

# Stellungnahme zur Dialogveranstaltung

## „Datenschutz und Datensicherheit im Internet“



Bundesinnenminister und Bundesbeauftragter für Informationstechnik laden Vertreter aus Gesellschaft, Wissenschaft und Wirtschaft ein, über das Thema Datenschutz und Datensicherheit im Internet zu diskutieren. Diese Stellungnahme stellt unsere Position dazu dar.

### Inhaltsverzeichnis

A. Vorbemerkung zu staatlicher Informationssammlung und Überwachung.....	1
B. Handlungsbedarf.....	4
C. Wie können Datenschutz und Datensicherheit im Internet verbessert werden?...6	
D. Welche Mittel können Provider und Diensteanbieter den Bürgern an die Hand geben, um ihre Daten und ihre IT besser zu schützen (Spamfilter, Virenschutz...)? .....	10
E. Können Datensicherheit, Datensparsamkeit, Zweckbindung und Transparenz beim Umgang mit personenbezogenen Daten technisch unterstützt werden?.....	11
F. Welche Rollen können einer Stiftung Datenschutz zukommen?.....	11
G. Wie können De-Mail und elektronischer Personalausweis als Angebote für besseren Selbstschutz eingesetzt werden?.....	12
H. Welche Rolle kann das BSI übernehmen, um die Datensicherheit im öffentlichen und nicht-öffentlichen Bereich zu fördern?.....	14

### A. Vorbemerkung zu staatlicher Informationssammlung und Überwachung

Im Bereich von Datenschutz und Datensicherheit kommt dem Staat eine **Vorbildfunktion** zu. Verletzt der Staat das informationelle Selbstbestimmungsrecht der Bürger durch ausufernde Informationssammlung und Überwachung, kann er von Bürgern und der Wirtschaft nicht glaubwürdig Anstrengungen für mehr Datenschutz und Datensicherheit verlangen. Im Übrigen gehen von der staatlichen Datenverarbeitung größere Gefahren aus als von der Datenverarbeitung durch Private, einerseits weil bei staatlichen Stellen verschiedenste Informationen über uns konzentriert sind, andererseits weil nur der Staat über Zwangsbefugnisse verfügt, die er

auf der Grundlage von Informationen einsetzen kann. Der falsche Verdacht staatlicher Stellen wirkt sich wegen der staatlichen Zwangsbefugnisse oftmals verheerend auf Betroffene aus, bis hin zu Freiheitsentzug, Verlust des Arbeitsplatzes oder Zerstörung der Familie.

Der Arbeitskreis Vorratsdatenspeicherung fordert gemeinsam mit vielen anderen Organisationen der Zivilgesellschaft „**Freiheit statt Angst**“:

### **1. Überwachung abbauen**

- Abschaffung der flächendeckenden Protokollierung der Kommunikation und unserer Standorte (Vorratsdatenspeicherung)
- Keine pauschale Registrierung aller Flugreisenden (PNR-Daten)
- Kein Informationsaustausch mit den USA und anderen Staaten ohne wirksamen Datenschutz
- Keine geheime Durchsuchung von Privatcomputern, weder online noch offline
- Keine pauschale Überwachung und Filterung von Internet-Kommunikation
- Keine Finanzierung der Entwicklung neuer Überwachungstechniken
- Abschaffung der flächendeckenden Erhebung biometrischer Daten, sowie von RFID-Ausweisdokumenten
- Abschaffung von Video-Überwachung und automatischer Verhaltenserkennungssysteme

### **2. Evaluierung der bestehenden Überwachungsbefugnisse**

Wir fordern eine unabhängige Überprüfung aller bestehenden Überwachungsbefugnisse im Hinblick auf ihre Wirksamkeit und schädliche Nebenwirkungen.

### **3. Moratorium für neue Überwachungsbefugnisse**

Nach der inneren Aufrüstung der letzten Jahre fordern wir einen sofortigen Stopp neuer Gesetzesvorhaben auf dem Gebiet der inneren Sicherheit, wenn sie mit weiteren Grundrechtseingriffen verbunden sind.

### **4. Gewährleistung der Meinungsfreiheit und des freien Meinungs- und Informationsaustauschs über das Internet**

- Verbot der Installation von Filtern in die Infrastruktur des Internet.
- Entfernung von Internet-Inhalten nur auf Anordnung unabhängiger und unparteiischer Richter.
- Einführung eines uneingeschränkten Zitierrechts für Multimedia-Inhalte, das heute unverzichtbar für die öffentliche Debatte in Demokratien ist.
- Schutz von Plattformen zur freien Meinungsäußerung im Internet (partizipatorische Websites, Foren, Kommentare in Blogs), die heute durch unzureichende Gesetze bedroht sind, welche Selbstzensur begünstigen (abschreckende Wirkung).

Die folgenden Vorschläge für eine **freiheitsfreundliche Innenpolitik** sind an anderer Stelle<sup>1</sup> näher ausgeführt:

