

Berlin, im April 2009  
Stellungnahme Nr. 31/2009

abrufbar unter  
[www.anwaltverein.de](http://www.anwaltverein.de)

## **Stellungnahme des Deutschen Anwaltvereins**

**durch die Ausschüsse Gefahrenabwehrrecht  
und Informationsrecht**

**zum**

**Entwurf eines Gesetzes zur Stärkung der Sicherheit in der  
Informationstechnik des Bundes vom 14.01.2009  
Bundsrats-Drucksache: 62/09**

Mitglieder des Ausschusses Gefahrenabwehrrecht:

Rechtsanwältin Dr. Heide Sandkuhl, Potsdam (Vorsitzende)  
Rechtsanwalt Wilhelm Achelpöhler, Münster  
Rechtsanwalt Prof. Dr. Rainer Hamm, Frankfurt am Main  
Rechtsanwalt Sönke Hilbrans, Berlin  
Rechtsanwältin Kerstin Ötjen, Freiburg (Berichterstatterin)

Zuständige DAV-Geschäftsführerin:

Rechtsanwältin Bettina Bachmann

Mitglieder des Ausschusses Informationsrecht:

Rechtsanwalt Dr. Helmut Redeker, Bonn (Vorsitzender)  
Rechtsanwalt Niko Härting, Berlin  
Rechtsanwalt Prof. Dr. Rainer Hamm, Frankfurt am Main  
Rechtsanwalt Prof. Dr. Jochen Schneider, München  
Rechtsanwalt Prof. Dr. Holger Zuck, Stuttgart (Berichterstatter)

Zuständiger DAV-Geschäftsführer:

Rechtsanwalt Jens Wagener, Berlin

## Verteiler:

- Bundesministerium des Innern
- Bundesministerium der Justiz
  
- Bundesrat
- Deutscher Bundestag - Vorsitzender des Rechtsausschusses
- Deutscher Bundestag - Vorsitzender des Innenausschuss
- Deutscher Bundestag - Rechtsausschuss
- Deutscher Bundestag - Innenausschuss
- Deutscher Bundestag - Ausschuss für Wirtschaft und Technologie
- Deutscher Bundestag - Ausschuss für Kultur und Medien
- Deutscher Bundestag - Verteidigungsausschuss
  
- Arbeitsgruppen Inneres der im Deutschen Bundestag vertretenen Parteien
- Arbeitsgruppen Recht der im Deutschen Bundestag vertretenen Parteien
  
- Justizministerien der Länder
- Landesministerien und Senatsverwaltungen des Innern
- Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
- Landesdatenschutzbeauftragte
- Innenausschüsse der Landtage
- Rechtsausschüsse der Landtage
  
- Bundesrechtsanwaltskammer
- Bundesnotarkammer
  
- Deutscher Richterbund
- Bund Deutscher Verwaltungsrichter
- Humanistische Union
- GRUR
- BITKOM
- DGRI
- Bundesverband der Freien Berufe (BFB)
  
- Vorstand und Landesverbände des DAV
- Vorsitzende der Gesetzgebungs- und Geschäftsführenden Ausschüsse des DAV
  
- NJW
- NStZ
- StraFo
- DANA - Datenschutznachrichten

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit ca. 67.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

---

1. Mit dem Gesetz beabsichtigt das Bundesministerium des Innern, dem BSI (Bundesamt für Sicherheit in der Informationstechnik) Befugnisse einzuräumen, technische Vorgaben für die Sicherung der Informationstechnik in der Bundesverwaltung zu machen. Das BSI soll zentrale Meldestelle für die IT-Sicherheit sein und Informationen über Sicherheitslücken und neue Angriffsmuster sammeln, diese auswerten und dann Informationen oder Warnungen an die Betroffenen oder an die Öffentlichkeit weitergeben. Im Telekommunikationsbereich soll die Bundesnetzagentur in Absprache mit dem BSI und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit Kataloge für Sicherheitsanforderungen erstellen, welche Anbietern von Telekommunikationsleistungen und ggf. auch der Öffentlichkeit dabei behilflich sein sollen, das Fernmeldegeheimnis durch technische Maßnahmen zu schützen. Hierfür wird den Telekommunikationsdiensteanbietern die Befugnis eingeräumt, Nutzungsdaten zu erheben und zu verwenden.
2. Der Ansatz, die IT-Sicherheit zu erhöhen, ist zwar zu begrüßen. Er darf aber nicht zu Lasten des **Datenschutzes** gehen:
  - a) Zu weit geht die Ermächtigung des BSI, die gesamte Sprach- und Datenkommunikation aller Unternehmen und Bürger mit Bundesbehörden ohne Anonymisierung oder Pseudonymisierung abzuhören und auszuwerten (§ 5). Es fehlt an der Anlassbezogenheit der Überwachung, sodass mangels Verhältnismäßigkeit ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung (Art. 1 und 2 GG) vorliegt. Dies gilt um so mehr, als die vollständige Überwachung der falsche Ansatz zur Erhöhung der IT-Sicherheit ist. Weniger die Schadprogramme sind das eigentliche Problem, sondern die Sicherheitslücken in der eingesetzten IT-Infrastruktur und Software, welche Schadprogrammen das Eindringen erst ermöglichen.
  - b) Die in § 5 vorgesehenen Abwehrmaßnahmen bestehen in der Erhebung und automatisierten Auswertung von Protokolldaten und an Schnittstellen anfallenden Daten. In diesem Zusammenhang kommt es zwangsläufig auch zur Erhebung und Auswertung von personenbezogenen Daten.

