Innenausschuss

A-Drs. 16(4)570 D

Stellungnahme

zu dem Entwurf eines Gesetzes
zur Stärkung der Sicherheit in der Informationstechnik des Bundes,
BT-Drs. 16/11967

in Vorbereitung der öffentlichen Anhörung
des Innenausschusses des Deutschen Bundestages
am 11.5.2009

vorgelegt von

Dr. Ralf Poscher
Professor für Öffentliches Recht, Rechtssoziologie
und Rechtsphilosophie
an der Ruhr-Universität Bochum

im Mai 2009

Inhaltsverzeichnis

I. Die datenschutzrechtliche Dialektik der Sicherheitssysteme

Der Gesetzentwurf hat ein Anliegen, das in Zeiten, in denen gezielte Angriffe auf Rechnersysteme an der Tagesordnung und als Mittel der strategischen Kriegsführung im Gespräch sind, zu Recht die Aufmerksamkeit des Gesetzgebers findet. Die Stärkung der Sicherheit der Informationssysteme des Bundes dient nicht zuletzt auch dem Datenschutz in der Bundesverwaltung. Der sorgfältige Umgang mit personenbezogenen Daten in der Bundesverwaltung würde erheblich entwertet, wenn die Daten der Bürger zwar innerhalb der Bundesverwaltung sorgsam verwaltet würden, aber dem Zugriff unbefugter Dritter ungeschützt ausgesetzt wären.

Die weitgehende Gleichläufigkeit des Interesses an der Sicherheit in der Informationstechnik des Bundes und des Datenschutzes bedeutet jedoch nicht, dass zwischen Maßnahmen zur Gewährleistung der Sicherheit der Informationssysteme und dem Schutz personenbezogener Daten nicht auch ein Spannungsverhältnis auftreten kann. Von den Instrumenten zur Sicherung der Informationstechnik selbst können neue und eigenständige Gefahren für den Datenschutz ausgehen. Durch Instrumente zur Sicherung der Informationstechnik werden Zugriffsmöglichkeiten auf den Datenaustausch und Datensammlungen geschaffen, die eigene datenschutzrechtliche Risiken und Missbrauchsgefahren bergen. Die Sicherung der Informationssysteme muss dieses Spannungsverhältnis bereits bei der Entwicklung neuer Sicherungsinstrumente beachten. Dass die Sicherung der Informationstechnik auch dem Datenschutz dient, darf nicht dazu führen, dass die von den Sicherungstechniken ausgehenden Gefährdungen des Datenschutzes und deren Bewältigung nicht bereits bei der Entwicklung der Sicherheitsinstrumente ebenbürtig berücksichtigt werden. Auch unter verfassungsrechtlichen Gesichtspunkten ginge es etwa nicht an, bei der Entwicklung der Sicherheitstechnik einseitig nur die unmittelbaren Sicherheitszwecke im Blick zu haben. Bereits bei der gesetzlichen Implementation neuer Sicherheitsinstrumente ist der Datenschutz gegenüber nicht-intendierten Auswirkungen der Sicherheitstechnik mit einzubeziehen. So können – auch aus verfassungsrechtlichen Gründen – Innovationen der Sicherheitstechnik Innovationen im Bereich des Datenschutzes verlangen. Die Regelungen des Entwurfs eines Gesetzes zur Stärkung der Sicherheit in der

Informationstechnik des Bundes müssen der Dialektik ihres Gegenstands in verfassungsrechtlich ausreichendem Maße Rechnung tragen.

II. § 5 BSIG-Entwurf

Von besonderer datenschutzrechtlicher Relevanz sind die Regelungen des § 5 BSIG-Entwurf.

Nach dem Schutzkonzept des § 5 BSIG-Entwurf werden in großem Umfang personenbezogene Daten erhoben, indem die Protokolldateien bei Kommunikationen mit informationstechnischen Systemen des Bundes erhoben, ausgewertet (§ 5 Abs. 1 Nr. 1 BSIG-Entwurf) und im Verdachtsfall bis zu drei Monate gespeichert werden (§ 5 Abs. 2 Satz 1 BSIG-Entwurf). Ferner werden alle an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten ausgewertet (§ 5 Abs. 1 Nr. 2 BSIG-Entwurf). Diese Auswertung bezieht sich nicht nur auf Protokoll- und Verkehrsdaten, sondern auf alle Daten der Datenströme und damit auch auf alle Inhalte der Kommunikationen.

