Jan-Hinrik Schmidt / Thilo Weichert (Hrsg.)

Datenschutz

Grundlagen, Entwicklungen und Kontroversen

bpb: Bundeszentrale für politische Bildung

Bonn 2012

Redaktion: Elke Diehl
Lektorat: Sven Lüders, Sarah Thomé

Umschlaggestaltung: Michael Rechl, Kassel
Umschlaggrafik: Ausschnitt aus dem Video zum Online-Spiel Data Dealer, im Internet unter http://www.datadealer.net
Illustrationen: Reinhard Alff, Dortmund
Satzherstellung und Layout: Naumilkat – Agentur für Kommunikation und Design, Düsseldorf
Druck: CPI books GmbH, Leck

ISBN: 978 – 3-8389-0190-9

www.bpb.de

Inhalt

* Im Text verweist ein Pfeil auf die im Glossar erläuterten Begriffe.

Vorwort

Angesichts einer Vielzahl technischer und medialer Innovationen ist die informationelle Selbstbestimmung der Bürgerinnen und Bürger wichtig und problematisch zugleich. Im Berufs- und Privatleben, gegenüber Unternehmen, Verwaltungs- und Gesundheitsbehörden, im Umgang mit den vernetzten Öffentlichkeiten des Internets oder als Person in öffentlichen Räumen: Überall werden Daten unterschiedlichster Art erhoben, gespeichert, verknüpft, zusammengeführt und kombiniert. Für den Einzelnen ist nicht mehr überschaubar, wer wann welchem Personenkreis gegenüber welche personenbezogenen Daten preisgibt und für welche Zwecke sie verwendet werden. Dadurch droht der Abbau oder Zerfall eines Grundrechts unserer Gesellschaft: die Möglichkeit und Fähigkeit, selbstbestimmt entscheiden zu können, wer Zugang zu Informationen über die eigene Person besitzt; mithin: die eigene Privatsphäre vor unerwünschten Zugriffen zu schützen.

Nachdem die Debatten der 1980er Jahre (Stichwort: Volkszählungsboykott) in der Folgezeit etwas abgeflaut waren, hat die Auseinandersetzung zum Thema »Datenschutz«, aber auch der entsprechende Handlungsbedarf in den vergangenen Jahren wieder deutlich zugenommen. Die Frage, unter welchen Bedingungen und mit welchen Instrumenten Datenschutz und informationelle Selbstbestimmung gewährleistet werden können, ist zu einem äußerst wichtigen gesellschaftlichen Konfliktfeld geworden. Privatpersönliche, politische, unternehmerische oder organisatorische Praktiken, Erwartungen und Begehrlichkeiten können miteinander in Widerspruch geraten – beispielsweise wenn es um das Management von Kundenbeziehungen, die Pflege von sozialen Beziehungen mittels *online*basierter Kommunikationsmedien oder die Entscheidung zwischen Freiheits- und Sicherheitsrechten geht. Bereits jetzt ist absehbar, dass die technische Entwicklung in den nächsten Jahren und Jahrzehnten weitere Fragen und Konfliktpotenziale beim Datenschutz aufwerfen wird, die individuell bewältigt und gesellschaftlich verhandelt werden müssen – zum Beispiel in den Bereichen der Bio- und Nanotechnologie.

Um als Mensch das Grundrecht auf informationelle Selbstbestimmung auszuüben, aber auch, um in den gesellschaftlichen Auseinandersetzungen Stellung beziehen und die eigene Meinung bilden und äußern zu können, ist ein zumindest grundlegendes Verständnis für die rechtlichen, technischen, politischen und gesellschaftlichen Rahmenbedingungen des Daten-

schutzes nötig. Der vorliegende Sammelband möchte einen Beitrag dazu leisten, das Themenfeld »Datenschutz« zu systematisieren und einen Überblick über den aktuellen Stand von Technik, Recht und gesellschaftlichen Debatten, über Herausforderungen, Chancen und Risiken sowie mögliche Szenarien der zukünftigen Entwicklung zu geben.

