentral und automatisiert auf Schadprogramme zu untersuchen.

Für neuartige Angriffe auf die Sicherheit der Computer der Bürgerinnen und Bürger werden unter anderem manipulierte Internetseiten genutzt: Besucher dieser Seiten können sich durch den bloßen Aufruf dieser eigentlich harmlosen und vertrauenswürdigen Internetseite ihren Computer mit einem Virus oder anderen Schadprogramm infizieren (sog. Drive-by Infections).

Für die Anbieter von Telemediendiensten im Internet bedeutet dies, dass sich die zu verfolgenden IT-Sicherheitsziele im Internet verändert haben. Sie müssen ihre Systeme einerseits zum Selbstschutz gegen Manipulationen, Hacking oder Verfügbarkeitsangriffe schützen. Andererseits müssen sie heute ihre Systeme auch gegen Angriffe wappnen, die diese Systeme nur als Zwischenstation für Angriffe auf die Nutzer der Dienste missbrauchen und von außen zunächst gar nicht erkennbar sind.

Zur Erkennung und Abwehr dieser Angriffe gegen Internetseiten und andere Telemedien kann die Erhebung und kurzfristige Speicherung und Auswertung der Nutzungsdaten durch den jeweiligen Diensteanbieter erforderlich sein. Daher sind auch Telemedienanbieter auf eine klare gesetzliche Regelung angewiesen, die ihnen eine solche Datenverarbeitung ausdrücklich gestattet.

Dies vorausgeschickt, nimmt die Bundesregierung zu den Vorschlägen des Bundesrates wie folgt Stellung:

**Zu Nummer 1**

Zu Buchstabe a

Zu Doppelbuchstabe aa

Die Bundesregierung wird den Vorschlag prüfen.

Sie weist allerdings darauf hin, dass im Falle der Bereitstellung von Sicherheitsprodukten auch für die Länder eine verfassungsgemäße Lösung für die Finanzierung gefunden werden muss.

Zu Doppelbuchstabe bb

Die Bundesregierung stimmt dem Vorschlag nicht zu.

Die konkrete Ausgestaltung der Beschlüsse der Föderalismuskommission II sollte dem Umsetzungsgesetz oder -Staatsvertrag hierzu auf der dann geschaffenen verfassungsrechtlichen Grundlage vorbehalten bleiben. Dies ist verfahrenstechnisch vorzugswürdig, weil sich die im Vorschlag genannten Gremien mit der Bund-Länder-Zusammenarbeit befassen, die im Rahmen der Föderalismusreform II neu geordnet wird. Insoweit genügt es, wenn das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) die Möglichkeiten der Bund-Länder-Zusammenarbeit nicht einschränkt und somit die konkrete Ausgestaltung der von der Föderalismuskommission II gefassten Beschlüsse nicht vorab limitiert. Eine solche Einschränkung steht indes nicht zu befürchten, da § 3 Absatz 2 des BSI-Gesetzes eine Unterstützung auch der Länder ausdrücklich vorsieht.

Zu Buchstabe b

Zu Doppelbuchstabe aa

Die Bundesregierung wird den Vorschlag prüfen.

Sie weist allerdings darauf hin, dass Eigenentwicklungen schon aufgrund des Haushaltsgrundsatzes der Sparsamkeit nur dann als Mittel zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nr. 11 in Betracht kommen, wenn keine geeigneten Produkte am Markt verfügbar sind. Dies ist vor allem bei den sehr spezifischen Sicherheitsanforderungen der Bundesverwaltung, insbesondere in sensiblen Bereichen, häufig der Fall.

Zu Doppelbuchstabe bb

Die Bundesregierung stimmt dem Vorschlag nicht zu.

Die konkrete Ausgestaltung der Beschlüsse der Föderalismuskommission II sollte dem Umsetzungsgesetz oder -Staatsvertrag hierzu auf der dann geschaffenen verfassungsrechtlichen Grundlage vorbehalten bleiben.

Zu Buchstabe c

Die Bundesregierung stimmt dem Vorschlag nicht zu.