1. Vereinbarkeit mit dem Recht auf informationelle Selbstbestimmung?

Die mit dem Schutzsystem des § 5 BSIG-Entwurf verbundenen Datenerhebungen, Speicherungen und Auswertungen verletzen das Recht auf informationelle Selbstbestimmung, soweit sie in dieses Recht eingreifen, ohne die verfassungsrechtlich geforderten Schutzstandards einzuhalten.

Die Datenerhebungen, Speicherungen und Auswertungen nach § 5 BSIG-Entwurf greifen auch insoweit in das Recht auf informationelle Selbstbestimmung ein, wie sie automatisiert erfolgen. Im Unterschied zu herkömmlichen automatisierten Schutzverfahren wie Viren-Scannern sind die automatisierten Datenerhebungen, Speicherungen und Auswertungen nach § 5 Abs. 1 und 2 BSIG-Entwurf darauf angelegt, in einem gestuften Verfahren auch auf nicht-automatisierte Weise ausgewertet zu werden. Jedenfalls in den Fällen, in denen eine solche nicht-automatisierte Auswertung erfolgt, ist nicht erst die nicht-automatisierte Auswertung, sondern bereits die automatisierte Erhebung und Auswertung an dem Recht auf infor-

mationelle Selbstbestimmung zu messen und in die Beurteilung des Grundrechtseingriffs einzubeziehen. Für die automatische Kennzeichenerfassung stellt das Bundesverfassungsgericht für die Personen, deren Daten nicht automatisch gelöscht werden, sondern für die Behörden verfügbar gehalten werden, fest, dass „bereits die zur Speicherung und Auswertung vorgenommene Kennzeichenerfassung in das Recht auf informationelle Selbstbestimmung ein<greift>, weil durch sie Daten personenbezogen für die Behörden verfügbar gemacht werden, die eine Basis für mögliche weitere Maßnahmen bilden können."

> BVerfGE 120, 378/400f.

Die nicht-automatisierte Auswertung führt dazu, dass auch bereits die automatisierte Erhebung, Auswertung und Speicherung Eingriffscharakter erhält.

Für die Verhältnismäßigkeit der mit § 5 BSIG-Entwurf verbundenen Eingriffe ist zum einen die Intensität der Eingriffe von Bedeutung, zum anderen, ob das Gesetz ausreichende verfahrensrechtliche Sicherungen

> Vgl. BVerfGE 100, 313/383f.; BVerfG NJW 2008, S. 822/831, 834.

und hinreichende materielle Eingriffschwellen vorsieht.

> Vgl. BVerfGE 120, 378/402; 115, 320/346, 358; BVerfG, NJW 2008, S. 822/831; zu den materiellen Eingriffsschwellen i.E. R. Poscher, Eingriffsschwellen im Recht der inneren Sicherheit, in: Die Verwaltung 2008, S. 345-374 m.w.N.

Für die Bewertung der Eingriffsintensität von informationellen Eingriffen hat das Bundesverfassungsgericht verschiedene Kriterien entwickelt. Danach ist für das Gewicht des Grundrechtseingriffs die Persönlichkeitsrelevanz der Informationen, die durch die Maßnahme erfasst werden können, von maßgeblicher Bedeutung. Insoweit ist für § 5 BSIG-Entwurf von einer besonders hohen Persönlichkeitsrelevanz auszugehen, da über die Auswertung des elektronischen Datenverkehrs an den Schnittstellen der Kommunikationstechnik des Bundes grundsätzlich auch die gesamte private elektronische Kommunikation einschließlich des elektronischen Telefonverkehrs von Mitarbeitern der Bundesverwaltung und ihren Kommunikationspart-

nern erfasst werden kann. So werden Mitarbeiter des Bundes etwa auch ihre privaten elektronischen Postfächer von Dienstrechnern abrufen. Bereits durch den Abruf der elektronischen Postfächer werden auch alle privaten elektronischen Kommunikationen der Behördenmitarbeiter der Auswertung nach § 5 BSIG-Entwurf unterworfen. Davon, dass § 5 BSIG-Entwurf auch Daten von besonders hoher Persönlichkeitsrelevanz erfasst, geht das Gesetz selbst aus, wie sich in § 5 Abs. 6 Satz 2 ff. BSIG-Entwurf zeigt, der sogar Vorkehrungen dafür trifft, dass Daten aus dem Kernbereich privater Lebensgestaltung der nicht-automatisierten Auswertung unterliegen können.