In insgesamt fünf großen Abschnitten beleuchtet der Band nicht nur die – allgemeinverständlich dargestellten – rechtlichen und technischen Rahmenbedingungen von Datenschutz, sondern auch dessen sozialwissenschaftliche, pädagogische, politische und psychologische Aspekte. Teil I beleuchtet den »Datenschutz im Kontext«, Teil II präsentiert »Brennpunkte und Kontroversen« der aktuellen Debatten, Teil III stellt die wesentlichen Elemente zum »Datenschutzrecht« in seinem Bestand und der weiteren Perspektiven vor, Teil IV skizziert den »Technischen und organisatorischen Datenschutz« und Teil V widmet sich dem »Datenschutz international«. Soweit dies möglich war, erfolgt auch eine kontroverse Diskussion von Themen. Teil VI (Anhang) enthält neben einem Glossar erklärungsbedürftiger Begriffe Literatur- und Internethinweise sowie weitere serviceorientierte Informationen.

Unsere gemeinsame Herausgebertätigkeit war nur deswegen möglich, weil uns verschiedene Personen in unterschiedlichen Phasen des Vorhabens zur Seite standen. Wir danken daher sehr herzlich Mareike Scheler und Felix Schröter für vorbereitende Recherchen und organisatorische Hilfe, Sven Lüders und Sarah Thomé für das hervorragende Lektorat sowie Elke Diehl für ihre konstruktive und ermutigende Unterstützung des Buchprojekts von seinen Anfängen bis zur Fertigstellung.

Hamburg/Kiel im Juli 2012

Jan-Hinrik Schmidt
Thilo Weichert

I. Datenschutz im Kontext

Einleitung

Die neun Beiträge des ersten Abschnitts stellen wesentliche Rahmenbedingungen und Entwicklungen des Datenschutzes dar, wobei vor allem der Bezug zum Konzept der »Privatsphäre« bzw. der »Privatheit« herausgearbeitet wird. Die Texte argumentieren jeweils aus unterschiedlichen disziplinären Perspektiven:

Kai von Lewinski fasst einleitend die kulturhistorische Entwicklung von Privatsphäre und Datenschutz zusammen.

Christoph Bieber zeigt aus dem Blickwinkel der Politikwissenschaft, wie der Datenschutz in den vergangenen Jahrzehnten immer auch ein Feld der politischen Auseinandersetzung gewesen ist.

Eine Akteurin und ein Akteur der aktuellen außerparlamentarischen netzpolitischen Bewegung – *Franziska Heine* und *Markus Beckedahl* – verdeutlichen in kurzen Beiträgen, wie das Thema »Datenschutz« zur Politisierung der »Generation *Online*« geführt hat.

Wiebke Loosen stellt die Zusammenhänge zwischen (massen-)medialer Kommunikation und Privatheit vor, während *Sabine Trepte* Erkenntnisse der Psychologie zu Datenschutz und Privatsphäre zusammenfasst.

Die verfassungsrechtlichen Grundlagen des Datenschutzes werden im Beitrag von *Hans-Jürgen Papier* dargestellt.

Marit Hansen zeigt, wie durch Überwachungstechnologien an verschiedenen Stellen des Alltags Daten über uns gesammelt werden.

Edgar Wagner schließlich plädiert dafür, den Datenschutz (auch) als Bildungsaufgabe zu verstehen.

Kai von Lewinski

Zur Geschichte von Privatsphäre und Datenschutz – eine rechtshistorische Perspektive

Die meisten historischen Darstellungen zur Geschichte des Datenschutzes in Deutschland beginnen mit der Volkszählungsentscheidung des Bundesverfassungsgerichts (1983), dem Bundesdatenschutzgesetz (1976/1977) oder bestenfalls dem hessischen Datenschutzgesetz (1970), dem ersten einschlägigen Gesetz hierzulande und wohl auch weltweit.[1] Das aus heutiger Sicht zentrale Motiv des Datenschutzes – der Schutz vor Datenmacht – ist jedoch viel älter als diese Gesetze und auch viel älter als der Begriff des »Datenschutzes« selbst.[2] Schutz vor Datenmacht – dahinter steckt die Überzeugung, dass informationelle Verhältnisse auch Machtbeziehungen sind und der Einzelne vor asymmetrischen Informationsbeziehungen geschützt werden muss. Eine Geschichte des Datenschutzes in diesem Sinne ließe sich aus der Geschichte menschlicher Geheimnisse und gesellschaftlicher Geheimhaltung sowie aus den wechselnden Grenzziehungen zwischen öffentlichen und privaten Sphären rekonstruieren.