1. Entwicklung einer **nationalen Kriminalpräventionsstrategie**
2. Programm zur **Stärkung des Sicherheitsbewusstseins** und zur sachlichen Information über Kriminalität in Deutschland
3. **Deutsche Grundrechteagentur**: Schaffung einer Deutschen Grundrechteagentur, die alle bestehenden Befugnisse und Programme der Sicherheitsbehörden systematisch und nach wissenschaftlichen Kriterien auf ihre Wirksamkeit, Kosten, schädlichen Nebenwirkungen, auf Alternativen und auf ihre Vereinbarkeit mit unseren Grundrechten untersucht (systematische Evaluierung). Auf dieser Grundlage sind sodann Grundrechtseingriffe aufzuheben, wo dies ohne Einbußen an Sicherheit – also ohne Einfluss auf die Kriminalitätsrate – möglich ist. Auf Maßnahmen, deren Effizienz so gering ist, dass die dadurch gebundenen Mittel an anderer Stelle mehr zu unserer Sicherheit beitragen können, ist ebenfalls zu verzichten.
4. **Gesetzes-TÜV**: Jeden Vorschlag für neue Sicherheitsgesetze ist schon im Referentenentwurfsstadium von der Deutschen Grundrechteagentur auf seine Vereinbarkeit mit unseren Grundrechten, auf seine Wirksamkeit, seine Kosten, seine schädlichen Nebenwirkungen und auf Alternativen zu begutachten („Gesetzes-TÜV“ nach dem Vorbild des Normenkontrollrats).
5. **Freiheitspaket**: Unnötige und exzessive Überwachungsgesetze der letzten Jahre sind mit einem „Freiheitspaket“ aufzuheben, darunter die Totalprotokollierung des Telekommunikationsverhaltens der gesamten Bevölkerung (Vorratsdatenspeicherung), die Übertragung von Polizeibefugnissen einschließlich Online-Durchsuchung auf das Bundeskriminalamt, die gemeinsame Datei aller Sicherheitsbehörden, die elektronische Speicherung biometrischer Körpermerkmale in Pass und Personalausweis, die Vernetzung der örtlichen Ausweisregister, die lebenslängliche Steuer-Identifikationsnummer, das elektronische Bankkontenverzeichnis, die verpflichtende elektronische Gesundheitskarte sowie die Überwachung von Wohnungen, Ärzten, Rechtsanwälten und anderer Vertrauenspersonen.
6. **Eingriffsmoratorium**: Ein Moratorium für weitere Eingriffe in unsere Rechte im Namen der Kriminalitätsbekämpfung ist erforderlich, insbesondere für Zugriffe der USA auf deutsche oder europäische Datenbanken, für die geplante Einführung einer elektronischen Flugreiseakte für jeden Fluggast und für das geplante Bundesmelderegister.
7. **Sicherheitsforschung**: Die Sicherheitsforschung aus Steuergeldern ist zu demokratisieren und an den Bedürfnissen und Rechten der Bürgerinnen und Bürger auszurichten.

---

<sup>1</sup> <http://www.daten-speicherung.de/index.php/sicherheit-in-freiheit-vorschlaege-aus-sicht-der-buergerrechte/>.

- 8. Entschädigung für Grundrechtsverletzungen des Gesetzgebers:** Das Bundesverfassungsgericht soll das Recht erhalten, den von einem verfassungswidrigen Gesetz in ihren Grundrechten verletzten Bürgerinnen und Bürgern (nicht nur den Beschwerdeführer/innen) eine angemessene Entschädigung zuzusprechen.
- 9. Stärkung der Verfassungskonformität:** Ein Drittel des Deutschen Bundestages oder zwei Fraktionen ist das Recht zu geben, ein Rechtsgutachten des Bundesverfassungsgerichts zur Verfassungskonformität eines Gesetzesvorhabens einzuholen. Der Bundespräsident soll darüber hinaus das Recht erhalten, bei verfassungsrechtlichen Zweifeln vor der Ausfertigung eines Gesetzes das Bundesverfassungsgericht anzurufen.
- 10. Verbandsklagerecht von Bürgerrechtsorganisationen:** Nach dem Vorbild anderer Verbandsklagerechte sollen Bürgerrechtsorganisationen die Möglichkeit erhalten, stellvertretend für die Allgemeinheit vor den Fachgerichten und dem Bundesverfassungsgericht gegen staatliche Grundrechtsverletzungen zu klagen.
- 11. Demokratisierung internationaler Verhandlungen:** Deutschland darf Beschlüssen und Verträgen auf europäischer und internationaler Ebene, die der Umsetzung oder Ratifizierung durch den Bundestag bedürfen, künftig nur nach vorheriger Genehmigung der Vertreter des Volkes im Bundestag zustimmen. Der Bundestag oder sein zuständiger Ausschuss sollten künftig zu jedem solcher Vorhaben eine Stellungnahme abgeben. An die Stellungnahme des Parlaments muss der deutsche Vertreter bei den Verhandlungen und bei der Abstimmung gebunden sein.

## B. Handlungsbedarf

**Die neuen Medien werden für das tägliche Leben immer wichtiger.** Immer mehr Aktivitäten finden in den Informations- und Kommunikationsnetzen statt. Dadurch bilden die neuen Medien eine immer wichtigere Säule für die Wirtschaft. „Wer sich langfristig Marktchancen und Innovationspotenziale sichern will, muss die Ängste und Befürchtungen der Verbraucher ernst nehmen“, mahnte der ehemalige Verbraucherschutzminister Seehofer.<sup>2</sup> Die erfolgreiche Entwicklung der Internetdienste hängt heute davon ab, dass die Nutzer darauf vertrauen können, dass ihre Privatsphäre gewahrt bleibt.<sup>3</sup> Dieser Zusammenhang ist durch verschiedene Umfragen ebenso erwiesen wie die Tatsache, dass viele Verbraucherinnen und Verbraucher derzeit aus Sorge um ihre Privatsphäre auf die Nutzung von Internetdiensten verzichten.<sup>4</sup>

---

2 Pressemitteilung vom 15.03.2006, <http://snipurl.com/novm>.

3 Erwägungsgrund 5 der RiL 2002/58/EG.

4 Vgl. nur Kommission, Umfrage „Your Views on Data Protection“, [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/lawreport/consultation/consultation-citizens\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/consultation/consultation-citizens_en.pdf), 8.