Im Hinblick darauf stellt sich das Problem, dass personenbezogene Daten auch solche aus dem Kernbereich privater Lebensgestaltung sein können, welche dem absoluten Schutz des informationellen Selbstbestimmungsrechts aus Art. 1 und 2 GG unterliegen, und dem staatlichen Zugriff entzogen sind. In eindeutigen Fällen ordnet § 5 Abs. 6 Satz 2 und 3 – richtig – ein Verwendungsverbot und eine Löschungspflicht an. Nicht immer wird jedoch eindeutig sein, ob Daten zum Kernbereich privater Lebensgestaltung gehören oder nicht. Dann soll, wenn die Daten nicht in eigener Verantwortung gelöscht werden, nach § 5 Abs. 6 Satz 4 das Bundesministerium des Inneren über die Verwertbarkeit entscheiden. Wegen des hohen Verfassungsrangs des Schutzguts der informationellen Selbstbestimmung ist eine Selbstkontrolle durch die Verwaltung allerdings unzureichend, um einen effektiven Grundrechtsschutz der BürgerInnen zu gewährleisten. Zu fordern ist daher, dass in einer solchen Situation der Gewaltenteilungsgrundsatz konsequent umgesetzt wird und die Entscheidung über die Verwertbarkeit der Daten einem unabhängigen Richter anvertraut wird.

- c) Die im Entwurf vorgesehene Änderung des Telemediengesetzes eröffnet öffentlichen und privaten Telediensteanbietern die Möglichkeit, das Kommunikationsverhalten der Nutzer umfassend festzustellen und zu protokollieren. Dies wird nach aller Erfahrung insbesondere für Werbe- und Marketingzwecke genutzt werden, nicht jedoch primär zur Erfüllung des Schutzzwecks der Erhöhung der IT-Sicherheit. Wenn höhere IT-Sicherheit durch Gefährdungen des Datenschutzes erkaufte werden muss, ist jedoch schon der Ansatz der Bestimmung zu hinterfragen, denn die informationelle Selbstbestimmung ist ein höheres Schutzgut als die technische Unversehrtheit von IT-Infrastrukturen.
  - d) Zu fragen ist im Übrigen, weshalb der Bundesrechnungshof und das Bundespräsidialamt von den Überwachungsmaßnahmen ausgenommen werden, nicht jedoch der Bundesdatenschutzbeauftragte (§ 2). Mit der dem Bundesdatenschutzbeauftragten zugewiesenen Unabhängigkeit ist dies schwer zu vereinbaren.
3. Die Erhöhung der IT-Sicherheit darf sodann nicht um den Preis der anlasslosen und permanenten **Verletzung des Fernmeldegeheimnisses** erfolgen. Nach § 5 soll eine ständige verdachts- und anlasslose vollständige Überwachung von Verbindungsdaten und Inhalten erfolgen, die mit Bundesbehörden in Verbindung treten.

Unabhängig davon, ob die Mittel zur vollständigen Überwachung überhaupt tauglich sind, ist eine solche vollständige Überwachung jeglicher Kommunikation unter Sicherheitsaspekten nicht angezeigt (s. dazu oben 1. a) und damit im Hinblick auf die Grundrechte auf informationelle Selbstbestimmung und das Fernmeldegeheimnis nicht verfassungsmäßig. § 11 des Entwurfs berechtigt in Verbindung mit § 5 zu Eingriffen in das Fernmeldegeheimnis. Zwar ist nach § 5 die Verarbeitung der personenbezogenen Daten nur mit gewissen Einschränkungen zulässig. Eine wirksame Kontrolle der Einhaltung dieser Einschränkungen fehlt jedoch. Vorgesehen ist nur eine nachträgliche Kontrolle durch den Datenschutzbeauftragten. Eine ex-post-Kontrolle erscheint angesichts des Gewichts der Grundrechtsbeschränkungen der informationellen Selbstbestimmung und des Fernmeldegeheimnisses nicht ausreichend, um die Verfassungsmäßigkeit von § 11 des Entwurfs zu gewährleisten. Daher müsste in den Entwurf auch insoweit ein Richtervorbehalt ex ante aufgenommen werden, welcher zumindest das Konzept der Überwachungsmaßnahmen umfasst.

4. Der Ansatz, die IT-Sicherheit zu erhöhen, darf auch nicht zur **Vernachlässigung von Aufgaben des Bundes im Bereich der Gefahrenabwehr** führen. Als problematisch ist insoweit anzusehen, dass das BSI nicht verpflichtet sein soll, bekannte Sicherheitslücken und Schadprogramme zu veröffentlichen und damit gerade Unternehmen und Bürger vor Angriffen (Spionage und Sabotage) zu warnen (**§ 7**). Die Geheimhaltung von Sicherheitslücken kann nicht in das Ermessen des BSI gestellt werden. Es kann nicht sein, dass ein staatliches Organ Sicherheitslücken verschweigt und damit insbesondere die Wirtschaft einer zusätzlichen Gefährdung aussetzt.