Die konkrete Ausgestaltung der Beschlüsse der Föderalismuskommission II sollte dem Umsetzungsgesetz oder -Staatsvertrag hierzu auf der dann geschaffenen verfassungsrechtlichen Grundlage vorbehalten bleiben.

§ 9 regelt zudem ausschließlich die Tätigkeit des Bundesamtes für Sicherheit in der Informationstechnik als Zertifizierungsstelle der Bundesverwaltung und unterscheidet sich diesbezüglich nicht von der bereits bestehenden Regelung des § 4 des BSI-Errichtungsgesetzes. Auch zukünftig ist nicht zu erwarten, dass der Arbeitskreis der Staatssekretäre für E-Government in Bund und Ländern in seinen Zuständigkeiten betroffen sein wird.

Bei Aufnahme des Punktes ist allerdings mit einer erheblichen Ausweitung des bürokratischen Aufwandes für das Zertifizierungsverfahren zu rechnen. Seitens der betroffenen Wirtschaftsunternehmen werden schon heute die angesichts der schnellen technischen Entwicklung zu langen Verfahrensdauern kritisiert. Diesem wird durch die weitgehende Auslagerung von Prüfaufgaben unter Aufsicht des BSI begegnet.

Für eine zügige Verfahrensabwicklung ist es auch in Anbetracht der wachsenden Zahl von Zertifizierungsverfahren unabdingbar, dass die Verantwortung allein beim BSI liegt. Lediglich aus überwiegend öffentlichen Interessen, insbesondere sicherheitspolitischen Belangen, kann das Bundesministerium des Innern der Erteilung eines Zertifikats widersprechen.

Die grundsätzliche Mitprüfung durch den Arbeitskreis der Staatssekretäre für E-Government in Bund und Ländern dürfte das Verfahren erheblich verzögern und im Ergebnis zu einem Abwandern der Industrie zu ausländischen Zertifizierungsstellen führen.

Zu Buchstabe d

Die Bundesregierung stimmt dem Vorschlag nicht zu.

Ungeachtet der Regelung des Artikels 80 Absatz 2 des Grundgesetzes dient die Angabe in der Ermächtigungsnorm, ob eine Verordnung mit oder ohne Zustimmung des Bundesrats zu erlassen ist, der Rechtsklarheit und hat sich in der Staatspraxis bewährt.

**Zu Nummer 2**

Die Bundesregierung hat die erbetene Prüfung vorgenommen.

Die Bundesregierung teilt nicht die Auffassung, dass es sich bei der automatisierten Auswertung nach Schadprogrammen um einen gravierenden Grundrechtseingriff handelt. Jedenfalls wird nach der Rechtsprechung des Bundesverfassungsgerichts die Eingriffsschwelle gar nicht erst überschritten, soweit die Daten unverzüglich ausgewertet und danach sofort und spurenlos wieder gelöscht werden (BVerfG v. 11. März 2008, 1BvR 2074/05, 1 BvR 1254/07), wie es der Gesetzentwurf in § 5 Absatz 1 Satz 2 vorsieht. Die Daten werden auch nicht anlasslos erhoben, sondern nur, um Gefahren für die Informationstechnik des Bundes abzuwehren.

Hinsichtlich der Kommunikationsinhalte kommt es lediglich dann zu einem Grundrechtseingriff, wenn der Verdacht besteht, dass der Datenverkehr ein Schadprogramm enthält und die entsprechenden Daten ausgesondert werden. Dieser Grundrechtseingriff ist allerdings verhältnismäßig. Insbesondere treffen die Absätze 2 bis 7 umfangreiche materielle und verfahrenssichernde Vorkehrungen, um mögliche Beeinträchtigungen des dann betroffenen Fernmeldegeheimnisses so gering wie möglich zu halten. Dabei ist zu berücksichtigen, dass – anders als z. B. bei der Telekommunikationsüberwachung – die Maßnahmen niemals darauf abzielen, Inhalte der Kommunikation zu erfassen. Vielmehr soll der Datenverkehr lediglich auf Schadprogramme untersucht werden.