So hat eine repräsentative Umfrage<sup>5</sup> ergeben, dass 61% der deutschen Internet-Nutzer beim Online-Shopping **um ihre Internetsicherheit besorgt** sind. 45% der befragten Nutzer sagten, dass die Internetsicherheit ihr Einkaufsverhalten beeinflusst; weitere 10% kaufen derzeit überhaupt nicht im Internet ein. 78% der Internet-Nutzer gaben an, dass ihre Hauptsorge dem Diebstahl ihrer persönlichen Daten und dem Weiterverkauf ihrer Daten an Dritte gilt. 85% der Nutzer beklagten, dass die Anbieter nicht genug tun, um ihre Kunden im Internet zu schützen. Einer Umfrage aus dem Jahr 2007<sup>6</sup> zufolge befürchten 54% der Internetnutzer, dass ihre persönlichen Daten im Internet ungeschützt sind. 31% der Befragten haben schon häufiger auf eine Bestellung im Internet verzichtet, weil sie ihre Daten nicht preisgeben wollten.

**Die Veröffentlichung der Sucheingaben von 600.000 Menschen** durch das Internetunternehmen AOL im Jahr 2006 hat die Dringlichkeit eines verbesserten Datenschutzes im Internet erstmals in das öffentliche Bewusstsein gerückt. Den 20 Mio. Datensätzen ließen sich Namen, finanzielle Informationen, Krankheiten, Informationen über das Sexualleben, teilweise sogar ganze Lebensschicksale von Internetnutzern entnehmen.<sup>7</sup> Ein Missbrauch solcher Informationen durch Kriminelle liegt nahe (z.B. für Einbrüche, Erpressung, Identitätsdiebstahl, Kontakte Pädophiler zu Minderjährigen, Stalking). 57% der Internetnutzer sind „sehr besorgt“ darüber, dass viele Internetunternehmen ihr Nutzerverhalten in personenbeziehbarer Form protokollieren.<sup>8</sup>

**Im Jahr 2008 wurden dann mehrere Fälle bekannt**, in denen persönliche Daten von Internetnutzern offen gelegt und dem Risiko eines Missbrauchs ausgesetzt wurden. 18.000 Personen, die im Internet bei der Anzeigenblatt-Tochter WBV Wochenblatt des Axel Springer Verlages – zum Teil unter Chiffre – Inserate aufgegeben hatten, mussten ihre Privatanschrift, E-Mail-Adresse, Handynummer und Kontodaten im Internet wieder finden.<sup>9</sup> Das mit Diskretion werbende Erotikunternehmen Beate Uhse veröffentlichte die E-Mail-Adressen Tausender von Personen, die sich Erotikvideos im Internet angesehen hatten.<sup>10</sup> Aus einem Internet-Forum des ZDF-Kinderkanals konnten sich beliebige Personen Klarnamen, Adresse, Telefonnummer und Geburtsdatum aller 1.000 registrierten Kinder verschaffen.<sup>11</sup>

Wegen der vielen Fälle von Datenmissbrauch (Handel mit Bankdaten, Überwachung am Arbeitsplatz, Missbrauch von Telekommunikationsdaten) sind inzwischen **80% der Bundesbürger „sehr besorgt“** um die Sicherheit ihrer Daten vor unbefugtem Zugriff oder Missbrauch.<sup>12</sup> Eine deutliche Mehrheit der Bevölkerung fordert eine Stärkung des gesetzlichen Datenschutzes.<sup>13</sup>

5 Forrester Custom Consumer Research,

<http://www.bsa.org/germany/presse/newsreleases/upload/BSA-Forrester-Deutsch.ppt>.

6 Institut Allensbach, Sicher im Netz?, [http://www.ifd-allensbach.de/news/prd\\_0717.html](http://www.ifd-allensbach.de/news/prd_0717.html).

7 Breyer, <http://www.daten-speicherung.de/index.php/aol-skandal-erfordert-aenderungen-am-telemediengesetz-entwurf/>.

8 Icomp, Consumer Understanding, <http://snipurl.com/7sfrm>.

9 Spiegel 43/2008 vom 20.10.2008, Seite 70.

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

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

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

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

## C. Wie können Datenschutz und Datensicherheit im Internet verbessert werden?

### I. Nicht-legislative Instrumente

Die folgenden **nicht-legislativen Instrumente** können den Datenschutz im Internet und den Selbstdatenschutz verbessern:

#### 1. Information

- positiv: **Information über die Bedeutung des Datenschutzes** und über Möglichkeiten, ihn zu verbessern (z.B. Schulen, Freiheitsredner<sup>14</sup>)
- positiv: **Auszeichnung datensparsamer und datensicherer Angebote** (Gütesiegel)
- negativ: **vergleichende Bewertung des Datenschutzniveaus** („Stiftung Datentest“)

#### 2. Finanzielle Anreize

- positiv: **Subventionen und Steuervorteile** für datensparsame und datensichere Produkte und Dienstleistungen
- positiv: Finanzielle **Förderung der Forschung und Entwicklung** datensparsamer und datensicherer Angebote (privacy-enhanced technologies)
- positiv: **Finanzielle Förderung privater Initiativen** zur Information über die Bedeutung des Datenschutzes und über Möglichkeiten, ihn zu verbessern (z.B. Freiheitsredner<sup>15</sup>)
- positiv: **Der Bund beschafft für den Eigengebrauch** nur noch datensparsame und datensichere IT-Produkte.
- positiv: Verpflichtet der Staat Private zur Datensammlung, muss er sie **vollständig entschädigen**, damit die Finanzierung der erforderlichen Datensicherheitsvorkehrungen auch bei kleinen Unternehmen gewährleistet ist.
- negativ: Risiken von Datenschutzverstößen durch verbesserte Ausstattung und wirkliche Unabhängigkeit<sup>16</sup> der **Aufsichtsbehörden** erhöhen

#### 3. Vorbildrolle des Staates

**Der Staat muss die eigene Ansammlung von Informationen** und Verpflichtungen Privater zur Datensammlung (z.B. Vorratsdatenspeicherung) abbauen und selbst ein hohes Datenschutzniveau gewährleisten.

