blickpunkt bundestag

SPEZIAL

www.bundestag.de

Datenschutz im Informationszeitalter

Titelbild: Tom Collicott/Masterfile

Foto: Bill Frymire/Masterfile

Datenschutz im Informationszeitalter

Neue Herausf in einer verne

Jeder Mensch hinterlässt eine Datenspur – in den Rechnern von Behörden, Unternehmen oder privat als Internetnutzer und Telefonkunde. Seine Daten werden gespeichert, verändert, weitergegeben oder auch gelöscht. Damit dies im Sinne der Betroffenen geschieht, sollen diese ihre Daten schützen und kontrollieren können. Doch in einer zunehmend vernetzten und informatisierten Lebenswelt wird dies immer schwieriger. Das erfährt jeder beim täglichen Surfen im Internet – und auch die jüngsten Skandale um Datenmissbrauch und illegalen Handel zeigen, dass neue Herausforderungen vor Politik und Bürgern liegen.

Inhalt

orderungen
etzten Welt

Vom „großen Bruder“ zu den vielen „kleinen Schwestern“

Fragen des Datenschutzes drehten sich von Beginn an immer darum, wie Menschen mit Computern umgehen. Als die ersten Datenschutzregelungen Anfang der 70er-Jahre eingeführt wurden, ging es darum, wie staatliche Stellen die über Bürger in ihren Rechenzentren gespeicherten Daten behandelten. Zunehmend kommen Computeranwendungen nicht mehr auf eigenen Rechnern zum Einsatz, sondern auf Servern im Internet. Daten werden auf Computern gespeichert, von denen man oftmals gar nicht mehr weiß, wo sie eigentlich ihren physischen Ort haben. Heute sind nahezu alle Rechner vernetzt, die Daten fließen von einer Recheninsel zur nächsten, werden gespeichert, geändert, erweitert, weitergegeben, aggregiert und kumuliert.

Lange Zeit speicherten Behörden Daten über Bürger in einem eng begrenzten Rahmen für bestimmte Zwecke. Seit den Terroranschlägen vom 11. September 2001 werden diese Daten in zunehmendem Maße nicht nur zwischen nationalen, sondern auch internationalen Behörden ausgetauscht. Für den Datenschutz markiert der 11. September in vielerlei Hinsicht eine Zäsur: Zu den einschneidenden Neuerungen in der Folge der Anschläge gehört etwa die Einführung biometrischer Merkmale in den Passdokumenten, insbesondere die Erfassung der Fingerabdrücke in Reisepässen. Auch die engere Zusammenarbeit von Polizei und Geheimdiensten in einem gemeinsamen Lagezentrum im Kampf gegen den Terror wurde als historischer Einschnitt wahrgenommen. Hier, so Kritiker, werde das nach 1945 eingeführte und in verschiedenen Gesetzen geregelte Trennungsgebot zur Zusammenarbeit von Polizei und Geheimdiensten missachtet.

Das Wiederaufleben der Rasterfahndung sowie die Erfassung von Flugpassagierdaten und ihre Weitergabe an ausländische Behörden gehören ebenfalls zu den Neuerungen im Bemühen um mehr Sicherheit. Im grenzüberschreitenden Datenverkehr der Behörden haben Bürger nur noch wenige Möglichkeiten, die Verwendung ihrer Daten zu überprüfen. Weitgehend unbekannt ist, dass auch Unternehmen davon betroffen sind. So müssen vor dem Grenzübertritt von Waren Zollbehörden eine Risikoanalyse durchführen – unter anderem, um terroristische Anschläge zu verhindern. Dies führt aber dazu, dass Wettbewerber in den USA auf Daten aus Passagierfragebögen und Frachtdokumenten europäischer Lieferanten zugreifen können. Schließlich halten viele Bürger die Anfang 2008 in Kraft getretene Vorratsdatenspeicherung für so bedrohlich, dass sie sich zu Zehntausenden einem Klageverfahren anschlossen, in dem die verdachtsunabhängige sechsmonatige Speicherung der Telefon- und Internetverbindungsdaten durch das Bundesverfassungsgericht überprüft wird.

Die informationelle Selbstbestimmung, so sind sich Datenschützer und Bürgerrechtler einig, ist mit diesen und anderen seit den Terroranschlägen eingeführten Maßnahmen sukzessive beschnitten worden. Ein Mehr an Sicherheit wurde versprochen – im Tausch gegen die Einschränkung von Freiheitsrechten. Wie prekär die Balance zwischen Freiheit und Sicherheit in einem demokratischen Rechtsstaat ist, wusste schon Benjamin Franklin. Er postulierte vor über 200 Jahren: „Jene, die Freiheit aufgeben, um eine vorübergehende Sicherheit zu erwerben, verdienen weder Freiheit noch Sicherheit.“

CHRONIK Datenschutz

Foto: action press/Becker & Bredel

1970 **Das erste Datenschutzgesetz** weltweit wird vom Bundesland Hessen verabschiedet. Es schützt die elektronisch verarbeiteten Daten vor dem Zugriff Unbefugter.

1977 **Das Bundesdatenschutzgesetz** regelt den Schutz personenbezogener Daten. Die Novelle 1990 legt fest, dass staatliche Stellen diese nur auf Grundlage eines Gesetzes verwenden dürfen.

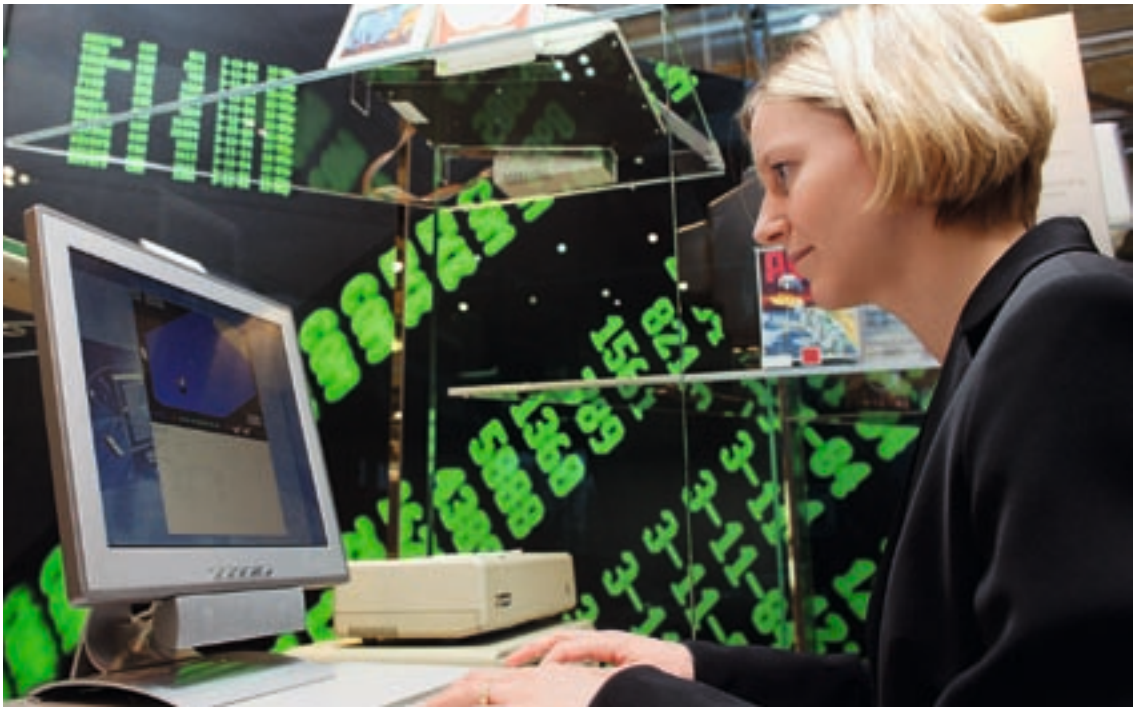
Foto: imago/suedraumfoto

Foto: Frank+Marc Darchinger GbR

1978 **Erster Bundesbeauftragter** für Datenschutz wird Hans Peter Bull (Bild links). Der Bundestag wählt den Datenschutzbeauftragten ab jetzt alle fünf Jahre.

1983 **Im Volkszählungsurteil** leitet das Bundesverfassungsgericht das „Recht auf informationelle Selbstbestimmung“ aus Art. 1 und 2 des Grundgesetzes ab.