Für das Gewicht des Grundrechtseingriffs ist nach dem Bundesverfassungsgericht ferner maßgeblich, ob die Betroffenen selbst Anlass für die Auswertung gegeben haben oder ob die Auswertung „praktisch jeden treffen kann“.

BVerfGE 120, 378/402.

Da die gesamte dienstliche und private elektronische Kommunikation von und mit Angehörigen der Bundesverwaltung betroffen ist und die Möglichkeit eines Schadprogrammverdachts nicht zuverlässig von den Kommunikationspartnern kontrolliert werden kann, können die u. U. sogar den Kernbereich privater Lebensgestaltung betreffenden Eingriffe praktisch jedermann treffen, der als Mitarbeiter der Bundesverwaltung oder mit einem solchen elektronisch kommuniziert. Auch insoweit ist das Eingriffsregime nach den Kriterien des Bundesverfassungsgerichts als besonders eingriffsintensiv einzustufen.

Die Intensität des Grundrechtseingriffs wird zudem noch dadurch erhöht, dass Erhebung, Speicherung und Auswertung für die Betroffenen heimlich erfolgt.

BVerfGE 120, 378/402 f.

Weiter fällt ins Gewicht, dass die Daten nach § 5 Abs. 4 und 5 BSIG-Entwurf auch in umfangreicher Weise zu Zwecken der Strafverfolgung und sonstigen polizeilichen und geheimdienstlichen Maßnahmen genutzt werden sollen, die in keinem Zusammenhang mit der Sicherung der Informationstechnik des Bundes stehen. Den Betroffenen drohen mithin auch über die Informationserhebungen hinausgehende Nachteile, wie sie das Bundesverfassungsgericht als

das Gewicht entsprechender Informationseingriffe erhöhend eingestuft hat.

BVerfGE 120, 378/403.

Schließlich hat das Gericht wiederholt betont, dass jenseits der Intensität des individuellen Grundrechtseingriffs wegen der gesellschaftlichen und demokratischen Relevanz besonders umfassender Überwachungssysteme auch der Umfang und das Ausmaß der Datenerhebung für das Gewicht der mit einer Regelung vorgesehenen Eingriffe in das Recht auf informationelle Selbstbestimmung besondere Bedeutung erlangt.

BVerfGE 100, 313/376, 392; 107, 299/320 f., 327; 109, 279/353; 113, 29/53; 113, 348/383; 115, 320/354; a.A. Richterin Haas in BVerfGE 115, 320/373 f.

§ 5 BSIG-Entwurf erfasst die gesamte dienstliche und private elektronische Kommunikation von und mit Bediensteten des Bundes, die über Schnittstellen der Kommunikationssysteme des Bundes erfolgt. Das von § 5 BSIG-Entwurf vorgesehene Eingriffsregime ist auch hinsichtlich seines Umfangs und Ausmaßes als besonders intensiv einzustufen.

Insgesamt sieht § 5 BSIG-Entwurf ein System von informationellen Eingriffen vor, das nach fast allen vom Bundesverfassungsgericht dafür entwickelten Kriterien als besonders eingriffsintensiv beurteilt werden muss. Es kann daher nur dann den verfassungsrechtlichen Verhältnismäßigkeitsanforderungen genügen, wenn es ausreichende Eingriffsschwellen und effektive verfahrensrechtliche Sicherungen bereithält, die der Intensität des Eingriffssystems entsprechen.

a) <u>Gestuftes Eingriffskonzept</u>

Grundrechtliche Sensibilität zeigt der Gesetzentwurf, indem er sich bemüht, durch ein gestuftes Konzept der Verdachts- und Auswertungsphasen nicht-automatisierte Datenverwertungen zu vermeiden. Hingewiesen sei etwa darauf, dass nach § 5 Abs. 2 S. 1 BSIG-Entwurf keinesfalls alle Protokolldaten gespeichert werden dürfen, sondern nur diejenigen, hinsichtlich derer bereits tatsächliche