## II. Erhöhung des gesetzlichen Schutzniveaus

Der Gesetzgeber hat weitere Möglichkeiten, Datenschutz und Datensicherheit im Internet zu verbessern. Möglich ist erstens eine Verbesserung des gesetzlichen, materiellen Schutzniveaus. Den besten und einzig wirksamen Schutz vor Datendiebstahl und Datenmissbrauch im Internet stellt es dar, wenn **von vornherein möglichst wenige persönliche Daten erhoben und gespeichert** werden. Internetnutzer er-

14 <http://www.freiheitsredner.de>.

15 <http://www.freiheitsredner.de>.

16 <http://www.daten-speicherung.de/index.php/kein-unabhaengiger-datenschutz-in-deutschland-und-den-usa/>.

warten daher, dass sie im virtuellen Leben ebenso anonym und überwachungsfrei handeln können wie es im wirklichen Leben weitgehend noch der Fall ist. Unter anderem sind dazu die folgenden Gesetzesänderungen erforderlich:

1. **Abschaffung der Vorratsdatenspeicherung**, um wieder eine anonyme Internetnutzung ohne das Risiko von Nachteilen infolge von Datenmissbrauch, Falschverdächtigung oder Datenpannen zu ermöglichen
2. **Erstreckung des Fernmeldegeheimnisses auf die Nutzung von Internetangeboten**
3. **Weitergabe von Informationen über Internetnutzer an Behörden** nur unter den Voraussetzungen, die für das Abhören von Telefonen gelten
4. Schaffung von Rechtssicherheit durch Klarstellung, dass der gesetzliche **Datenschutz auch für Internet-Protocol-Adressen** gilt
5. **Verbot der Erstellung von Nutzerprofilen ohne Einwilligung des Nutzers** durch Änderung des Telemediengesetzes
6. Stärkung des Rechts auf anonyme Internetnutzung durch ein **wirksames Koppelungsverbot** im Telemediengesetz
7. **Schutz der Nutzer vor unangemessenen Datenverarbeitungs-Einwilligungsklauseln**, indem klargestellt wird, dass derartige Klauseln der gerichtlichen Kontrolle unterliegen
8. **Keine Surfprotokollierung**: Ablehnung des Vorschlags im Regierungsentwurf eines „Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes“, Internetanbietern die präventive, flächendeckende Aufzeichnung des Surfverhaltens zur „Störungserkennung“ zu gestatten; Aufhebung des § 5 BSI-Gesetz
9. **Maßnahmen zur Gewährleistung der Datensicherheit (§ 9 BDSG) müssen dem Stand der Technik entsprechen**: In den letzten Monaten sind immer wieder schwerwiegende Datenpannen mit Millionen von Betroffenen bekannt geworden, die hätten vermieden werden können, wenn die Verarbeitungssysteme auf dem Stand der Technik gewesen wären (z.B. durch Anwendung von Updates)

Für den Bereich des Telemedienrechts liegt bereits ein ausführliches **Forderungspapier** samt Formulierungsvorschlägen vor, das unter anderem vom Chaos Computer Club, der Deutschen Vereinigung für Datenschutz, dem FoeBuD, dem FifF, der Humanistischen Union, dem Netzwerk Neue Medien, dem Netzwerk recherche und dem Verbraucherzentrale Bundesverband unterstützt wird.<sup>17</sup>

---

<sup>17</sup> [http://www.daten-speicherung.de/data/Forderungen\\_Telemedienrecht\\_26-02-2009\\_publ.pdf](http://www.daten-speicherung.de/data/Forderungen_Telemedienrecht_26-02-2009_publ.pdf).

### III. Verbesserte Durchsetzung des bestehenden Schutzniveaus

Noch wichtiger als eine Erhöhung des gesetzlichen Datenschutzniveaus erscheint eine effektivere **Durchsetzung des bestehenden Datenschutzrechts**. Der Gesetzgeber kann die Durchsetzung des bestehenden Rechts wie folgt verbessern:

- 1. Klarstellung, dass Datenschutzbestimmungen auch dem Schutz eines fairen Wettbewerbs dienen.** Die Einhaltung des Datenschutzrechts ist wettbewerbsrelevant, weil sich hiergegen verstoßende Unternehmen im Wettbewerb mit datenschutzkonform arbeitenden Konkurrenten einen unlauteren Vorteil durch Rechtsbruch verschaffen. Bisher sind die Gerichte in Deutschland der Meinung, dass Datenschutzvorschriften nicht wettbewerbsschützend seien. Das Wettbewerbsrecht ist aber ein effizientes, unbürokratisches und erfolgreiches Rechtsdurchsetzungsinstrument, das auf den Bereich des Datenschutzes erstreckt werden sollte.
- 2. Klagebefugnis für Verbraucher- und Datenschutzverbände einführen.** Die Gerichte in Deutschland haben entschieden, dass Datenschutzvorschriften nicht Verbraucherschützend seien und Verbraucherverbände den Schutz von Verbraucherdaten nicht einklagen können. Die Verbandsklagebefugnis der Verbraucherverbände ist aber ein effizientes, unbürokratisches und erfolgreiches Rechtsdurchsetzungsinstrument, das durch Erweiterung des Unterlassungsklagengesetzes auf den Bereich des Datenschutzes erstreckt und auch Datenschutzverbänden an die Hand gegeben werden sollte. Bei von Einzelnen angestregten Prozessen wegen datenschutzwidriger Praktiken gibt es immer wieder Finanzierungsschwierigkeiten; außerdem wird das Urteil von der Gegenseite oftmals nur für den jeweiligen Kläger umgesetzt und nicht für alle Kunden.
- 3. Einführung einer Haftung kommerzieller Hersteller und Importeure für den Fall, dass unsichere informationstechnische Produkte zu Datenschutzverletzungen führen (Produkthaftung).** Im Softwarebereich wäre es sinnvoll, die Produkthaftung kommerzieller Hersteller informationstechnischer Produkte auf Vermögensschäden zu erstrecken, die dadurch entstehen, dass ein Produkt nicht wirksam (auf dem Stand der Technik) vor Computerattacken oder Datenverlust geschützt ist. Dann würden Softwarehersteller für die Folgen ihrer Sicherheitslücken („Bugs“) haften, die schon oft für Verluste persönlicher Daten und von Betriebsgeheimnissen gesorgt haben. Das Haftungsrecht ist ein sehr effektives Rechtsdurchsetzungsinstrument, wie sich etwa im Bereich der Arbeitssicherheit gezeigt hat. Es sollte auch für den Datenschutz nutzbar gemacht werden. Kommerziellen Herstellern ist die Haftung zumutbar, weil sie sich - wie in anderen Bereichen üblich - gegen das Haftungsrisiko versichern können. Die Versicherer werden über die Prämienhöhe Anreize für mehr Produktsicherheit in der Branche setzen.
- 4. Verschuldensunabhängige Haftung für Datenschutzverletzungen mit pauschaler Entschädigungssumme.** Die Datenverarbeiter sollten den von Datenpannen Betroffenen auch für immaterielle Schäden haften (z.B. Sorge um einen möglichen Missbrauch ihrer Daten infolge einer Datenpanne), und

zwar verschuldensunabhängig. Ein Regelwert für den immateriellen Schaden sollte festgelegt werden (z.B. 200 Euro pro Person). Entschädigungszahlungen wegen Datenpannen könnte der für die Verarbeitung Verantwortliche vom Hersteller ersetzt verlangen (siehe oben), wenn ein unsicheres Produkt für den Schaden verantwortlich ist. Durch die Einführung einer Haftung für Datenpannen samt pauschaler Entschädigungssummen wären große Datenverarbeiter gezwungen, sich gegen Datenschutzverletzungen zu versichern. Durch die Versicherungsprämie hätten sie ein eigenes finanzielles Interesse daran, die Schadenswahrscheinlichkeit zu senken. Auf dem Gebiet der Unfallversicherung hat ein solches System bereits zu einem drastischen Rückgang der Zahl der Arbeitsunfälle geführt.

- 5. Privacy by design: Kommerzielle informationstechnische Produkte und Dienste dürfen nicht so voreingestellt sein, dass der Verwender gegen deutsches Datenschutzrecht verstößt.** Kommerzielle Computerprodukte (z.B. Software) und Dienste (z.B. Tracker, Werbung) müssen mit einer sicheren und datensparsamen Grundeinstellung angeboten werden. Dies ist derzeit leider bei den vorherrschenden amerikanischen Produkten nicht der Fall, weil es in den USA bekanntlich im privaten Bereich keinerlei Datenschutzgarantien gibt. Kommerziellen Anbietern informationstechnischer Produkte und Dienste ist es zumutbar, Produkte und Dienste für den europäischen Markt mit datenschutzkonformen Voreinstellungen anzubieten. Es ist auch gesamtwirtschaftlich sinnvoller, wenn der Hersteller sein Produkt rechtskonform gestaltet als wenn sämtliche Abnehmer das Produkt erst rechtskonform einstellen oder sogar umprogrammieren müssen. Die Datenschutzbeauftragten sollten das Recht erhalten, Anforderungen an eine datenschutzkonforme Produktgestaltung zu definieren.
- 6. Information der Nutzer auch über die typische Dauer der Aufbewahrung ihrer Daten** (§ 4 Abs. 3 BDSG). Auf der Grundlage dieser Information können die Nutzer sich für datensparsame Anbieter entscheiden und das Risiko reduzieren, Opfer von Datenpannen und Datenmissbrauch zu werden.
- 7. Auskunftsanspruch über Datensicherheit:** Den Kunden eines Unternehmens könnte ein Auskunftsanspruch bezüglich der vorhandenen Sicherheitsmechanismen zum Schutz ihrer Daten eingeräumt werden. Stellen fachlich versierte Kunden auf diese Weise Sicherheitsmängel fest, können sie die Aufsichtsbehörden darauf aufmerksam machen.
- 8. Whistleblowing:** Mitarbeiter von Unternehmen und Behörden sind eine wichtige Informationsquelle, die sich nutzen lässt, indem man eine **Möglichkeit zur anonymen Erteilung von Hinweisen auf Sicherheitslücken** bereit stellt und die Betroffenen gesetzlich vor Nachteilen schützt. Eine starke Einbindung der Beschäftigten ist auch angesichts der Tatsache sinnvoll, dass ein Großteil der Schäden durch Computerkriminalität auf Mitarbeiter des geschädigten Unternehmens zurückzuführen ist.
- 9. Benachteiligungsverbot bei Gebrauchmachen von Datenschutzrechten:** In der Praxis werden unabdingbare Regelungen des Datenschutzrechts immer wieder dadurch unterlaufen, dass Unternehmen mit einer ordentlichen Kündigung reagieren, wenn Betroffene von ihren gesetzlich garantierten

Rechten Gebrauch machen. Zu diesen unabdingbaren Betroffenenrechten zählt insbesondere das Recht, Auskunft über die zur eigenen Person gespeicherten Daten verlangen zu dürfen sowie die Rechte auf Berichtigung, Löschung und Sperrung personenbezogener Daten. Es muss verboten werden, Menschen zu benachteiligen, nur weil sie von ihren gesetzlichen Datenschutzrechten Gebrauch machen.