Foto: PA/Carsten Rehder



Arbeitsplatz Computer: Der Mensch lebt heute im Netzwerk weltweiter Datenströme

Foto: epd/Werner Krüper

Aus diesem Grund versteht sich das Grundgesetz als Abwehr staatlicher Eingriffe in die Sphäre der Bürger.

Spuren im Internet

Es ist aber längst nicht mehr nur der Staat, der vieles über die Bürger weiß, sondern es sind zahlreiche Unternehmen: Telekommunikationsunternehmen, Internetbetreiber, Versicherungen, Handelskonzerne, Medienunternehmen und nicht zuletzt Suchmaschinenbetreiber. Jede Tasteneingabe kann aufgezeichnet und ausgewertet werden. Die Rede ist daher auch längst nicht mehr von der Gefahr, die von einem „großen Bruder" ausgeht, sondern wie es um die vielen „kleinen Schwestern" und den Nachbarn von nebenan bestellt ist.

Da es nur noch wenige Arbeitsplätze gibt, die nicht auf irgendeine Weise mit Kommunikations- und Informationstechnologien verbunden sind, gibt es nur noch wenige Arbeitnehmer, die nicht durch und in ihrer Arbeit neue Daten erzeugen. Arbeitnehmer in Callcentern können bekanntlich lückenlos überwacht werden, doch auch die Arbeit von Kassiererinnen kann von einer digitalen Kasse minutiös aufgezeichnet werden. Überprüfbar ist auch, welche Route etwa ein Versicherungsvertreter im Außendienst einschlägt, wie schnell er fährt, wie viele Pausen er macht.

Selbst private Tätigkeiten wie das Einkaufen, die ursprünglich allein nur etwas mit dem Austausch von Waren gegen Geld zu tun hatten, sind digitalisiert: Die Kasse registriert die Kontodaten der Bankkarte, mit der man

Foto: PA/Gero Breloer

1991 **Das Stasi-Unterlagen-Gesetz** erweitert das Recht zu wissen, wer welche Daten zur eigenen Person verarbeitet, auf die Bestände eines aufgelösten Geheimdienstes.

2001 **Infolge der Terroranschläge** vom 11.9.2001 greift der Staat mit umfangreichen „Sicherheitspaketen" massiv in die Privatsphäre ein, unter anderem durch die Erweiterung der Rasterfahndung.

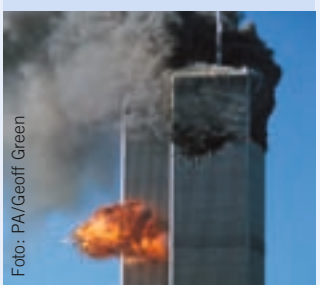


Foto: PA/Geoff Green

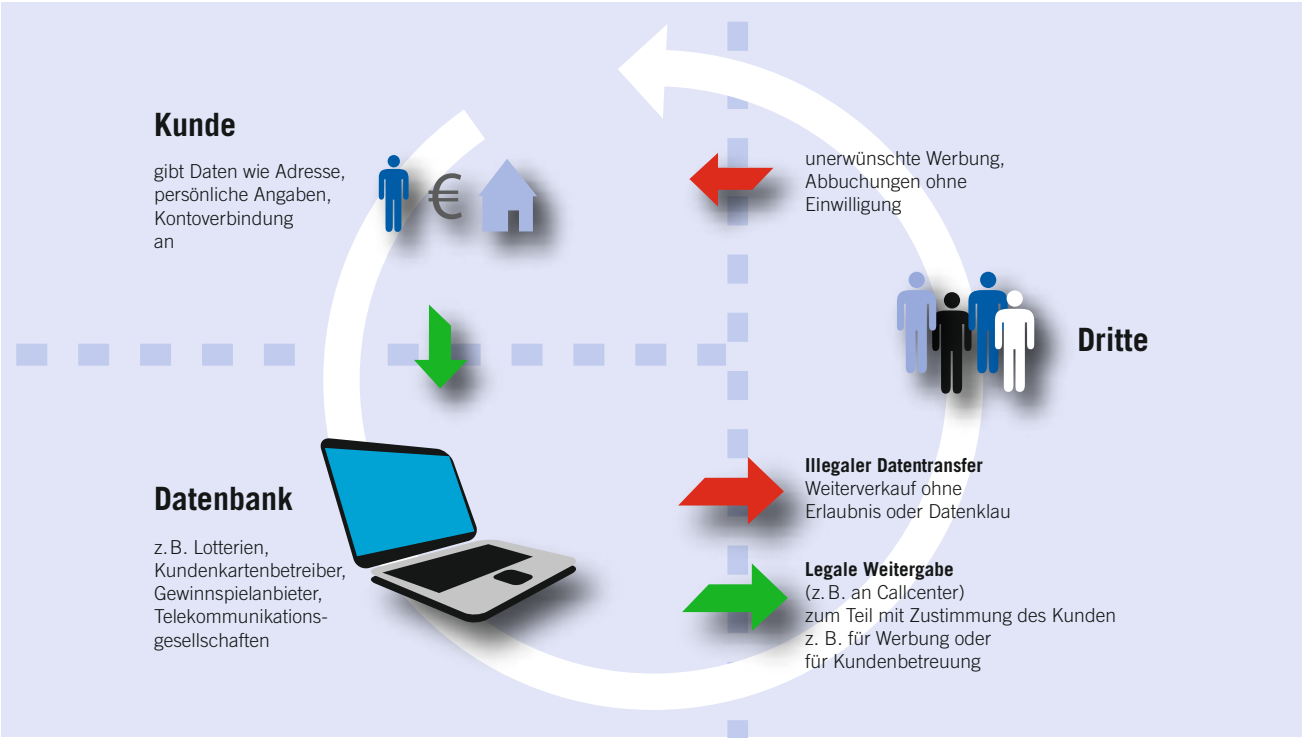
Foto: ullstein bild

2005 **Der biometrische Reisepass** wird eingeführt, in dem das Passfoto auf einem Chip gespeichert ist. 2010 wird voraussichtlich der elektronische Personalausweis folgen.

2008 **Das Bundesverfassungsgericht** kreiert im Urteil zu Online-Durchsuchungen das Grundrecht auf „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme".

Foto: PA/Uli Deck

Illegaler Datenhandel und Datenmissbrauch



Grafik: Marc Mendelson

bezahlt hat; über den RFID-Chip in der Ware lässt sich der gesamte Lebenszyklus eines Produkts nachvollziehen. Nicht zu reden von intelligenten Videoüberwachungssystemen, die jede körperliche Bewegung nach Verdachtsmomenten analysieren können.

Fraglich ist auch, wie man mit dem „Gedächtnis“ des Internets umgehen soll: Wie lange sollen Daten im Internet abrufbar sein? Wie lassen sich Persönlichkeitsrechte wirksam schützen? Eine US-Universität hatte einer Studentin die letzte Bestätigung verweigert, die sie zum Lehramt befähigt hätte. Grund war ein auf der Kontaktplattform MySpace veröffentlichtes Partyfoto, das sie als „betrunkenen Piraten“ zeigte. Daten können heute so gut wie nicht mehr aus dem Netz entfernt werden, da sie – einmal online – über verschiedene Dienste kopiert und archiviert werden. Außerdem lassen sich Informationen über eine Person aus Fototauschplattformen, Diskussionsforen, Bookmarks, Blogs und Kontaktplattformen zusammenführen. Damit können Persönlichkeitsprofile erstellt werden. Genutzt wird dies etwa von Personen-Suchmaschinen. Wer nicht im Internet gefunden werden kann, so scheint es, existiert nicht. Damit entsteht jedoch auch eine Elite medial Unsichtbarer, die über die notwendige Kompetenz und die Mittel verfügt, ihr Leben vor der Öffentlichkeit zu schützen.

Doch selbst wenn Menschen ihre Daten in dieser Weise „managen“ könnten, gäbe es noch immer viele Daten über sie, die sie nicht selbst verursacht haben und daher auch erst einmal nicht direkt kontrollieren können. Freunde und Bekannte können etwa Bilder von ihnen auf Fotoplattformen im Internet veröffentlichen und kommentieren, ohne dass sie darüber gleich erfahren. Kriminelle, Spaßvögel oder Stalker können sich illegal Kreditkartennummern besorgen, online Bestellungen für eine Person aufgeben oder sie in Foren verleumden.