Wirklich relevant wurde das, was wir heute »Datenschutz« nennen, aber erst, als in der Neuzeit der Staat und später auch Unternehmen gegenüber dem Einzelnen ein informationelles Übergewicht gewannen (Datenmacht). Das Bewusstsein um die Gefahren dieser fragilen Beziehung findet sich im juristischen Konzept des Persönlichkeitsrechts wieder, auf dessen Grundlage das heutige Datenschutzrecht aufbaut. Gegenwärtig erleben wir eine erneute Verschiebung dieser Informationsbalance. Das Internet hat einige globale Unternehmen hervorgebracht, die zu mächtigen Datensammlern und Datenhändlern aufgestiegen sind. Mit der Erkenntnis, dass heute neben dem Staat auch die Unternehmen der Informationsgesellschaft (und auf Grundlage ihrer Dienste faktisch auch Privatpersonen, also die Gesellschaft als solche) auf riesige Mengen an personenbezogenen Daten zugreifen können, verschiebt sich der Fokus des Datenschutzes erneut.

1 Ursprünge der Vertraulichkeit in der Bürokratie und Entdeckung des Individuums

Das »natürliche« informationelle Gleichgewicht dörflicher Gemeinschaften wurde in den ersten Hochkulturen verändert, vor allem mit der Nutzung der Schrift als neuem Informationsmedium. Die zunehmende Arbeitsteilung und die Entstehung städtischer Lebensformen lässt einen Bedarf erkennen, das Leben der Menschen zu erfassen – ihre Arbeits- und Abgabenleistung, ihren Nahrungsbedarf, ihr militärisches Potenzial. Die schriftliche Fixierung solcher Informationen war die Basis, auf der sich erste Formen der Steuerung von (Verwaltungs-)Abläufen und damit erste bürokratische Strukturen herausbildeten. Allerdings wurde diese frühe »Verdatung« – soviel wir wissen – nicht als Problem erfahren. Doch unterschieden schon die Griechen des perikleischen Athens (circa 500 v. Chr.) zwischen dem Landgut (*oikos*) als dem Privaten und dem Stadtplatz (*agora*) als dem Öffentlichen. Diese Unterscheidung kann als konzeptionelle Vorläuferin der Privatsphäre angesehen werden. Und an ersten Verschwiegenheitsregeln für einzelne Berufe lässt sich ein Bedarf an Geheimhaltung erkennen. So reklamiert der berühmte Eid des Hippokrates (um 400 v. Chr.): »Was ich bei der Behandlung oder auch außerhalb meiner Praxis im Umgange mit Menschen sehe und höre, das man nicht weiterreden darf, werde ich verschweigen und als Geheimnis bewahren.«

Im Mittelalter entfielen die administrativen Voraussetzungen für Datenmacht, weil viele Errungenschaften der Antike in Vergessenheit geraten und insbesondere die modern anmutenden bürokratischen Ordnungen des Römischen Reiches zerfallen waren. Überhaupt war das Mittelalter durch personale Herrschaftsverbände (Lehnswesen) gekennzeichnet; persönliche (Ver-)Bindungen zwischen Lehnsherrn und Vasall, Grundherrn und Hintersasse waren die Grundlage des sozialen Zusammenlebens. Anonymität war nicht – anders als dann im 20. Jahrhundert – das gesellschaftliche Leitbild. Vielmehr war die Einordnung in einen auf persönlicher Bindung beruhenden (Personen-)Verband die Voraussetzung sozialer Existenz.

Der Ursprung des heutigen Datenschutzes liegt dann im Spannungsverhältnis zwischen dem (erneuten) Entstehen bürokratischer Datenmacht des modernen Staates[3] und der Entdeckung des Menschen als Individuum.