**10. Zertifizierungspflicht:** Im Bereich wichtiger Informationssysteme oder anlassbezogen nach dem Auftreten von Datenschutzverstößen ist eine Zertifizierungspflicht denkbar, um sicherzustellen, dass die betroffenen Systeme nach dem Stand der Technik geschützt sind. Eine Zertifizierung könnte turnusmäßig wie im Bereich der Kfz-Überwachung (Hauptuntersuchung) gefordert werden.

## **D. Welche Mittel können Provider und Diensteanbieter den Bürgern an die Hand geben, um ihre Daten und ihre IT besser zu schützen (Spamfilter, Virenschutz...)?**

Die folgenden Angebote könnten Provider und Diensteanbieter ihren Kunden unterbreiten:

- 1. Datenschutzfreundliche Voreinstellungen** für Dienste und Software.
- 2. Datenschutzfreundliche Zusatzfunktionalitäten** (Plugins) für Standardsoftware.
- 3. Datenschutzfreundliche Bundlingangebote**, z.B.:
  - E-Mail-Anbieter könnten ein **Verschlüsselungspaket** für Standard-E-Mail-Software bereit stellen.
  - Internet-Zugangsanbieter könnten eine **Anonymisierungsoption** anbieten, bei welcher der gesamte Datenverkehr verschlüsselt über einen nicht auf Vorrat speichernden Anonymisierungsdienst geleitet wird.

Wichtig ist der Netzgemeinde, dass der Nutzer stets **über die Aktivierung von Schutzverfahren selbst entscheiden** kann (opt-in oder wenigstens opt-out) und ihm nichts aufgezwungen wird. Fortgeschrittene Internetnutzer können z.B. anstelle des vom Anbieter angebotenen Spam- oder Virenfilters andere Produkte auf ihrem eigenen Rechner einsetzen wollen. Die Verantwortung für den Schutz der eigenen Daten und IT ist bei dem Betroffenen am besten aufgehoben; es müssen allerdings die richtigen Anreize gesetzt werden.<sup>18</sup> Das Fernmeldegeheimnis ist in jedem Fall zu wahren, so dass sich Kommunikationsmittler nicht in Kommunikationsprozesse einschalten dürfen, auch nicht zum vermeintlichen Schutz der Nutzer.

---

<sup>18</sup> Näher Seite ff.

## **E. Können Datensicherheit, Datensparsamkeit, Zweckbindung und Transparenz beim Umgang mit personenbezogenen Daten technisch unterstützt werden?**

**Privacy by design:** Kommerzielle informationstechnische Produkte (z.B. Software) und Dienste (z.B. Tracker, Werbung) müssen so voreingestellt sein, dass der Verwender deutsches Datenschutzrecht wahrt. Kommerzielle Software muss die Anforderungen des Datenschutzrechts an Datensparsamkeit und Datensicherheit auf dem Stand der Technik erfüllen. Zur Umsetzung einer entsprechenden gesetzlichen Pflicht sind geeignete Verfahren erforderlich.<sup>19</sup>

**Privacy-enhanced technologies:** Datenschutzfreundliche und transparenzwahrende Techniken (privacy-enhanced technologies, PET) sollten erforscht und gefördert werden.

## **F. Welche Rollen können einer Stiftung Datenschutz zukommen?**

**Als Vorbedingung muss die Stiftung finanziell und organisatorisch unabhängig** von Unternehmen und Staat sein. Die Satzung der Stiftung Warentest kann nur bedingt als Vorbild verwendet werden, weil diese Stiftung – anders als die Stiftung Datenschutz – keine staatlichen Angebote testet. Die Stiftung sollte vom Deutschen Bundestag errichtet werden und nicht von der Exekutive. Die Stiftung Warentest verfügt derzeit über ein Stiftungskapital von 22 Mio. Euro; dies sollte auch für eine Stiftung Datentest machbar sein.

**Hauptaufgabe der Stiftung sollte der „Datentest“** (analog „Warentest“) sein. Die Stiftung sollte Produkte und Dienstleistungen einer Art vergleichen im Hinblick auf die Menge der erhobenen Daten und die Dauer ihrer Aufbewahrung, die Datenverwendung und -weitergabe (etwa ins Ausland oder zu Werbezwecken) und die Datensicherheit. Man sollte auch den öffentlichen Bereich nicht ausnehmen. Beispielsweise könnten die Datenschutzvorkehrungen bei verschiedenen Arbeitsagenturen verglichen werden. Verbraucher können heutzutage realistischerweise nicht überblicken, was einzelne Anbieter mit ihren Daten machen. Wenn es eine „Stiftung Datentest“ gäbe, könnten Verbraucher sich ausgehend von deren Urteil (z.B. „gut“ oder „unbefriedigend“) leicht für ein datenschutzfreundliches Produkt entscheiden. Hersteller würden schon präventiv für mehr Datenschutz sorgen, um eine Empfehlung zu erzielen und schlechte Publicity zu vermeiden.