Anhaltspunkte vorliegen, dass sie im Falle der Bestätigung eines Verdachts benötigt werden. Nur soweit ein konkreter Verdacht besteht dürfen Daten auch nicht automatisiert verwendet werden – zunächst nur zur Bestätigung oder Widerlegung des Verdachts (§ 5 Abs. 3 S. 1 BSIG-Entwurf) und nur im Falle der Bestätigung auch für darüber hinausgehende Zwecke (§ 5 Abs. 3 S. 1 BSIG-Entwurf). Durch das gestufte Konzept kann allerdings nicht vermieden werden, dass nicht-automatisierte Verwertungen von Daten erfolgen, die auch höchstpersönlichen Inhalt haben können.

b) Fehlende Anonymisierung oder Pseudonymisierung

Besonders durch die in § 5 Abs. 2 BSIG-Entwurf vorgesehene bis zu dreimonatige Speicherung aller mit einem Verdacht in Zusammenhang stehender Protokolldaten werden große Datenbestände über das Kommunikationsverhalten der in der Bundesverwaltung Beschäftigten und ihrer Kommunikationspartner angelegt. Einen Schutz dieses Datenbestandes vor Missbräuchen durch Anonymisierung oder Pseudonymisierung sieht der Gesetzentwurf jedoch nicht vor. Ohne einen solchen Schutz kann dieser sensible Datenbestand jedoch missbraucht werden, etwa um die Kommunikationsbeziehungen bestimmter Mitarbeiter oder Dritter mit Mitarbeitern der Bundesverwaltung zu kontrollieren. Anhand des ungeschützten Datenbestandes ließe sich etwa ermitteln, welcher Bundesbedienstete zu welchen Journalisten, politischen Vereinigungen, Bürgerinitiativen etc. dienstliche oder private Kontakte gepflegt hat. Angesichts der Sensibilität entsprechender Daten erscheint ein Schutz jedenfalls durch eine Pseudonymisierung geboten.

Den Sicherheitsinteressen muss eine Pseudonymisierung nicht entgegenstehen. Sie kann so eingerichtet werden, dass sie im Falle einer Verdachtsbestätigung, soweit dies zur Abwendung informationstechnischer Gefahren notwendig ist, wieder aufgehoben werden kann. Auch für diese Fälle ist aber – etwa durch einen passwortgestützten Behördenleitervorbehalt und eine Dokumentation der Aufhebung der Pseudonymisierung – sicherzustellen, dass ein Missbrauch, soweit als möglich ausgeschlossen bleibt und jedenfalls eindeutige rechtliche und politische Verantwortlichkeiten etabliert werden. Für eine solches Pseudonymisierungverfahren reicht ein Hinweis auf § 3a Bundesdatenschutzgesetz nicht aus, da es ein eingriffsspe-

zifisches Regelungskonzept erfordert, dass sich den allgemeinen Regeln nicht entnehmen lässt. Der Gesetzgeber, der über die Anlage großer sensibler Datenbestände erhebliche Missbrauchsgefahren schafft, muss selbst dafür Sorge tragen, dass die Datenbestände durch spezifische datenschutzrechtliche Regelungen gesichert sind.

c) Keine unabhängige Kontrolle der Auswertungen

Schon vor der Speicherung bietet bereits der Zugriff auf alle dienstlichen und privaten Kommunikationen an den Schnittstellen der Bundesverwaltung nach § 5 BSIG-Entwurf erhebliche Missbrauchsmöglichkeiten. So kann der umfassende Zugriff auf die Datenströme etwa dazu genutzt werden, sie auf Daten zu durchsuchen, die sich nur vordergründig auf Schadprogramme, in der Sache aber auf die Kommunikation bestimmter Bediensteter oder Dritter beziehen. Durch die Zugriffsmöglichkeit auf den Datenstrom ließen sich etwa die dienstlichen und privaten Kontakte von Mitarbeitern oder die Kontaktaufnahme bestimmter Dritter auslesen. Nach den jüngsten Erfahrungen mit den Datenschutzskandalen in den materiell oder auch nur formell privatisierten Teilen der Bundesverwaltung im Bereich der Telekommunikation und des Bahnverkehrs gehört nur wenig Fantasie dazu, sich das elektronische Pendant zur Spiegel- oder Cicero-Affäre vorzustellen.