Dass diese Daten auch aus umfangreichen Kundendatenbanken von Unternehmen stammen können, zeigten im Jahr 2008 gleich mehrere Fälle. Verbraucherschützern wurde eine CD mit persönlichen Daten von mehr als einer Million Bundesbürgern zugespielt. Genutzt wurde sie von Mitarbeitern in einem Callcenter. Personenbezogene Daten können auf vielfältige Weise in Umlauf geraten: Im Oktober wurde bekannt, dass 17 Millionen T-Mobile-Kundendaten bereits 2006 geklaut und im Internet in kriminellen Kreisen gehandelt wurden. Zu den gestohlenen Kundendaten zählen nicht nur Handynummern, Adressen, Geburtsdaten, sondern teilweise auch E-Mail-Adressen.

Welchen Standards muss der Datenschutz in Unternehmen genügen?

Angesichts der Dimensionen des Datenhandels und möglichen Datenmissbrauchs stellt sich nicht nur die Frage nach höheren Strafen gegen den illegalen Datenhandel, sondern auch nach präventiven Maßnahmen. Welchen Standards müssen Datenschutz- und IT-Sicherheitskonzepte in Unternehmen genügen? Wie können Verbraucher erfahren, ob diese Konzepte datenschutzkonform sind? Wie müssen Verfahrens- und Produktbewertungen (sogenannte Audits) gestaltet werden, die hierüber verlässlich Auskunft geben können?

Nicht nur im Umgang mit Kundendaten gilt es jedoch, das Vertrauen der Betroffenen wiederzugewinnen. Die in jüngster Zeit bekannt gewordenen Bespitzelungen von Arbeitnehmern beim Discounter Lidl und der Fast-Food-Kette Burger King, bei Novartis, Lufthansa oder der Deutschen Telekom zeigen, dass der Arbeitnehmer verstärkt als Risikofaktor, nicht aber als Partner wahrgenommen wird.

Recht auf Auskunft

Deutlich wird die zunehmend wichtige Rolle der betrieblichen Datenschutzbeauftragten. Diskutiert wird nun, ob sie nicht nur mehr Kompetenzen brauchen, sondern ob ihnen auch ein den Betriebsräten ähnlicher Schutz zukommen soll. Fraglich ist auch, ob die staatlichen Datenschutzbeauftragten rechtlich, personell und organisatorisch stärker als bisher dazu befähigt werden sollen, auch präventiv in privaten Unternehmen zu kontrollieren.

Weitere Konfliktfelder gibt es im Bereich der wirtschaftlichen Verfügbarkeit personenbezogener Daten. Eine Besonderheit hierbei sind Geodaten, die den Aufenthalt von Personen beziehungsweise Gegenständen oder den Standort von Wohnungen lokalisieren können. Mit dem Geo-Scoring können raumbezogene Daten so ausgewertet werden, dass etwa die Kreditwürdigkeit einzelner Straßenzüge, wenn nicht gar einzelner Gebäude ermittelt werden kann.

Theoretisch hat jeder das Recht auf Auskunft, Benachrichtigung, Einwilligung und Widerspruch, was die Verwendung seiner persönlichen Daten betrifft. Außerdem dürfen Daten nur für den Zweck verwendet werden, für den sie gespeichert wurden. Doch Datenschützer stellten schon vor Jahren fest, dass ihnen angesichts der Vielzahl und Alltäglichkeit der Datenbewegungen eine effektive Kontrolle nicht mehr möglich ist. Deshalb sollten Werkzeuge entwickelt werden, mit deren Hilfe die Menschen in der Lage wären, das Schicksal ihrer eigenen Daten selbst in die Hand zu nehmen, also ihre Datenspur zu kontrollieren. Erste sogenannte Identitätsmanagementsysteme wurden bereits für Internetdienste entwickelt, für die Menschen unterschiedliche Zugangsdaten und Profile verwenden. Auf diese Weise ist der Einzelne in der Lage zu bestimmen, was mit seinen Daten geschieht. Doch alltägliche Praxis sind solche Werkzeuge noch lange nicht.

Inzwischen gibt es mehrere wegweisende Urteile des Bundesverfassungsgerichts: Ein Grundrecht auf informationelle Selbstbestimmung wurde bereits 1983 aus dem Grundgesetz abgeleitet. Auch die Definition des „Kernbereichs privater Lebensgestaltung“ und eines „Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“ hat Karlsruhe vorgenommen. Angesichts des tief greifenden Wandels in allen gesellschaftlichen Bereichen beschäftigt sich die Politik mit der Frage, ob der Datenschutz und das Recht auf informationelle Selbstbestimmung nicht prominent im Grundgesetz verankert werden sollte. Hierzu hat die Fraktion Bündnis 90/Die Grünen einen Gesetzentwurf vorgelegt. Klar ist: Die umfassenden Herausforderungen der Informationsgesellschaft verlangen ein neues Verständnis des Datenschutzes – und eine Antwort. ■

Virtuelles Datenschutzbüro
Ein gemeinsamer Bürgerservice der Datenschutzinstitutionen:

www.datenschutz.de

Datenschutz

Die Prinzipien

In Deutschland hat jeder ein Recht auf Auskunft, Benachrichtigung, Einwilligung und Widerspruch, was die Verwendung seiner persönlichen Daten betrifft. Jeder, unabhängig von Alter, Wohnsitz und Nationalität, hat ein Recht zu erfahren, woher die Daten, die zu seiner Person gespeichert werden, stammen und an wen sie weitergegeben werden. Wollen Behörden und Unternehmen die Daten an andere Stellen übermitteln, müssen sie alle Betroffenen benachrichtigen. Personenbezogene Daten dürfen grundsätzlich nur dann erhoben, verarbeitet und genutzt werden, wenn dies gesetzlich ausdrücklich erlaubt ist oder wenn der Betroffene dazu freiwillig seine Einwilligung schriftlich erklärt hat. Dabei hat jeder das Recht, einer Nutzung oder Verarbeitung seiner freiwillig abgegebenen Daten zu widersprechen.

Grundlegend ist das Prinzip der Zweckbindung: Behörden und Unternehmen dürfen personenbezogene Daten nur zu den Zwecken verarbeiten, für die sie erhoben beziehungsweise gespeichert worden sind. Allerdings gibt es Ausnahmen: Eine nicht zweckgebundene Verarbeitung ist erlaubt, wenn eine Rechtsvorschrift eine andere Verarbeitung vorsieht, wenn der Betroffene eingewilligt hat oder es offensichtlich im Interesse des Betroffenen liegt. Wenn Daten allgemein zugänglich sind oder veröffentlicht werden dürfen, dürfen sie ebenfalls verwendet werden. Auch zur Verfolgung von Straftaten, für die Forschung oder wenn die Rechte anderer schwerwiegend bedroht sind, ist eine Verwendung erlaubt. Unternehmen dürfen bestimmte, gesetzlich eng umrissene Kundendaten außerdem für Zwecke der Werbung, der Markt- oder Meinungsforschung verarbeiten.

Navigationssystem im Automobil (rechts): Im modernen Verkehr entstehen eine Vielzahl persönlicher Daten. Supermarkt der Zukunft (Bild unten): Waren werden mit RFID-Technologie identifiziert

Entwicklungen im privaten Sektor

Daten über alle Lebensbereiche

Eine wachsende Armada nützlicher Geräte erzeugt persönliche Daten – angefangen von Navigationssystemen in Autos über Ortsdaten in mobilen Geräten wie Handys bis hin zu Gegenständen, die mit RFID-Chips versehen sind. Das soll dem Anwender nützen. Doch dabei entwickelt sich auch ein schwer überschaubares Panoptikum der Datennutzung.

Wie sehr jeder Einzelne bereits in den Fokus privater Unternehmen gerückt ist, wurde etwa deutlich, als eine US-Zeitschrift an ihre Abonnenten eine Ausgabe mit einem personalisierten Titelblatt verschickte. Es zeigte die Luftaufnahme des eigenen Hauses – der Verlag hatte auf kommerzielle Satellitendaten zurückgegriffen. Mit den hochauflösenden Luftbildaufnahmen von Google Earth ist das inzwischen nicht nur betuchten Verlagen, sondern jedem möglich. Menschen erlauben – freiwillig und manchmal auch unfreiwillig – in öffentlich zugänglichen Fotodatenbanken Einblicke in ihr Privat- und Berufsleben. Dabei geben nicht allein die Bilder selbst Auskunft, wo man wohnt, was man gern isst oder welche Veranstaltungen man besucht. Die auf Fotoplattformen generierten Daten zeigen auch persönliche Beziehungen auf, also wer wen kennt. Inzwischen gibt es bereits Kameras, die nicht nur die Zeit, sondern auch den Ort der Aufnahme speichern.