In einem langen Prozess begannen sich nach 1500 die modernen Territorial- und Nationalstaaten zu bilden. Sie lösten die mittelalterlichen personalen Herrschaftsverbände auf und konzentrierten die Herrschaft bei dem durch den Fürsten personifizierten Staat. Dieser konnte seine Herrschaft nicht mehr durch überschaubare persönliche Treue- und Schutzver-

pflichtungen ausüben, sondern musste eine Bürokratie aufbauen. Bürokratie wiederum ist auf Informationen über die Untertanen angewiesen. Ausgehend von den Kirchenbüchern entwickelte sich schrittweise eine hoheitliche Erfassung der Bevölkerung, seit etwa 1700 gibt es zunehmend systematische Datenerhebungen.

Die Aufklärung stellte parallel dazu den einzelnen Menschen in den Mittelpunkt der Welt. Mit der Entdeckung des Individuums kam dem Einzelnen ein Wert an sich zu. Der Mensch war nicht mehr (nur) Mittel zu einem höheren (Staats-)Zweck oder Objekt von Herrschaft, sondern Subjekt. Gedanklich wurde dies meist an der Ehre des Einzelnen festgemacht. Die juristische Entdeckung des Persönlichkeitsrechts wird allgemein auf den französischen Juristen Hugo Donellus (1527–1591) und seine Interpretation des römischrechtlichen Gebots des *alterum non laedere* (»Du sollst den anderen nicht schädigen«) als immateriellen Ehrschutz zurückgeführt. Damit war die konzeptionelle Basis für ein vom Individuum her gedachtes Abwehrrecht gegen Eingriffe in die Persönlichkeitssphäre gelegt.[4]

Gleichsam als entgegengesetzte Rechtsposition des Staates – modern gesprochen: als Eingriffsbefugnis – entstand die Vorstellung, dass der Zugriff auf Informationen über den Einzelnen ein hoheitliches Recht sei. Das Aufsichtsrecht des Staates (*ius inspectionis*)[5] wurde teilweise sogar als eine vierte Staatsgewalt (neben Gesetzgebung, Verwaltung und Rechtsprechung) begriffen, die damals noch nicht voneinander getrennt, sondern vielmehr in der Hand des Fürsten vereint waren.

Die einander gegenüberstehenden Rechtspositionen – Persönlichkeitsrecht des Einzelnen und Informationserhebungsbefugnis des Staates – sind der eigentliche Ursprung des modernen Datenschutz*rechts*. Allerdings war es – auch mangels Rechtsschutzmöglichkeiten des Einzelnen – nicht das individuelle Persönlichkeitsrecht, das die (wachsende) Datenmacht des Staates beschränkte, sondern zunächst die Binnenrationalität der Verwaltung. Die zunehmend notwendige Arbeitsteilung und Spezialisierung innerhalb der öffentlichen Hand machten es notwendig, dass bestimmte Informationserhebungen und -speicherungen einzelnen Behörden zugewiesen wurden. Nicht mehr jeder Teil des Staates erfuhr alles auf eine Person Bezogene, sondern nur der jeweils zuständige.

In einzelnen Teilbereichen lassen sich in Form staatlicher Verschwiegenheitspflichten aber auch spezifische Vorläufer des Datenschutzes als »informationelle Selbstbestimmung« feststellen.[6] So ist etwa das Postgeheimnis seit dem Ende des 17. Jahrhunderts bekannt, auch das Steuergeheimnis wurde vergleichsweise früh anerkannt. Allerdings waren diese ersten Datenschutzrechte weniger vom Persönlichkeitsschutz, sondern von staat-

lichen Interessen motiviert: Einer indiskreten Post werden keine Sendungen anvertraut und sie kann kein Porto einnehmen, einer geschwätzigen Steuerverwaltung werden möglicherweise abgabenrelevante Tatsachen verschwiegen.

Vor allem aber müssen für diese Zeit die faktischen Begrenzungen der Informationsverarbeitung berücksichtigt werden. Der Staat war nicht in der Lage, komplexere Datenbanken aufzubauen, die vielen lokalen und speziellen Datensammlungen standen unverbunden nebeneinander. Die rechte Hirnhälfte des »Großen Bruders«[7] wusste noch nicht, was in seiner linken Hirnhälfte abgespeichert war. Aber das Vernetzen der Informationen setzte bald ein, beispielsweise im Vormärz (circa 1815–1848), als die Polizeien der deutschen Staaten kooperierten, um »demokratische Umtriebe« zu kontrollieren.