Auch insoweit gilt, dass der Gesetzgeber, der entsprechende Gefahrenquellen für den Datenschutz und damit auch für den Rechtsstaat und die Demokratie schafft, gleichzeitig mit der Implementation entsprechender Instrumente auch datenschutzrechtliche Sicherungsmechanismen schaffen muss. Insoweit wäre etwa daran zu denken, dass das Gesetz Dokumentationspflichten für die verwendeten Überprüfungsalgorithmen und ihre effektive Kontrolle durch eine unabhängige Stelle wie den Bundesdatenschutzbeauftragten vorsieht.

d) Keine ausreichenden Verwertungsgrenzen für Zufallsfunde

Durch die umfassende Auswertung der Datenströme zu und von informationstechnischen Systemen des Bundes sind in der Phase der nicht-automatisierten Auswertung einzelner Kommunikation – etwa elektronischer Post oder elektronischer Dokumente – Zufallsfunde

unvermeidlich. Dokumente, die im Rahmen der nicht-automatisierten Auswertung geöffnet werden müssen, um sie auf Schadprogramme zu überprüfen, können für die Betroffenen belastende oder kompromittierende Informationen enthalten. Die Dokumente können etwa auf begangene oder geplante Straftaten hinweisen, die in keinem Zusammenhang mit dem Schadprogramm stehen, das sie aus der Perspektive der Kommunikationspartner zufällig transportieren. Es handelt sich um Zufallsfunde, wie sie auch im Rahmen anderer behördlicher Ermittlungen anfallen können. Anders als etwa die Strafprozessordnung in § 477 Abs. 2 S. 2 StPO oder das G10-Gesetz und anders als es in der Rechtsprechung als rechtsstaatliches Erfordernis anerkannt ist,

> BVerfGE 57/170, 200; BVerfG NStZ 1988, 32 f.;
> BGHSt 26/298, 303; 28/122, 127.

findet sich jedoch in § 5 BSIG-Entwurf keine ausreichende Beschränkung der Verwertung von Zufallsfunden.

Nach § 5 Abs. 4 Satz 1 BSIG-Entwurf wäre etwa auch ein Zufallsfund an die Strafverfolgungsbehörden zu übermitteln, der auf eine Verleumdung, einen Betrugsfall oder eine Urheberrechtsverletzung hinweist, die mittels Telekommunikation begangen wurden, ohne dass entprechende Fälle geringerer Kriminalität im Zusammenhang mit der Verwendung von Schadprogrammen stehen müssen. Dies ist umso bedenklicher, als das Überwachungsinstrument des § 5 BSIG-Entwurf – anders als eine gezielte Telekommunikationsüberwachung – den gesamten dienstlichen und privaten elektronischen Verkehr aller Mitarbeiter der Bundesverwaltung erfasst. Alle elektronischen Kommunikationen aller Mitarbeiter der Bundesverwaltung und ihrer Kommunikationspartner werden systematisch der Möglichkeit von Zufallsfunden ausgesetzt. § 5 BSIG-Entwurf wirkt – ohne dies zu intendieren oder vermeiden zu können – wie ein groß angelegtes System zur Produktion von Zufallsfunden, das in dieser Dimension bislang noch nichts Vergleichbares kennt. Soll ein solches System verhältnismäßig sein, so sind materielle Verwertungsschwellen für Zufallsfunde festzusetzen, die wegen des umfassenden Charakters der Auswertungen jedenfalls nicht unterhalb der Verwertungsgrenze für die individuelle Telekommunikationsüberwachung liegen sollten. Zu überlegen wäre zudem, ob hinsichtlich repressiver und präventiver Verwertungen zu differenzieren ist und besonders gefährdete Berufsgruppen – etwa Journalisten – besonders zu

schützen wären, wie dies § 108 Abs. 3 StPO bereits vorsieht. Die Übermittlungsbefugnis für „Straftaten von erheblicher Bedeutung“ genügt zudem ohne eine Konkretisierung durch Regelbeispiele nicht den verfassungsrechtlichen Bestimmtheitsanforderungen.