Personenbezogene Daten sind in der Informationsgesellschaft ein wertvoller Rohstoff, für den sich nicht nur Behörden, sondern im Besonderen Unternehmen interessieren: Telekommunikations- und Internetverbindungsdaten geben Auskunft, wann, wo und wie oft Kontakte stattfinden. Waren- und Kassendaten lassen sich danach auswerten, wer welches Produkt wann, wo und wie oft kauft. Werden diese Daten nicht nur vereinzelt, sondern gruppenweise erhoben und analysiert, lassen sich Trends erkennen. Damit können Unternehmen und Behörden auf unerwünschte Entwicklungen rechtzeitig reagieren: Handelskonzerne können etwa Preisanpassungen für bestimmte Produkte und Kundengruppen für begrenzte Zeiträume vornehmen.

Foto: Caro/Oberhaeuser

Jedes vormals stumme Ding, das von Menschen für bestimmte Zwecke benutzt wird, kann Daten über seine Verwendung erzeugen und damit etwas über das Verhalten seiner Benutzer aussagen. Getrieben wird die Entwicklung von der Frage der perfekten Logistik, mit der sich inzwischen ganze Industriezweige beschäftigen: Welchen Weg nimmt ein ganz bestimmtes Teilchen im Laufe seines Lebensprozesses? Schon länger ist es keine große Herausforderung mehr, den Warenfluss einer mit

Foto: Jochen Tack

einem sogenannten RFID-Chip versehenen Rasierklinge lückenlos nachzuvollziehen – und – inklusive Diebstahlsicherung – zu kontrollieren.

RFID steht für „Radio Frequency Identification“. Die Chips enthalten einen sogenannten Miniaturtransponder, über den sie per Funk die auf ihnen gespeicherten Informationen wie Artikelnummern, Internetadressen, Produktherkunft und -beschaffenheit abgeben können. Die Verwendungsmöglichkeiten der RFID-Chips sind jedoch nahezu unbegrenzt. Die Funketiketten lassen sich auf Waren, auf Verpackungen oder auf Ausweisen anbringen, aber auch auf der Arbeitskleidung, um etwa Mitarbeiter jederzeit im Gebäude orten zu können.

Brisant wird es, wenn Handelsunternehmen die RFID-Daten mit dem Konsumverhalten der Nutzer verbinden und für Marketingzwecke auswerten. Häufig haben die Verbraucher der Verwendung sogar zugestimmt und ihre persönlichen Daten gegen Rabatte und Sonderaktionen eingetauscht – etwa beim Bezahlen mit Kundenkarten. Getestet wurde die Zusammenführung von RFID-Daten und Daten über das Verbraucherverhalten bereits – ohne Wissen der Kunden.

Die Organisation vieler Lebensbereiche basiert aber auch auf ortsbezogenen Daten. Digitale, sogenannte interaktive Telefonbücher können bereits nicht nur die Kontaktdaten, sondern auch die Präsenz- und Standortdaten speichern. Auf diese Weise erfährt man auf einen Blick, wie jemand wo am besten zu erreichen ist. Das Handy wird damit für jeden Teilnehmer zum Ortungsinstrument.

Mit entsprechender „Intelligenz“ ausgestattete Fahrzeuge erlauben ähnliche Anwendungen. So gibt es seit Kurzem ein Geschäftsmodell, das auf der Auswertung von Autofahrerdaten basiert. Es wertet die gefahrenen Kilometer, Straßen und Uhrzeiten aus und schließt so auf das Fahrverhalten. Wenig risikofreudige Autofahrer sollen mit niedrigeren Versicherungssätzen belohnt werden und nicht mehr die fahrerischen Fehlleistungen des statistischen Mittels mitfinanzieren. Entsprechende Versicherungspolicen sind bereits seit über einem Jahr auch auf dem deutschen Markt erhältlich.

Mit solchen maßgeschneiderten Diensten hält das Scoring Einzug in die Versicherungswirtschaft. Die Strategie, personenbezogene Daten für Preismodelle und -konditionen auszuwerten, ist aus dem Handel bekannt. So ermitteln Auskunfteien für jede Anschrift in Deutschland einen Wert, der sich aus den Kreditinformationen der Schufa, der Adresse, dem Alter und der Gebäudeeinschätzung ermittelt. Versicherungen und Handelsunternehmen nutzen solche Dienste, um danach ihre Risikoeinschätzung zu erstellen. Mit dem Autofahrer-Scoring wird nun auch das individuelle Verhalten bewertet.

Eigentlich sollten Bürger eigenständig über die Datenabgabe entscheiden dürfen. Doch zu zahlreichen Angeboten wie etwa den RFID-Fußballtickets bei der WM 2006 gibt es keine Alternative. Sie müssen die Bedingungen der Anbieter und Hersteller akzeptieren – oder verzichten. Rechtliche Lösungen stehen im Fall von RFID noch aus. ■

RFID-Studie
des Bundesamts für Sicherheit in der Informationstechnik:

www.bsi.bund.de/themen

Ein Bürger vor Dani Karavans Kunstwerk „Grundgesetz 49“ im Berliner Parlamentsviertel. Die Grundrechtsartikel formulieren fundamentale Schutzrechte.

Datenschutz als Grundrecht

Freie Entfaltung der Persönlichkeit

Ist Datenschutz ein Grundrecht? Europaweit genießt der Datenschutz Grundrechtsstatus, doch eine entsprechende Formulierung fehlt bislang im Grundgesetz. In vielen Verfassungen der Bundesländer ist das Recht auf den Schutz der personenbezogenen Daten allerdings verankert. Die Väter und Mütter des Grundgesetzes haben den Datenschutz zwar nicht ausdrücklich als Grundrecht benannt – doch mehrere Urteile des Bundesverfassungsgerichts haben seinen Grundrechtsrang klar formuliert.

Mit dem Volkszählungsurteil gab das Bundesverfassungsgericht 1983 den Gegnern der Volkszählung recht und schrieb das „Recht auf informationelle Selbstbestimmung“ fest. Es wurde zur Basis des modernen Datenschutzrechts. Die Grundüberlegung des obersten Gerichts bestand darin, dass „eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung“ mit dem „Recht auf informationelle Selbstbestimmung“ nicht vereinbar wäre, „in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß“. Beeinträchtigend für diese Selbst-

bestimmung sei es, wenn ein Mensch nicht mehr „mit hinreichender Sicherheit überschauen kann“, welche Informationen über ihn „in bestimmten Bereichen seiner sozialen Umwelt bekannt sind“. Denn „wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden“.

Wie wichtig diese für ein demokratisches Selbstverständnis der Bürger ist, beschrieb das Gericht an folgendem Beispiel: „Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte verzichten.“ Damit seien dann aber nicht mehr nur „die individuellen Entfaltungschancen des Einzelnen“ beeinträchtigt, sondern die des Gemeinwohls“, da die „Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist“.

Für das Gericht ist die informationelle Selbstbestimmung also elementar für eine lebendige Demokratie. Sie ist damit auch ein Maßstab, der an jede neue Technologie und ihre Verwendung angelegt werden muss. In zwei Urteilen im Jahr 2008 hat das Bundesverfassungsgericht das Grundrecht auf informationelle Selbstbestimmung sogar noch erheblich gestärkt und sogar ein neues Grundrecht zum Schutz digitaler Kommunikation geschaffen. Anlass hierfür waren Gesetze gegen Terror und Schwerkriminalität, die datenschutzrechtliche Grundsätze nicht hinreichend berücksichtigt hatten.

Mit dem Urteil vom 27. Februar 2008 zur Zulässigkeit von Online-Durchsuchungen schuf das Gericht das „Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“. Es stellte darin fest, dass eine Überwachung der Nutzung von IT-Systemen und eine Auswertung der auf den Speichermedien befindlichen Daten weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung ermöglichen. Daraus ergebe sich, so die Richter, ein erhebliches Schutzbedürfnis, dem die bisherigen Regelungen jedoch keine Rechnung tragen würden.