2 Persönlichkeitsrecht als Freiheitsrecht

Im 19. Jahrhundert, ausgehend von der Anerkennung von Menschenrechten in der US-amerikanischen und der französischen Verfassung, brach sich allmählich die Vorstellung Bahn, dass dem Einzelnen Ansprüche nicht nur im Rahmen eines philosophischen Konzepts zukämen, sondern auch als Rechtspositionen. In den ersten modernen Verfassungen in Deutschland, die im Laufe des 19. Jahrhunderts entstanden, finden sich so auch Verbürgungen der Privatsphäre und der Vertraulichkeit. Genannt werden können hier vor allem der Schutz der Wohnung (vor Durchsuchungen) und das Briefgeheimnis. Von einer umfassenden und allgemeinen Anerkennung des Datenschutzes kann zu dieser Zeit allerdings nicht gesprochen werden.

In der zweiten Hälfte des 19. Jahrhunderts tauchte – einhergehend mit dem Aufkommen der (Massen-)Presse – ein zweiter Aspekt des heutigen Datenschutzes auf: der Schutz gegen informationelle Eingriffe durch Private. Die sensationslüsterne Berichterstattung über Personen in der Boulevardpresse wurde als Beeinträchtigung von deren Ehre begriffen. Auf dem Gebiet des Urheberschutzes sollten die wirtschaftlichen (Verwertungs-) Interessen der produktiven Persönlichkeit geschützt werden.

Gleichwohl entwickelte sich hieraus in Deutschland bis zur Mitte des 20. Jahrhunderts kein umfassender Persönlichkeitsrechtsschutz. Vor allem die insoweit anachronistische römischrechtliche Tradition des Bürgerlichen Gesetzbuchs (BGB) von 1900 verhinderte lange die Anerkennung eines umfassenden immateriellen Persönlichkeitsrechts. Gegen schwerwie-

gende Persönlichkeitsverletzungen konnte als eine Form der Ehrverletzung jedoch gerichtlich vorgegangen werden, und aufsehenerregende Aufnahmen des entstehenden Fotojournalismus – etwa von Bismarck auf dem Totenbett – führten in Deutschland zu partiellen gesetzlichen Regelungen wie dem Kunsturhebergesetz (KUG) von 1907.

Im Gegensatz hierzu wurde in den USA zu dieser Zeit das Konzept der *Privacy* (Privatheit) in einem umfassenden Sinne entwickelt. Maßgeblich hierfür war ein Aufsatz der Juristen Warren und Brandeis aus dem Jahre 1890, in dem diese ein »*Right to be let alone*« postulierten.[8] Allerdings ist diese amerikanische *Privacy* stark vom durch die eigenen vier Wände umgrenzten Raum gedacht und bezieht sich deshalb nicht auf die soziale Sphäre und den öffentlichen Raum.

3 Verstärkung der Datenmacht durch Informationstechnik

Im 20. Jahrhundert verstärkte sich die Datenmacht des Staates und zunehmend auch die von Unternehmen gegenüber dem Einzelnen. Zur Finanzierung neuer Staatsaufgaben, vor allem im Sozialbereich, griff und greift das Steuerwesen immer stärker auf personenbezogene Daten der Einzelnen zu (siehe auch den Beitrag von Polenz in diesem Band, S. 145 ff.). Möglich wurde dies durch neue Techniken der Informationsverarbeitung, etwa die seit Ende des 19. Jahrhunderts – zuerst in den Vereinigten Staaten – eingesetzten Lochkartenautomaten (Hollerith-Maschinen). Auch die Entwicklung von Leitz-Ordnern erleichterte das Anlegen geordneter Aktensammlungen, und strukturierte Karteisysteme lassen durch ihre Reiter und Lochungen bereits erste Ansätze automatisierter Verarbeitung erkennen.

Welches Missbrauchspotenzial die Datenmacht moderner Bürokratien haben kann, zeigte sich in der Zeit des Nationalsozialismus. Mit Hilfe der Melderegister konnte die planmäßige Vernichtung der jüdischen Bevölkerung vorbereitet werden; auch über andere Gruppen (etwa Homosexuelle) wurden Datenbanken angelegt und für deren Verfolgung genutzt. Überhaupt trieb der »totale Staat« die Verdatung voran, etwa mit der Einführung des Personalausweises (Kennkarte) oder dem – nicht mehr realisierten – Projekt einer nationalen Datenbank über alle Bürgerinnen und Bürger (»Deutscher Turm«)[9].