> BVerfGE 110, 33/65 ff.; 113, 348/379; vgl. bereits BVerfGE 103, 21/33 f.

e) Keine ausreichende demokratische Kontrolle

Umfassende heimliche Überwachungsinstrumente, bei denen die Kontrolle durch den individuellen Rechtsschutz zumindest sehr stark eingeschränkt ist, bedürfen der besonderen demokratischen Kontrolle. Dies gilt auch für das Überwachungsregime des § 5 BSIG-Entwurf. Es muss auch durch eine besondere demokratische Kontrolle sichergestellt werden, dass es nicht zu nicht-intendierten Effekten oder Missbrauch der technischen Überwachungsinstrumente kommt. Eine solche demokratische Kontrolle kann über verschiedene Wege erreicht werden. Berichte an parlamentarische Gremien und Gesetzesevaluationen gehören insoweit zu den klassischen Instrumenten. Dem informationstechnischen Umfeld des Gesetzes angemessener wäre aber u.U. ein § 100b Abs. 5 und 6 StPO entsprechendes Verfahren, durch das die Öffentlichkeit über das Internet besonders auch über die Anzahl der personenbezogenen Datenübermittlung an Polizeien, Staatsanwaltschaften und Geheimdienste und die Anzahl der Übermittlungen von Zufallsfunden informiert wird. Dies würde es der Öffentlichkeit erlauben, zu kontrollieren, ob die umfassende technische Überwachung der Kommunikation über informationstechnische Systeme der Bundesverwaltung zu nicht-intendierten Überwachungseffekten führt. Eine besondere demokratische Kontrolle kann dazu beitragen, die gesellschaftlichen und demokratischen Risiken des § 5 BSIG-Entwurf zu kompensieren und so zur Verhältnismäßigkeit der mit ihm verbundenen Eingriffe beitragen.

In seiner jetzigen Form wird § 5 BSIG-Entwurf den materiellen und verfahrensrechtlichen Anforderungen nicht gerecht, die das Recht auf informationelle Selbstbestimmung an besonders persönlichkeitsrelevante, heimliche, von den Betroffenen nicht veranlasste und flächendeckende Eingriffe stellt. Bereits das den Eingriff legitimierende Gesetz muss ausreichende Mechanismen des Datenschutzes

gewährleisten, die die datenschutzrechtlichen Risiken der Instrumente und ihre Eingriffswirkung ausreichend minimieren, kompensieren und kontrollierbar machen.

2. Vereinbarkeit mit dem Kernbereichsschutz (Art. 1 Abs. 1 GG)?

In § 5 Abs. 6 BSIG-Entwurf geht das Gesetz selbst davon aus, dass der Auswertungsmechanismus auch Daten aus dem Kernbereich der privaten Lebensgestaltung erfassen kann. Entsprechende Zufallsfunde besonders in privaten Kommunikationen der Mitarbeiter des Bundes sind leicht vorstellbar. Für Maßnahmen, die erkennbar auf den Kernbereich privater Lebensgestaltung zugreifen können, hat das Bundesverfassungsgericht ein zweistufiges Schutzkonzept gefordert, durch das zum einen die Erhebung von Kernbereichsdaten soweit als möglich vermieden und zum anderen, soweit diese Daten unvermeidlich anfallen, ein Ausschluss ihrer weiteren Verwertung sichergestellt wird.

> BVerfGE 109, 279 /320, 324, 328; 113, 348 /392;
> BVerfG, NJW 2008, 822 /834.

Durch ein effektives zweistufiges Schutzkonzept bringt der Staat die Achtung vor dem Kernbereich privater Lebensgestaltung zum Ausdruck, die die Menschenwürdegarantie von ihm fordert.

> I.E. dazu R. Poscher, Menschenwürde und Kernbereichsschutz, JZ 2009, S. 269-277 m.w.N.