Um dieses Schutzdefizit zu beheben, definierten die Richter das neue Grundrecht, das schwerwiegende Eingriffe in die Privatsphäre auf ein Mindestmaß begrenzt. Es ist dann anzuwenden, wenn ein Eingriff Systeme erfasse, die „personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen“. Nur wenn es Anhaltspunkte einer konkreten Gefahr für bestimmte Rechtsgüter gebe, sei dieses Recht nachrangig zu behandeln. Solche Rechtsgüter seien etwa „Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt“.

In einem weiteren Urteil vom 11. März 2008 entschied das Bundesverfassungsgericht, dass eine automatische Erfassung und Speicherung von Kfz-Kennzeichen auf Straßen und Plätzen ohne konkreten Anlass unzulässig ist. Zweck und Umfang des Datenabgleichs müssen klar benannt werden. Die Richter stellten fest, dass das Sammeln des Bewegungsverhaltens des Fahrers oder sonstige persönlichkeitsrelevante Informationen über einzelne Fahrten ein Grundrechtseingriff „von erheblichem Gewicht“ sein könne.

Über die Verfassungsbeschwerde gegen die Vorratsdatenspeicherung beziehungsweise das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen“ hat das Gericht noch nicht entschieden. Die Beschwerdeführer zeigen sich optimistisch, dass eine Analogie zur automatisierten Erfassung von Kfz-Kennzeichen herzustellen ist.

Die im Grundgesetz verankerten Grundrechte gelten im Verhältnis des Staates zu seinen Bürgern. Nur mittelbar wirken sie auch im Verhältnis der Bürger untereinander, da aus der Rechtsprechung entsprechende Prinzipien abgeleitet werden. Damit Bürger ihre Rechte aus der Verfassung klar entnehmen können, wird nun die Verankerung eines umfassenden Kommunikationsgrundrechts im Grundgesetz gefordert. ■

„Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“

Aus dem Volkszählungsurteil des Bundesverfassungsgerichts 1983

Urteile zum Datenschutz
auf der Website des Bundesverfassungsgerichts:

www.bundesverfassungsgericht.de

Foto: DBT/studio kohlmeier

Datenschützer Peter Schaar im Gespräch

„Kein Grundrecht zweiter Klasse“

Deutschlands oberster Datenschützer Peter Schaar plädiert für eine Kehrtwende im Verhältnis von Datenschutz und innerer Sicherheit und mahnt mehr Zurückhaltung des Staates beim Zugriff auf persönliche Daten der Bürger an.

Blickpunkt Bundestag: Es sind turbulente Zeiten für den Datenschutz. Wann war dies zuletzt der Fall?
Peter Schaar: Zu Zeiten der Volkszählung 1983 war das Thema Datenschutz vielleicht noch stärker als heute in der Diskussion. Es gab Proteste und Demonstrationen. Ein Ergebnis war bekanntlich das Volkszählungsurteil des Bundesverfassungsgerichts, das aus der Verfassung erstmals ein Grundrecht auf informationelle Selbstbestimmung abgeleitet hat. Pünktlich zum 25. Jubiläum haben wir jetzt wieder eine heiße Debatte über Datenschutz, die dem Anliegen nur nützlich sein kann.
Blickpunkt: Sie sind für eine Wiederwahl als Bundesbeauftragter vorgeschlagen. Wie verstehen Sie ihr Amt und wie lautet Ihre Bilanz nach fünf Jahren?
Schaar: Unabhängige Datenschutzbeauftragte sind wichtig, und natürlich hat der Bundesbeauftragte eine herausgehobene Stellung. Seine Funktion als Warner und Mahner wird in der Öffentlichkeit inzwischen stärker wahrgenommen. Dies zu erreichen, hatte ich mir vorgenommen. Das ist natürlich auch den Umständen geschuldet, ich hoffe aber, auch mit meinen Initiativen und meiner Überzeugungsarbeit dazu beigetragen zu haben. Der Datenschutz ist heute nicht mehr generell auf der schwächeren Seite. Im Gegenteil, in den vergangenen Monaten wurde zumindest für den Bereich der Wirtschaft sogar ein parteiübergreifender Konsens sichtbar, die Bürgerinnen und Bürger beim Datenschutz besserzustellen.
Blickpunkt: Ist das Amt des Bundesbeauftragten politisch richtig verankert?
Schaar: Natürlich könnte man sich fragen, ob es weitere Schritte in Richtung einer noch stärkeren Unabhängigkeit des Datenschutzbeauftragten geben sollte. Die EU-Kommission hat Deutschland wegen mangelnder Unabhängigkeit der Datenschutzaufsicht in den Bundesländern vor dem EuGH verklagt. Manche Frage, die sich in diesem Verfahren stellt, kann man auf den Bund übertragen, etwa die Rechtsaufsicht der Bundesregierung über den Bundesbeauftragten oder die Dienstaufsicht seitens des Bundesinnenministers. Für unsere praktische Arbeit hatte dies bisher aber keine Bedeutung. Gleichwohl könnte eine Entscheidung des Europäischen Gerichtshofs auch Auswirkungen auf den Bund haben. Denkbar ist zudem, den Datenschutzbeauftragten beim Bundestag anzusiedeln.
Blickpunkt: Würden Sie eine Anbindung an das Parlament bevorzugen?
Schaar: Das würde wohl seine Unabhängigkeit gegenüber der Regierungstätigkeit stärken, ich bin mir aber nicht

Der Bundesbeauftragte
für den Datenschutz und die Informationsfreiheit:

www.bfdi.bund.de

Foto: Picture-Alliance/Frank May

Zur Person:
Peter Schaar, Jahrgang 1954, wurde am 17. Dezember 2003 vom Bundestag zum Bundesbeauftragten für den Datenschutz (seit 1. Januar 2006 „für den Datenschutz und die Informationsfreiheit") gewählt. Der Volkswirt war von 1994 bis 2002 stellvertretender Dienststellenleiter des Hamburgischen Datenschutzbeauftragten.

sicher, ob dies zu einem „besseren Datenschutz" führen würde. Auf jeden Fall muss gewährleistet bleiben, dass der BfDI auch weiterhin frühzeitig in das Gesetzgebungsverfahren eingebunden bleibt, auch schon vor einem Kabinettsbeschluss.

Blickpunkt: Im Grundgesetz steht kein ausdrückliches Grundrecht auf Datenschutz. Reichen die Urteile des Bundesverfassungsgerichts?

Schaar: Ich befürworte ein schwarz auf weiß in der Verfassung verbrieftes Grundrecht auf Datenschutz. Das ist keine symbolische Forderung. In der Vergangenheit wurde der Datenschutz häufig als Grundrecht zweiter Klasse gesehen, eben weil er nicht ausdrücklich im Grundgesetz steht. In die Verfassung übernommen werden sollten deshalb das Grundrecht auf informationelle Selbstbestimmung aus dem Verfassungsgerichtsurteil von 1983 zur Volkszählung und das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme aus dem Urteil zur heimlichen Online-Durchsuchung. Wer sich gegen ein verbrieftes Datenschutzgrundrecht wendet, müsste eigentlich aus denselben Gründen auch gegen andere Grundrechte, etwa dasjenige auf Unverletzlichkeit der Wohnung, sein.

Blickpunkt: Der Staat selbst sammelt große Mengen an Daten. Sind sie in guten Händen?

Schaar: Ich glaube nicht, dass der Staat allgemein mit den Daten von Bürgern unvorsichtig umgeht. Aber er will – aus im Einzelfall durchaus nachvollziehbaren Gründen – immer mehr über seine Bürger wissen. Weil der Staat, anders als die Wirtschaft, auf Zwangsmittel zurückgreifen kann, ist er aber zu besonderer Zurückhaltung verpflichtet. Diese Zurückhaltung kann ich im Augenblick nicht überall erkennen.

Blickpunkt: Seit dem 11. September 2001 wird die „innere Sicherheit" großgeschrieben, der Datenschutz eher klein. Ist es Zeit für eine beherzte Kehrtwende, so wie in der Finanzmarktpolitik?