Die Stiftung könnte daneben die Aufgabe erhalten, zivilgesellschaftliche Aktionen zur Verbesserung des Datenschutzes und auch die wissenschaftliche Überwachungsforschung **finanziell zu unterstützen** (z.B. Aufklärungsaktionen wie die 'Freiheitsredner'). Mittel hierfür gibt es bisher kaum.

---

<sup>19</sup> Näher Seite ff.

Nach dem Vorbild des Verbraucherzentrale-Bundesverbands könnte der Stiftung ferner die Aufgabe übertragen werden, gegen Datenschutzverletzungen zu klagen. Dies würde eine **Verbandsklagebefugnis** im Bereich von Verletzungen des Rechts auf informationelle Selbstbestimmung bedingen, die daneben auch Verbraucher- und Datenschutzvereinen verliehen werden sollte.

Der Koalitionsvertrag nennt als **weitere Aufgaben** der Stiftung die Bildung im Bereich des Datenschutzes zu stärken, den Selbstdatenschutz durch Aufklärung zu verbessern und ein Datenschutzaudit zu entwickeln. Da diese Aufgaben aber bereits von anderen Akteuren wahrgenommen werden (z.B. Seminarveranstalter, Datenschutzbeauftragte), sollte sich die Stiftung auf die Finanzierung und Koordinierung solcher Angebote beschränken und sich auf ihre Hauptaufgabe - den Datentest - konzentrieren.

## **G. Wie können De-Mail und elektronischer Personalausweis als Angebote für besseren Selbstdatenschutz eingesetzt werden?**

De-Mail und elektronischer Personalausweis können nicht für besseren Selbstdatenschutz eingesetzt werden. Umgekehrt kann von der Benutzung dieser Angebote nur **abgeraten** werden.

Was **De-Mail** angeht:

1. Aufgrund der Architektur von De-Mail fließen alle Daten und Kontakte auf die Person **rückführbar an einer zentralen Stelle** zusammen; die Verwendung mehrerer, nicht in Verbindung zu bringender Identitäten ist nicht möglich. Ein übergreifendes Konto für sämtliche Kontakte ermöglicht eine Verknüpfung ganz unterschiedlicher Dateien. Wo viele Informationen zusammenlaufen, droht viel Missbrauch, geschehen viele Pannen und kann viel überwacht werden.
2. Der nicht rückverfolgbare Versand von Nachrichten **ohne Absenderangabe**, wie ihn die Post ermöglicht, steht hier nicht zur Verfügung.
3. Stattdessen wird jeder Kontakt über die De-Mail-Adresse und jeder Zugriff auf das Postfach aufgezeichnet und identifizierbar **sechs Monate lang auf Vorrat** gespeichert (§ 113a TKG).
4. Die hinterlegten persönlichen Daten des Nutzers sind für eine **Vielzahl von Sicherheitsbehörden und Geheimdiensten** unter nichtigen Voraussetzungen anforderbar (§ 113 TKG), die Identität hinter einer De-Mail-Adresse ist für über 1.000 Personen und Stellen in einem Onlineverfahren abrufbar (§ 112 TKG).
5. Der De-Mail-Gesetzentwurf sieht sogar die **Identifikation gegenüber Privaten** vor – eine schwerwiegende Verletzung des Fernmeldegeheimnisses, die bislang undenkbar war.

6. De-Mail wird zurzeit wohl von der **Deutschen Telekom AG** betreut, die Daten ihrer Kunden zweckentfremdet und verloren hat wie wohl kein anderes deutsches TK-Unternehmen.
7. De-Mail gaukelt Vertraulichkeit vor, sorgt aber nicht für eine **Ende-zu-Ende-Verschlüsselung**. Dadurch können Diensteanbieter und Sicherheitsbehörden die Kommunikationsinhalte mitlesen, was weit hinter der Vertraulichkeit postalischer Kommunikation zurückbleibt. Erforderlich wäre stattdessen, alle staatlichen Stellen zu verpflichten, PGP-Schlüssel anzubieten.

De-Mail ist insgesamt das **Gegenteil von sicherer und vertraulicher Kommunikation**. Besonders falsch ist die Zielsetzung des Projekts, „die nicht-anonyme und sichere elektronische Kommunikation zum Normalfall“ machen zu wollen. Nur anonyme Kommunikation ist sicher vor missbräuchlicher Aufdeckung des Kontakts.

Was den **Elektronischen Personalausweis** angeht:

1. Es braucht wenig Fantasie, um vorherzusehen, dass die zunächst freiwilligen **Identifizierungsverfahren nach und nach obligatorisch werden** werden und die anonyme Nutzung von Angeboten unmöglich werden wird, sei es der Abruf von Verwaltungsinformationen oder der Einkauf im Internet. Im Internet wird eine Identifizierung mit Personalausweis viel öfters gefordert werden als im „wirklichen“ Leben; auf diese Weise verändert sich unsere Gesellschaft. Unter die Räder kommt dabei, dass es durchaus legitime Gründe geben kann, einem Versandhaus nicht seinen wirklichen Namen anzuvertrauen, etwa wenn die bestellte Ware eigene Krankheiten oder auch sexuelle Aktivitäten betrifft.
2. Wenn kostenlose Dienste zur Anmeldung **unnötig Namen und Adresse abfragen**, konnte man sich bisher dagegen schützen, indem man falsche Angaben machte. Verlangt der Anbieter künftig eine elektronische Identifizierung, wird dies nicht mehr möglich sein.
3. Bislang genügte es vollauf, seine Daten bei der Behörde in ein Formular einzutragen und vielleicht seinen Ausweis vorzuzeigen. Es ist nicht erforderlich, die Daten direkt, zeichengenau und womöglich noch mit der Ausweisnummer in den Behördencomputer einzulesen. Genau dies wird künftig der Fall sein und einen **übergreifenden Datenabgleich** ungleich leichter machen.
4. Wie sich im Fall von Bank- und Kreditkarten zeigt, ist es zudem nur eine Frage der Zeit, bis elektronische Personalausweise von Straftätern kopiert werden (**Identitätsdiebstahl**), um im Namen des Opfers im Internet Unheil anzurichten. In den USA führt derartiges regelmäßig zu falschen Verdächtigungen und Festnahmen. Die vermeintliche Sicherheit der Identifikation ist keine, wie schon die verbreitete Weitergabe von ec-Karten-PINs zeigt.
5. Das Projekt wird wohl bereits daran scheitern, dass zur Verwendung dieser Funktionen **Lesegeräte für jeden PC** erforderlich wären. Ähnliche Versuche beim Online-Banking und im „elektronischen Rechtsverkehr“ sind weitgehend gescheitert. Auch ein elektronischer Personalausweis wird hoffentlich schlichtweg nicht genutzt werden. In anderen Ländern sind vergleichbare Dokumente unbekannt und auch nicht erforderlich.