Dabei sollte das Gesetz auch im Hinblick auf die Zukunftsoffenheit der Entwicklung der informationstechnischen Möglichkeiten den Anspruch nicht aufgeben, soweit dies technisch möglich ist oder werden sollte, bereits auf der ersten Stufe die Erhebung von Kernbereichsdaten zu vermeiden. Eine – wenn auch defizitäre –

> R. Poscher, Menschenwürde und Kernbereichsschutz,
> JZ 2009, S. 269/276 m.w.N.

entsprechend zukunftsoffene Regelung enthält etwa auch § 20k Abs. 7 S. 1und 2 BKAG, obwohl für die Online-Durchsuchung jedenfalls zurzeit noch ähnliche Probleme bei dem technischen Ausschluss bereits der Erhebung von Kernbereichsdaten bestehen. Auch § 5 BSIG-Entwurf sollte den gesetzlichen Anspruch für die Erhebungsphase nicht aufgeben.

Auf der Auswertungsebene setzt das Bundesverfassungsgericht besonders darauf, dass eine unabhängige Stelle über die Kernbereichsrelevanz von Daten und ihre Verwertung entscheidet.

BVerfGE 109, 279/333 f.

Damit soll sichergestellt werden, dass sich der Staat unvermeidbar erhobene Kernbereichsdaten nicht doch zu Nutze macht. Nach § 5 Abs. 6 S. 3 BSIG-Entwurf erfolgt die Kontrolle jedoch nicht durch eine unabhängige Stelle, sondern durch das Bundesministerium des Inneren, zu dessen Geschäftsbereich nicht nur die Aufgaben des Bundsamts für die Sicherheit in der Informationstechnik gehören, sondern auch die Aufgaben einer Reihe weiterer Behörden, die aus polizeilichen oder geheimdienstlichen Gründen ein Interesse an der Verwertung der Daten haben könnten. Aufgrund der Identität der Verwertungsinteressen zwischen Bundesamt und Bundesministerium kann das Bundesministerium keine unabhängige Stelle im Sinn eines effektiven Kernbereichsschutzes sein.

In seiner jetzigen Form verstößt § 5 Abs. 6 BSIG-Entwurf gegen die von Art. 1 Abs. 1 GG geforderte Achtung vor dem Kernbereich privater Lebensgestaltung.

3. Vereinbarkeit mit der Rechtsschutzgarantie?

Zur Wahrung des in Art. 19 Abs. 4 GG garantierten effektiven Rechtsschutzes des Betroffenen regelt § 5 Abs. 3 S. 4-6 BSIG-Entwurf die verfassungsrechtlich gebotene Benachrichtigung des Betroffenen über heimlich durchgeführte Auswertungen.

Zur Gebotenheit der Benachrichtigung selbst im Anwendungsbereich von Art. 10 Abs. 2 S. 1 GG s. BVerfGE 30, 1/21.

Da sich der Schutzzweck der Maßnahmen nach dem Gesetzentwurf nicht nur auf den Bestand und die Sicherung des Bundes oder eines Landes richtet, kommt eine Rechtfertigung des Ausschlusses des Rechtsschutzes nach Art. 10 Abs. 2 S. 2 i.V.m. Art. 19 Abs. 4 S. 3 GG nicht in Betracht. Gleichwohl ist die Rechtsschutzgarantie ausgestaltungsbedürftig und kann zum Schutz gewichtiger Rechtsgüter modifiziert und auch eingeschränkt werden.

BVerfGE 109, 279/366.

Bloße administrative Erleichterungen rechtfertigen hingegen einen Ausschluss der Benachrichtigung nicht.

BVerfGE 100, 313/398 f.

Der Ausschluss der Benachrichtigung bei unverhältnismäßigem Ermittlungsaufwand nach § 5 Abs. 3 S. 3 BSIG-Entwurf darf daher nicht so verstanden werden, dass jedweder Ermittlungsaufwand eine Benachrichtigung ausschließt.

Einschränkend ausgelegt werden muss auch die Ausnahme überwiegender schutzwürdiger Belange Dritter. So hat das Bundesverfassungsgericht etwa festgestellt, dass der bloße Legendenschutz eines verdeckten Ermittlers oder einer Vertrauensperson einen Ausschluss der Benachrichtigung nicht zu rechtfertigen vermag.

BVerfGE 109, 279/302 f.