Schaar: Ein grundlegender Wechsel der Sichtweise ist nötig. Immer mehr Daten zu sammeln und auszuwerten, bringt nicht mehr Sicherheit. Es kann aber sehr schnell zu einem Daten-GAU führen, der das Vertrauen grundlegend erschüttert – auch auf internationaler Ebene. Deshalb fordere ich einen sehr viel kritischeren Blick auf die Möglichkeiten, Daten zu erheben und zu verarbeiten. Ich trete auch für einen klaren internationalen Rechtsrahmen ein. Mir leuchtet nicht ein, dass Staaten ihre Finanzmärkte regulieren und zugleich – ich denke hier besonders an die USA – beim Umgang mit persönlichen Daten

Der Bundesbeauftragte für den Datenschutz

Unabhängige Instanz

„Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI)“ heißt das Amt des obersten deutschen Datenschützers etwas sperrig, seit am 1. Januar 2006 neue Aufgaben hinzugekommen sind: Seitdem räumt das Informationsfreiheitsgesetz jedem Bürger voraussetzungslos ein Recht auf Zugang zu Behördeninformationen ein. Und jeder kann nun den Bundesbeauftragten anrufen, wenn er dieses Recht als verletzt ansieht. Angesichts der jüngsten Fälle massenhaften Datenmissbrauchs steht jedoch jene Funktion im Vordergrund, die das Amt im Januar 1978 begründete: die unabhängige Kontrolle des Datenschutzes bei öffentlichen Stellen des Bundes und bei Telekommunikations- und Postunternehmen. Nicht zu den Aufgaben gehört die Kontrolle des Datenschutzes in der allgemeinen Privatwirtschaft. Dies ist Sache der Aufsichtsbehörden der Länder – vielfach der Innenministerien, in einigen Fällen auch des Landesdatenschutzbeauftragten. Letztere sind zudem zuständig für den Datenschutz im Bereich der Verwaltungen der Länder und der Gemeinden.

Wichtig ist die Unabhängigkeit des Bundesbeauftragten, damit er seinen Aufgaben nachkommen kann. Von der Bundesregierung vorgeschlagen, wird er vom Bundestag für fünf Jahre gewählt. Der amtierende Bundesdatenschutzbeauftragte Peter Schaar wurde 2003 auf Vorschlag von Bündnis 90/Die Grünen gewählt. Damals stimmte die Unionsfraktion gegen das Grünenmitglied. Knapp fünf Jahre später hat ihn Innenminister Wolfgang Schäuble (CDU/CSU) mit Unterstützung der Unionsfraktion für eine Wiederwahl vorgeschlagen. Sie ist nur einmal möglich. Angesiedelt ist der Beauftragte am Bonner Sitz des Bundesinnenministeriums. Er untersteht zwar dessen Dienstaufsicht und der Rechtsaufsicht der Bundesregierung. Eine Fachaufsicht besteht jedoch nicht, was die Unabhängigkeit des Datenschützers unterstreicht.

Ein wichtiges Kontrollinstrument des Bundesbeauftragten ist sein Tätigkeitsbericht, den er alle zwei Jahre dem Bundestag vorlegt. Als Schaar zuletzt im April 2007 das gut 200 Seiten starke Dokument überreichte, bemängelte er eine starke Einschränkung des Datenschutzes zugunsten der inneren Sicherheit und forderte, der Staat müsse das Grundrecht auf informationelle Selbstbestimmung wieder stärker unter Schutz stellen.

Foto: DBT/Sylvia Bohn

Rechenschaft gegenüber dem Bundestag: Alle zwei Jahre übergibt der Bundesbeauftragte seinen Tätigkeitsbericht

auf möglichst wenig Regulierung drängen. Guter Schutz ist die Voraussetzung dafür, dass die Bürger ihre Daten auch preisgeben, ohne die Angst, dass damit Schindluder getrieben wird. Das gilt für die Wirtschaft wie für staatliche Stellen.

Blickpunkt: Aber wer sich gesetzestreu verhält, hat doch nichts zu verbergen.

Schaar: Jeder hat etwas zu verbergen, weil jeder ein Recht hat, sich privat und ungehindert mit anderen Menschen auszutauschen. Der Staat hat keinen Anspruch darauf, jeden Schritt seiner Bürger zu kontrollieren. Ein weiteres Problem in diesem Zusammenhang ist die „Vernachrichtendienstlichung“ der Polizei. Seit rund 20 Jahren setzt sie immer mehr verdeckte Methoden ein. Darüber hinaus gibt es einen massiven Austausch von Informationen zwischen Polizei und Nachrichtendiensten. Dagegen bin ich nicht prinzipiell, das Ausmaß geht inzwischen aber zu weit.

Blickpunkt: Was lernt der Datenschützer aus den jüngsten Fällen von Datenhandel und -missbrauch in der Wirtschaft?

Schaar: Der Bundesbeauftragte lernt daraus erstens, dass es um die Datenschutzkultur selbst bei einigen großen Unternehmen nicht so bestellt war oder ist, wie wir uns das wünschen. Hier ist mehr Kontrolle nötig, und das bedeutet eine Aufstockung der Mittel bei den Aufsichtsbehörden. Momentan gilt: Wer Datenschutzregeln missachtet, geht ein relativ geringes Risiko ein, entdeckt zu werden, weil die Datenschutzaufsicht schwach ausgestattet ist. Unterstützung erhoffe ich mir auch aus dem Bundestag im Rahmen der Haushaltsberatungen. Zweitens: Wenn Daten verloren gehen, müssen Mechanismen installiert werden, die den Schaden begrenzen, vor allem eine Informationspflicht über Datenschutzverletzungen. Drittens dürfen persönliche Daten für Werbung nur mit Einwilligung der Betroffenen weitergegeben werden, und es muss für sie nachvollziehbar sein, woher die Daten stammen. Schließlich müssen endlich die Voraussetzungen für Datenschutzgütesiegel geschaffen werden. Deshalb setze ich darauf, dass noch in dieser Legislaturperiode das Datenschutzauditgesetz beschlossen wird. ■

Foto: Stefan Boness/Ipon

Für den Datenschutz auf die Straße: Demonstration im Oktober 2008 in Berlin

Datenschutz in der Debatte

Von Gütesiegel bis Datenhandel

Das Datenschutzrecht wird derzeit auf mehreren Ebenen debattiert. Zum einen sind mehrere Entwürfe und Vorhaben der Bundesregierung in der Diskussion. Außerdem gibt es seitens einzelner Bundestagsfraktionen, des Bundesrats und auch der EU-Kommission Initiativen zur Regelung datenschutzrechtlicher Teilbereiche.

Datenschutzaudit Derzeit wird ein Referentenentwurf für ein Bundesdatenschutzauditgesetz diskutiert. Eine prinzipielle Regelung für ein Datenschutzaudit wurde bereits 2001 im novellierten Bundesdatenschutzgesetz (BDSG) erlassen, doch ein Ausführungsgesetz fehlt bislang. Anbieter von Datenverarbeitungssystemen und -programmen sowie datenverarbeitende Stellen sollen künftig ihre Datenschutzmaßnahmen und -regeln sowie die entsprechenden technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen. Das Zertifikat soll in einem zweiten Schritt möglicherweise durch eine staatliche oder staatlich beauftragte Stelle vergeben werden. Mit dem Zertifikat beziehungsweise mit dem Gütesiegel sollen Unternehmen oder Behörden zwei Jahre lang bundesweit werben dürfen. Außerdem sollen auch Gütesiegel an Hersteller von Hardware- und Softwareprodukten vergeben werden. Der Bundesdatenschutzbeauftragte soll ein öffentliches Register der Gütesiegel führen, das über das Internet einsehbar sein soll. Ein ähnliches Audit- und Gütesiegelverfahren wird in Schleswig-Holstein bereits seit Jahren erfolgreich praktiziert.

Scoring Als Gesetzentwurf liegt eine Novelle des Bundesdatenschutzgeset-

zes (BDSG) vor, die sich auf das Scoring für die Bonitätsprüfung von Verbrauchern bezieht. Geklärt wird unter anderem, welche Daten bei den zugelassenen Bewertungsverfahren verwendet und übermittelt werden dürfen. Eine rein automatisierte Berechnung eines Score-Wertes ist nicht mehr zulässig – er soll künftig auch durch eine Person bewertet werden. Verbraucher sollen außerdem mehr darüber erfahren können, auf welche Weise der Wert, der ihre Kreditwürdigkeit ausdrückt, ermittelt wird. Dies bezieht sich auch auf jene Daten, welche für die Erstellung des Score-Werts hinzugezogen werden, die anonym oder bei Dritten gespeichert sind. Erkundigt sich ein Verbraucher nach Kreditkonditionen, soll sich dies künftig nicht mehr negativ auf seinen Score-Wert auswirken.