Einen **wirksamen Selbstdatenschutz** im Internet bieten etwa die folgenden Maßnahmen: Das Internet sollte man ausschließlich unter Verwendung von Anonymisierungsdiensten, die nicht auf Vorrat speichern, nutzen. Man sollte sich im Internet nur unter Fantasienamen bewegen. Überflüssige Fragen im Internet sollten nicht oder nicht richtig beantwortet werden. Wenn eine E-Mail-Adresse angegeben werden muss, sollte eine anonyme Wegwerfadresse verwendet werden. Angebote von US-amerikanischen Firmen und aus anderen Staaten ohne Datenschutz sollten vermieden werden. E-Mail-Konten sollten nur bei Anbietern unterhalten werden, die auf die Erhebung (korrekter) Personendaten des Nutzers verzichten und die E-Mail-Nutzung nicht auf Vorrat speichern.

Unternehmen und Behörden brauchen **kein staatliches Verfahren zur Authentifizierung** via Internet. Bei kostenpflichtigen Leistungen muss ohnehin nur die Zahlung sicher gestellt werden, nicht auch die Identität des Nutzers. Die Zahlung kann anonym über Vorkasse oder anonyme Online-Bezahldienste (z.B. Paysafecard, Ukash) erfolgen. Bei nachträglicher Zahlung kann mit Einwilligung des Kunden eine Bonitätsauskunft eingeholt werden.

Kommt es tatsächlich auf die Identität des Nutzers an, kann dieser **auf verschiedene Weise authentifiziert** werden: Durch Anforderung einer Unterschrift per Post oder Fax, durch Erhebung einer Bank- oder Kreditkartenverbindung, durch das PostIdent-Verfahren oder durch eine persönliche Registrierung unter Vorzeigen eines Ausweisdokuments. Auf diese Weise kann von dem Betroffenen auch eine E-Mail-Adresse erfragt werden, über die Behörden und Unternehmen mit dem Betroffenen kommunizieren können. Vertraulichkeit kann durch eine Ende-zu-Ende-Verschlüsselung (PGP) sichergestellt werden. Die Verfahren De-Mail und elektronischer Personalausweis sind aus den oben genannten Gründen abzulehnen. Die vorhandenen Verfahren haben sich im Wirtschaftsleben bewährt.

**Insgesamt sollten De-Mail und elektronischer Personalausweis wieder eingestellt** und die dadurch eingesparten Mittel für eine Verbesserung von Datenschutz und Datensicherheit eingesetzt werden.<sup>20</sup>

## **H. Welche Rolle kann das BSI übernehmen, um die Datensicherheit im öffentlichen und nicht-öffentlichen Bereich zu fördern?**

Zuallererst sollte das BSI von der verfassungswidrigen Befugnis zur globalen und pauschalen **Surfprotokollierung** nach § 5 BSI-Gesetz keinen Gebrauch machen.

Zur Stärkung der Datensicherheit ist **Information und Beratung** in grundsätzlichen und aktuellen Fragen der Datensicherheit sinnvoll. Ob allerdings das BSI neben Datenschutzbeauftragten und Stiftung Datentest hiermit beauftragt werden sollte, bedarf näherer Prüfung.

**Eingriffsbefugnisse des BSI für die Abwehr von IT-Gefahren**, wie sie im Koalitionsvertrag vorgesehen sind, sind strikt abzulehnen. Die Zuständigkeit der Länder für die Gefahrenabwehr hat sich bewährt. Eine Zentralisierung erhöht den Schaden

---

<sup>20</sup> Näher Seite ff.

von Machtmissbrauch und Pannen auf ein inakzeptables Maß, weil das Fehlverhalten einer Person oder Behörde Auswirkungen auf Bürger in der gesamten Bundesrepublik hätte. Gegebenenfalls können die Länder spezialisierte Stellen für die Abwehr informationstechnischer Gefahren einrichten. Für den Fall länderübergreifender Gefahren müssen die Länder eine praktikable Zuständigkeitsregelung finden. Das BSI darf allenfalls auf Anforderung der zuständigen Landespolizei beratend tätig werden.

16.01.2010

### **Arbeitskreis Vorratsdatenspeicherung**

Der Arbeitskreis Vorratsdatenspeicherung (AK Vorrat) ist ein deutschlandweiter Zusammenschluss von Datenschützern, Bürgerrechtlern und Internetnutzern, die sich gegen die ausufernde Überwachung im Allgemeinen und gegen die Vollprotokollierung der Telekommunikation und anderer Verhaltensdaten im Besonderen einsetzen.

Homepage und Kontakt: <http://www.vorratsdatenspeicherung.de>