Problematisch ist der Ausschluss der Benachrichtigung der betroffenen Person nach § 5 Abs. 3 S. 4 BSIG-Entwurf, „wenn die Person nur unerheblich betroffen wurde und anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat“, die auch dann greifen soll, wenn die Ermittlung mit verhältnismäßigem Aufwand möglich ist und keine Interessen Dritter entgegenstehen. Weder ist insoweit eine Kontrolle der Interessenvermutung durch eine unabhängige Stelle vorgesehen, noch wird sich die Erheblichkeit und die Interessenlage ohne rechtliches Gehör des Betroffenen zuverlässig beurteilen lassen. Es ist nicht ersichtlich, warum dem Betroffenen das Urteil über seine Interessenlage nicht selbst überlassen wird. Art. 19 Abs. 4 GG schützt gerade auch die Eigenverantwortung der Grundrechtsträger bei der Durchsetzung ihrer Rechte.

P. M. Huber, in: H. v. Mangoldt/F. Klein/C. Starck, Kommentar zum Grundgesetz, Band 1, 5. Auflage 2005, Art. 19 Rn. 344.

Diese Bedenken wiegen umso schwerer als § 5 Abs. 3 S. 4-6 BSIG-Entwurf anders als sonstige Eingriffsregelungen zu Art. 10 GG auch keinen Richtervorbehalt kennt. § 5 Abs. 3 S. 4 BSIG-Entwurf sollte gestrichen werden.

III. § 7 BSIG-Entwurf

Grundsätzlich sollte die Behörde verpflichtet werden, ihre Erkenntnisse nicht nur den Herstellern von betroffenen Produkten, sondern auch der Öffentlichkeit mitzuteilen, soweit dadurch nicht die Erfüllung der Sicherheitsaufgaben des Bundesamtes für Sicherheit in der Informationstechnik oder anderer Behörden nachteilig betroffen sind. Kommerzielle Interessen Dritter – etwa der Hersteller von betroffenen Produkten – sollten eine Benachrichtigung der Öffentlichkeit nicht ausschließen.

IV. § 15 Abs. 9 TMG-Entwurf

§ 15 Abs. 9 TMG-Entwurf sieht eine § 5 Abs. 2 BSIG-Entwurf vergleichbare Speicherungsbefugnis für Diensteanbieter hinsichtlich der Nutzungsdaten vor. Die Befugnis geht jedoch insoweit über § 5 Abs. 2 BSIG-Entwurf hinaus als sie für die Speicherung der Nutzungsdaten keine tatsächlichen Anhaltspunkte für einen Gefahrenzusammenhang verlangt und die Speicherung nicht befristet. Sie kann auch zu intensiveren Belastungen führen, wenn sich mit den Nutzungsdaten bestimmte Nutzer mit bestimmten Inhalten in Verbindung bringen lassen, was u.a. die – auch wirtschaftlich u.U. interessante – Ermittlung von Interessenprofilen erlaubt. Ferner bestehen gegenüber privaten Dienstanbietern nur geringere Aufsichtsmöglichkeiten, um einen Missbrauch der Befugnis auszuschließen.

§ 15 Abs. 9 TMG-Entwurf enthält aber trotz seiner niedrigeren Speicherungsschwellen und trotz des gesteigerten Missbrauchspotentials keinerlei gesetzliche Vorkehrungen, die den Missbrauch zumindest erschweren und rechtliche Verantwortlichkeiten etablieren. Schon systematisch leuchtet nicht ein, zum Schutz der nationalen Sicherheit nur verdachtsbedingte, befristete Speicherungen zuzulassen, zum Schutz privater Interessen aber keine entsprechenden Beschränkungen vorzusehen. Ferner müssten auch in § 15 TMG-Entwurf befugnisspezifische datenschutzrechtliche Sicherungen wie Anonymisierung, Pseudonymisierung, Dokumentationspflichten, Verantwortlichkeiten und unabhängige Kontrollen in die gesetzliche Regelung der Befugnisse integriert werden. Auch rechtspolitisch ist befremdlich, dass nach einer Welle von Datenschutzskandalen neue weitere Datensammlungsbefugnisse eingeführt werden, die nicht

einmal mit rudimentären datenschutzrechtlichen Sicherungen versehen, geschweige denn in eine umfassendere, den neuen Anforderungen angemessene datenschutzrechtliche Konzeption eingebettet sind.