Geodaten Ein Referentenentwurf der Bundesregierung für ein geplantes Gesetz über den Zugang zu digitalen Geodaten zielt darauf ab, die Verwendung von Geodaten zu regeln. So sollen Daten entweder gesperrt oder freigegeben werden. Datenschützer fordern, die Daten ähnlich einer Ampel differenzierter zu klassifizieren. Mit Grün gekennzeichnete Daten dürften frei verwendet werden. Gelb markierte Daten dürften bei berechtigtem Interesse genutzt werden. Rot würde schutzwürdige Interessen und ein striktes Zugangsverbot signalisieren. Hintergrund: Bis Mai 2009 müssen alle EU-Mitgliedsstaaten die Geodaten-Richtlinie in nationales Recht umsetzen, die den Zugang zu Geoinformationsdaten europaweit regelt.

Standpunkte der Fraktionen:

	CDU/CSU – Fraktion im Deutschen Bundestag	SPD Bundestagsfraktion
Gehört der Datenschutz ins Grundgesetz?	Das Grundrecht auf informationelle Selbstbestimmung folgt aus dem allgemeinen Persönlichkeitsrecht des Artikels 2 Absatz 1 des Grundgesetzes. Datenschutz ist insoweit bereits im Grundgesetz verankert.	Vorrangig sollte eine umfassende Modernisierung des Datenschutzes, die Anpassung an die veränderten technischen Möglichkeiten und die Definition des Datenschutzes aus der Sicht von Bürgern sowie ihrer Schutzinteressen erfolgen. Die Frage, ob und wie Datenschutz ins Grundgesetz aufgenommen werden soll, wird in der SPD derzeit diskutiert.
Was muss gegen Datenmissbrauch und illegalen Datenhandel getan werden?	In der Privatwirtschaft, die 90 Prozent der personenbezogenen Daten verwaltet, brauchen wir mehr Kontrolle, mehr individuelle Verantwortlichkeit, größere Sorgfalt im Datenumgang und bei Missbrauch: Publizität und höhere Strafen. Vor allem muss den Bürgern bewusst werden, dass sorgloser Umgang mit eigenen Daten den Missbrauch häufig erst ermöglicht.	Zum Schutz der Bürger vor Datenmissbrauch ist nötig: vorherige Einwilligung bei der Verwendung personenbezogener Daten, Stärkung der Auskunftsrechte der Kunden, Verschärfung der Strafen bei Rechtsverletzungen, Stärkung der Kontrollrechte der Datenschutzbeauftragten.
Brauchen wir ein Arbeitnehmerdatenschutzgesetz?	Datenschutz im Arbeitsverhältnis bedarf keines Sonderrechts. Die Parteien des Arbeitsvertrages unterliegen sämtlichen datenschutzrechtlichen Vorschriften, insbesondere des Bundesdatenschutzgesetzes. Wo Bedarf besteht, die komplexen Vorschriften im Arbeitsverhältnis handhabbar zu machen, können vorzugsweise freiwillige betriebsnahe Lösungen getroffen werden.	Es fehlen bislang klare Regelungen zum Datenschutz von Arbeitnehmern im Betrieb, obwohl der elektronischen Verarbeitung von Mitarbeiterdaten im Arbeitsverhältnis immer größere Bedeutung zukommt, zum Beispiel durch Personalverwaltungs- und Informationssysteme. Diese Lücke muss rasch geschlossen werden. Das gilt auch für die europäische Ebene.

Arbeitnehmerdatenschutzgesetz

Seit Jahrzehnten fordern Datenschützer ein Arbeitnehmerdatenschutzgesetz, nun gibt es hierzu eine Initiative im Bundesrat. Ziel ist es, mehr Rechtssicherheit für Arbeitnehmer und Unternehmen zu schaffen. Ebenfalls diskutiert wird, ob den betrieblichen Datenschutzbeauftragten mehr Kompetenzen, aber auch ein den Betriebsräten ähnlicher Schutz zukommen soll. Überlegt wird auch, ob sie verpflichtet werden sollen, in bestimmten Fällen die staatlichen Datenschutzstellen zu informieren. Anlass sind die bekannt gewordenen Überwachungen von Mitarbeitern in einigen großen Unternehmen. Derzeit ist zwar die Datenerhebung und -verarbeitung im Arbeitsverhältnis nur erlaubt, wenn es der Wahrung berechtigter Interessen dient und die schützenswerten Interessen der Betroffenen nicht überwiegen. Doch in der Praxis sind Grenzziehungen nicht eindeutig zu bewerkstelligen.

Grundgesetz

Derzeit werden auch Pläne diskutiert, den Datenschutz im Grundgesetz zu verankern. Überlegt wird, die informationelle Selbstbestimmung direkt in das Grundgesetz einzubauen sowie ein Grundrecht auf Informationsfreiheit zu schaffen. Bislang gelten mehrere Urteile des Bundesverfassungsgerichts als wegweisend: Das Volkszählungsurteil, das das Recht auf informationelle Selbstbestimmung feststellt, das Urteil zum großen Lauschangriff, das den absoluten Schutz des Kernbereichs privater Lebensgestaltung definiert sowie das Urteil zu heimlichen Online-Durchsuchungen, das das Recht auf „Gewährleistung der Vertraulichkeit

FDP im Deutschen Bundestag

Das Informationszeitalter basiert auf Daten. Der Datenschutz hat daher eine zentrale Bedeutung, weil die Gewissheit, nicht überwacht zu werden, Voraussetzung für die Wahrnehmung anderer Freiheiten ist. Im Grundgesetz sind die Freiheitsrechte in klaren und jedermann verständlichen Worten verfasst. Daher gehört Datenschutz ins Grundgesetz.

Unter anderem Folgendes: Unternehmen erhalten ein Datenschutzgütesiegel. Die Datenschutzaufsicht muss schlagkräftiger werden. Verträge dürfen nicht von der Angabe von Daten abhängen. Jede Datenverwendung muss genehmigt sein. Daten brauchen Marker zur Rückverfolgbarkeit. Eine Stiftung Datenschutz soll Produkte und Dienstleistungen vergleichen und bewerten.

Die Interessen von Arbeitgebern und Arbeitnehmern müssen in Einklang gebracht werden. Videoüberwachung bis in Umkleidekabinen darf es nicht geben. Protokollierung von E-Mails ohne Wissen des Betroffenen ist unzulässig. Was den Arbeitgeber nichts angeht, darf er nicht verlangen – Datensparsamkeit ist der beste Datenschutz. Arbeitnehmerdaten brauchen einen klaren rechtlichen Schutz.

DIE LINKE. im Bundestag

Der Vorschlag, den Datenschutz ins Grundgesetz aufzunehmen, löst das aktuelle Problem nicht. Denn dadurch ergibt sich nicht zwangsläufig eine stärkere Beachtung des Datenschutzes durch Staat und Privatwirtschaft. Diese Forderung wäre dann überlegenswert, wenn zuvor etwa das Bundesdatenschutzrecht modernisiert werden würde.

Die Linke fordert ein Sofortprogramm zur Stärkung des Datenschutzes. Hierzu gehört für uns neben einer Modernisierung des Datenschutzrechtes eine verbesserte Ausstattung der Bundes- und der Landesdatenschutzbeauftragten, ein Moratorium und eine Evaluation aller datenschutzrelevanten Sicherheitsgesetze und der sofortige Stopp der Vorratsdatenspeicherung.

Ein gutes Arbeitnehmerdatenschutzgesetz ist eine sinnvolle Ergänzung eines modernisierten Datenschutzrechtes und angesichts der Fälle der Ausspähung von Mitarbeiterinnen und Mitarbeiter in Unternehmen dringend notwendig. Die Linke hat hierzu einen entsprechenden Antrag erarbeitet und wird diesen umgehend in die parlamentarische Debatte geben.

BÜNDNIS 90 DIE GRÜNEN Bundestagsfraktion

Der Datenschutz ist heute so wichtig, dass er ins Grundgesetz gehört. Wir möchten, dass die Bürgerinnen und Bürger durch einen einfachen Blick in die Verfassung erkennen können, welche Freiheitsrechte sie haben. Gerichtsentscheidungen allein reichen dafür nicht. Verfassungsgeber ist das Parlament und nicht das Bundesverfassungsgericht.