Der Einsatz von vergleichbar arbeitenden Programmen zur Erkennung und Abwehr von Schadprogrammen (sog. Virenscanner) ist bei Diensteanbietern, Unternehmen und Privatpersonen sehr weit verbreitet. Auch in Behörden sind auf der Grundlage von Dienstvereinbarungen mit den Beschäftigten bereits entsprechende Programme im Einsatz. Ein Einschüchterungseffekt bei den Nutzern der Kommunikationstechnik als Folge des Einsatzes von Virenscannern konnte bislang nicht beobachtet werden.

**Zu Nummer 3**

Die Bundesregierung stimmt dem Vorschlag zu.

**Zu Nummer 4**

Die Bundesregierung wird den Vorschlag prüfen.

Sie ist allerdings der Ansicht, dass jedenfalls bei besonders schwerwiegenden Gefahren eine sofortige Warnung der Öffentlichkeit möglich bleiben muss, wenn ansonsten ein Zeitverlust zu befürchten ist, vgl. § 40 Absatz 3 des Lebensmittel- und Futtermittelgesetzbuchs.

**Zu Nummer 5**

Zu Nummer 1 Buchstabe a

Die Bundesregierung wird den Vorschlag prüfen.

Sie weist allerdings darauf hin, dass die bestehende Regelung des § 15 Absatz 3 Diensteanbietern die Möglichkeit bieten soll, die Geschäftsentwicklung zu beobachten und entsprechend im Hinblick auf Angebot und Nachfrage zu reagieren. Der Offlinehandel kann dies relativ einfach, beispielsweise über die Verfolgung von Warenumsätzen. Im Onlinebereich bedarf es hierfür der elektronischen Datenverarbeitung. Dabei ist auch eine Anonymisierung der Daten nicht möglich, da der Diensteanbieter bestimmte Bezugsgrößen benötigt, die er über die Nutzung von Pseudonymen erhält. Dem Datenschutzinteresse wird dadurch genügt, dass die Pseudonyme nicht mit den Daten des Nutzers zusammengeführt werden dürfen.

Zu Nummer 1 Buchstabe b und Nummer 2

Die Bundesregierung stimmt dem Vorschlag hinsichtlich einer Ergänzung der Bußgeldvorschrift in § 16 des Telemediengesetzes zu. Im Hinblick auf die Formulierung des § 15 Absatz 9 weist sie darauf hin, dass sich der Vorschlag im Gesetzentwurf der Bundesregierung am Wortlaut der Regelung in § 100 Absatz 1 des Telekommunikationsgesetzes orientiert. Die dortige Regelung ist verfassungsrechtlich nicht zu beanstanden. Der Telekommunikationsdatenschutz unterliegt grundsätzlich und mit Blick auf das EU-Recht (Richtlinie 2002/58/EG) engeren Vorgaben als der Telemediendatenschutz. Es ist weiterhin unbestritten, dass Telemedienanbieter im Hinblick auf den Schutz ihrer technischen Einrichtungen das gleiche Schutzbedürfnis haben wie Telekommunikationsanbieter, das TMG hier aber eine Lücke aufweist. Daher besteht hier kein Anlass, bei Telemedienanbietern wesentlich engere Anforderungen an die Voraussetzungen des Umgangs mit den personenbezogenen Daten der Nutzer zu stellen als dies bei Telekommunikationsanbietern der Fall ist.

Die Bundesregierung schließt sich jedoch dem Vorschlag an, die Regelung des § 15 Absatz 9 in die Bußgeldvorschrift aufzunehmen. Auch die TKG-Regelung enthält in § 149 Nummer 17 TKG eine entsprechende Bewehrung.

**Zu Nummer 6**

Die Bundesregierung hat die erbetene Prüfung vorgenommen.

Sie hat den Artikel 3 des Gesetzentwurfs am 14. Januar 2009 der Europäischen Kommission nach Artikel 8 der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 204, S. 37), zuletzt geändert durch die Richtlinie 2006/96/EG des Rates vom 20. November 2006 (ABl. L 363, S. 81), notifiziert.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln, Telefon (02 21) 97 66 83 40, Telefax (02 21) 97 66 83 44
ISSN 0722-8333