4 Technikgläubigkeit und Staatsskepsis

Die auch durch die Datenmacht des Staates in ihrem Ausmaß erst mögliche planmäßige und industrielle Vernichtung von Menschen im Nationalsozialismus hatte zunächst keine merkliche Auswirkung auf die allgemeine Beurteilung der (staatlichen) Datenverarbeitung. Vielmehr ist die Nachkriegszeit durch eine Technikgläubigkeit und einen Technikoptimismus gekennzeichnet. In den 1950er Jahren setzte die Verwaltungsautomatisierung ein, zuerst im Sozial- und Steuerwesen, nachdem erste elektronische Großrechenanlagen verfügbar waren. In den 1960er und 1970er Jahren verbreitete sich die Idee von der Planbarkeit gesellschaftlicher und wirtschaftlicher Entwicklungen, was eine entsprechende Datengrundlage voraussetzte. Der Datenhunger des Staates wuchs und wurde durch den Ausbau des Sozialstaates weiter vergrößert. Die Gliederung des Staates in verschiedene Verwaltungszweige und die föderale Schichtung Deutschlands wurde eher als Hindernis und noch nicht als (rechtsstaatliche) Sicherung der »informationellen Gewaltenteilung« empfunden.

Allmählich aber kam auch Skepsis auf. Insbesondere die 68er-Bewegung hegte Zweifel an der Gutartigkeit des Staates und der Herrschaft der Technokraten.[10] Vor allem die Sicherheitsbehörden wurden kritisch beäugt. Tatsächlich wurde als Reaktion auf die terroristischen Auswüchse der Oppositionsbewegung – insbesondere die Rote Armee Fraktion (RAF) – ein im demokratischen Deutschland bis dahin beispielloser Überwachungsapparat aufgebaut. Die ersten automatisierten Rasterfahndungen fanden in dieser Zeit statt und hatten auch Erfolg, indem man die Allgemeinheit flächendeckend auf bestimmte Merkmale (etwa kurzfristige Anmietung in anonymen Hochhauswohnungen, Barzahlung der Stromrechnung) durchkämmte.

5 Erste Datenschutzgesetze und Volkszählungsurteil

Das unterschwellige Unbehagen über die staatliche Datenmacht führte im Jahr 1970 zu den ersten Datenschutzgesetzen. Bemerkenswert ist allerdings, dass diese Regelungen nicht aufgrund eines schon artikulierten öffentlichen Drucks entstanden, sondern quasi vorauseilend geschaffen wurden.[11]

Der Ruhm der ersten gesetzlichen Regelung des Datenschutzes kommt dem hessischen Datenschutzgesetz von 1970 zu (siehe dazu auch den Beitrag von Bieber in diesem Band, S. 34 ff.). Als Gegen- und Tariergewicht zu der Zentralisierung der Datenverarbeitung im Lande (»Großer Hessen-

plan«) wurden erstmals Datenschutzregelungen geschaffen. Sie hatten zwar vornehmlich den Schutz der Datenverarbeitung vor unbefugten Eingriffen zum Gegenstand, fokussierten sich also nach heutiger Terminologie auf die Datensicherheit. Mit der Einführung eines (unabhängigen) Datenschutzbeauftragten wurde in diesem Zusammenhang aber eine bis heute für das deutsche Datenschutzrecht strukturprägende Institution geschaffen, die auch dem Schutz des Persönlichkeitsrechts des Einzelnen diente. Das hessische Gesetz führte vor allem den Begriff des Datenschutzes erstmals in die Gesetzessprache ein.

In den folgenden Jahren entstanden in weiteren Bundesländern Datenschutzgesetze, 1977 verabschiedete der Bund ein entsprechendes Gesetz. Dieses erste Bundesdatenschutzgesetz enthielt auch Regelungen für den Datenschutz in Unternehmen, was vor allem → Auskunfteien und Adresshandel betraf. In der Praxis spielten die Vorschriften zum Datenschutz im Privatsektor zunächst aber kaum eine Rolle, da die Regulierung in diesem Bereich – beispielsweise das heute noch bestehende sogenannte → Listenprivileg – eher zurückhaltend und zugleich das Datenverarbeitungspotenzial der Privaten aufgrund der teuren EDV-Anlagen noch beschränkt war.