Wir fordern in unserem Antrag „Datenschutz stärken“ eine umfassende Modernisierung des Datenschutzgesetzes: unter anderem Informationspflichten bei Datenschutzpannen, Kennzeichnungspflicht für die Herkunft personenbezogener Daten, absolute Kopplungsverbote, Stärkung des Opt-in-Gedankens und der Aufsichtsbehörden – keine weiteren Prüfvorbehalte!

Skandale wie bei LIDL, Telekom und Co. zeigen, dass die betrieblichen Beauftragten gestärkt werden müssen. Dies ist auch eine jahrzehntelange Forderung der Datenschutzbeauftragten von Bund und Ländern und der Gewerkschaften. Die bislang verstreuten Vorschriften gehören zusammen. Die Frage, wo das dann geregelt wird, ist allerdings nachrangig.

und Integrität informationstechnischer Systeme“ begründet. Bündnis 90/Die Grünen haben hierzu einen Gesetzentwurf vorgestellt.

RFID-Regelung Im Logistikbereich werden Daten in geschlossenen Netzen weitergereicht. Datenschutzrechtlich ist dies überschaubar. Wenn Dinge nach einem Kauf weiterhin Daten abgeben, ist die Verantwortlichkeit des Dienstleisters gegenüber dem Kunden nicht eindeutig geklärt. Hier könnten Profile einzelner Verbraucher erstellt werden. Insbesondere die Transparenz halten Datenschützer für verbesserungswürdig. Dazu gehören sogenannte Opt-out-Möglichkeiten für die Nutzer, wie etwa die Deaktivierung der RFID-Chips. Als problematisch gelten angesichts des grenzüberschreitenden Waren- und Datenverkehrs außerdem die EU-weit unterschiedlichen Datenschutzstandards. Entsprechende Regelungen werden derzeit auf EU-Ebene diskutiert.

Datenhandel In diesem Jahr wurden mehrere Fälle von Datenmissbrauch und illegalem Datenhandel bekannt. Datenschützer fordern nun höhere Strafen gegen den illegalen Datenhandel. Die Zwecke, für die Daten gesammelt werden dürfen, sollen noch klarer bestimmt und enger gefasst werden. Entsprechend sollte eine ausdrückliche Zustimmung des Kunden vorliegen, unabhängig etwa vom Kaufvertrag. Diskutiert wird auch eine Regelung, die telefonisch geschlossene Verträge ohne schriftliche Bestätigung für unwirksam erklärt. Schließlich sollen die staatlichen Datenschutzbeauftragten dazu befähigt werden, auch präventiv in Unternehmen zu kontrollieren. Beim Datenschutzgespräch im September 2008 wurden Maßnahmen im Bereich Datenhandel angekündigt, das Bundesinnenministerium will dem Kabinett im November einen Gesetzentwurf vorlegen.

Vorratsdatenspeicherung Da Kundendaten wie die von T-Mobile zu Abrechnungszwecken, aber auch zu Zwecken der Strafverfolgung sechs Monate gespeichert werden müssen, wird von den Oppositionsfraktionen und verschiedenen politischen Gruppen die Abschaffung der Anfang des Jahres in Kraft getretenen Vorratsdatenspeicherung gefordert, insbesondere mit dem Argument, dass das Missbrauchspotenzial groß und unkalkulierbar sei. Das Urteil des Bundesverfassungsgerichts zur Verfassungsbeschwerde gegen die Vorratsdatenspeicherung steht noch aus.

Umstrittenes Sammeln von Geodaten: Ein Kamerafahrzeug des Internetkartenanbieters Google Earth nimmt in Berlin 360-Grad-Bilder einer Straße auf

Foto: Picture-Alliance/Gero Breloer

Infotipps

Institutionen

Der Bundesbeauftragte
für den Datenschutz und die Informationsfreiheit
www.bfdi.bund.de

Bundesamt
für Sicherheit in der Informationstechnik
www.bsi.bund.de/themen

Konferenz
der Datenschutzbeauftragten
www.datenschutz.de/dsb-konferenz

Virtuelles Datenschutzbüro
getragen von verschiedenen Datenschutzinstitutionen
www.datenschutz.de

Vereine und Verbände

Berufsverband
der Datenschutzbeauftragten Deutschlands e. V.
www.bvdnet.de

Gesellschaft
für Datenschutz und Datensicherung e. V.
www.gdd.de

Deutsche Vereinigung
für Datenschutz e. V.
www.datenschutzverein.de

Arbeitskreis
Vorratsdatenspeicherung
www.vorratsdatenspeicherung.de

Rechtliche Grundlagen

Bundesdatenschutzgesetz
Website „Gesetze im Internet“
www.gesetze-im-internet.de/bdsg_1990

Bundesverfassungsgericht
Urteile zum Datenschutz (ab 1998)
www.bundesverfassungsgericht.de

Europäische Union

Datenschutzportal
der Europäischen Union
www.ec.europa.eu/justice_home/fsj/privacy

Datenschutzbeauftragter
der Europäischen Union
www.edps.europa.eu

Infomaterial bestellen

Infomaterial und Broschüren über die Arbeit des Deutschen Bundestages sowie Flyer, Poster, CD-ROMs und DVDs können Sie per Post oder Telefon bestellen oder bequem per Mausklick auf ihren Bildschirm holen und herunterladen.

Bestellung per Post:
Deutscher Bundestag
– Referat Öffentlichkeitsarbeit –
Platz der Republik 1
11011 Berlin

Bestellung per Telefon oder Fax:
Telefon: (0 30) 2 27-3 20 72 und -3 53 90
Fax: (0 30) 2 27-3 62 00

Bestellung im Internet:
PDF-Download und Onlinebestellung unter

www.bundestag.de/interakt/infomat

Dort finden Sie eine aktuelle Übersicht aller Informationen (Broschüren, CD-ROMs etc.).

Impressum

Herausgeber:
Deutscher Bundestag,
Referat Öffentlichkeitsarbeit

Chefredaktion:
Britta Hanke-Giesers
(Leiterin Referat Öffentlichkeitsarbeit),
Michael Reinold
Koordination:
Michael Reinold, Sylvia Bohn
(Referat Öffentlichkeitsarbeit)
Telefon: (0 30) 2 27-3 78 68
Fax: (0 30) 2 27-3 65 06
E-Mail: michael.reinold@bundestag.de

Beauftragte Agentur:
MEDIA CONSULTA Deutschland GmbH
Wassergasse 3, 10179 Berlin
Telefon: (0 30) 6 50 00-2 20
Fax: (0 30) 6 50 00-1 92
E-Mail: blickpunkt@media-consulta.com
Geschäftsführung:
Dipl.-Kfm. Harald Zulauf
Redaktion:
Helmut Spörl (Leiter),
Klemens Vogel, Birgit Lettenbauer

Autorin: Christiane Schulzki-Haddouti;
Interview: Helmut Spörl

Art Direction:
Sylvia Müller, Anita Drbohlav
Produktion:
René Hanhardt
Onlineproduktion:
Nils Grobmeier
Lektorat:
Katleen Krause
Druck:
Koelblin Fortuna, Baden-Baden

Redaktionsschluss:
27. Oktober 2008

Bildnachweis:

Die Texte aus Blickpunkt Bundestag gibt es auch im Internet: www.blickpunkt-bundestag.de

Foto: Picture-Alliance/Rolf Vennenbernd

Datenschutz ist ein Grundpfeiler der Demokratie. Dass jeder selbst über die Preisgabe und Verwendung seiner persönlichen Daten bestimmen kann, hat das Bundesverfassungsgericht 1983 als eine Voraussetzung für die freie Entfaltung der Persönlichkeit definiert. Heute, in einer Welt der globalen Datenströme, stehen Bürger und Politik vor völlig neuen Herausforderungen. Der Datenhunger der Sicherheitsbehörden, Datenmissbrauch in der Wirtschaft und Technologien, die eine Vielzahl personenbezogener Daten erzeugen, rücken den Datenschutz ins Zentrum der Aufmerksamkeit. BLICKPUNKT BUNDESTAG SPEZIAL zeigt, was Datenschutz heute bedeutet: Vor welchen Aufgaben steht die Informationsgesellschaft im öffentlichen und im privaten Sektor? Wie ist der Datenschutz als Grundrecht abgesichert? Und welche politischen Initiativen sind in der aktuellen Diskussion?

www.bundestag.de