In das allgemeine öffentliche Bewusstsein trat der Datenschutz erst mit dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983.[12] Hintergrund war ein allgemeiner Zensus, der – rückblickend im Verhältnis von Anlass und Ausmaß kaum mehr verständlich – die politische Auseinandersetzung hochkochen ließ; *Big Brother* schien ein Jahr vor dem symbolischen »1984« vor der Tür zu stehen.[13] In seiner nach wie vor wegweisenden Entscheidung schuf das Bundesverfassungsgericht aus der interpretierenden Zusammenschau des verfassungsrechtlich gewährleisteten Persönlichkeitsrechts (Artikel 2 Absatz 1 GG) und der Menschenwürde (Artikel 1 Absatz 1 GG) das »Recht auf informationelle Selbstbestimmung«.[14] Ausgehend von dem psychologischen Befund, dass der Mensch sich unter (potenzieller) Beobachtung befangen verhält (siehe auch den Beitrag von Trepte in diesem Band, S. 59 ff.), leitete es aus der Verfassung das Recht ab, dass jede Person grundsätzlich selbst über die Erhebung und Verwendung der auf sie bezogenen Daten entscheiden können müsse. Daraus folgerte das Gericht, dass alle (staatliche) Datenverarbeitung auf einer gesetzlichen Grundlage beruhen muss (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.).

In der Folge kam es zu zahlreichen gesetzlichen Regelungen, die für jeweils spezifische Bereiche die Datenverarbeitung durch die öffentliche Hand erlaubten. Das Volkszählungsurteil stieß damit jene aus heutiger

Sicht zu beklagende Entwicklung an, dass die gesetzlichen Regelungen über den Datenschutz unendlich zersplittert und nur noch mit Expertenwissen nachvollziehbar sind. Diese Unübersichtlichkeit der rechtlichen Grundlagen schadet dem Anliegen des Datenschutzes selbst: Sie ist *ein* Grund für die zahlreichen Wissenslücken vieler Menschen über das Datenschutzrecht und dessen nach wie vor teils mangelhafte Umsetzung.

6 Exkurs: Datenmacht in der DDR

Die teilweise hysterische, später dann feinziselierte Datenschutzdiskussion in der Bundesrepublik der 1980er Jahre überdeckt manchmal, dass auf der anderen Seite des »Eisernen Vorhangs« ein tatsächlicher Überwachungsstaat bestand. Die DDR hatte in Gestalt der Staatssicherheit (Stasi) einen Bespitzelungs- und Überwachungsapparat aufgebaut, der den der Nationalsozialisten in seiner Totalität übertraf, freilich aber »nur« für die politische Unterdrückung und nicht auch für die systematische Vernichtung von Menschen genutzt wurde. Allerdings konnte der ostdeutsche Überwachungsstaat Orwell'sche Ausmaße nicht (mehr) erreichen, insbesondere weil die Kapazitäten der Datenverarbeitung und -auswertung der Sicherheitsbehörden den anfallenden Informationsmengen nicht gewachsen waren. Die Staatssicherheit erstickte förmlich an ihren Daten.

Die Erfahrungen mit dem ostdeutschen Regime haben der Datenschutzdiskussion im wiedervereinigten Deutschland wichtige Impulse verliehen. Vor allem im Rahmen der Aufarbeitung der Stasi-Tätigkeit wurde die Bedeutung der staatlichen Datenmacht erkennbar. Viele Betroffene teilten die schmerzlich-resignierende Erfahrung der ostdeutschen Bürgerrechtlerin Bärbel Bohley (»Wir wollten Gerechtigkeit und bekamen den Rechtsstaat«), als sich frühere Täter gegen die Veröffentlichung ihrer Tätigkeit mit Hilfe des Datenschutzrechts wehren konnten.

7 Anwachsen unternehmerischer Datenmacht

Die großen Schlachten des Datenschutzes wurden also zunächst gegenüber dem datenmächtigen Staat geschlagen. Im Laufe der 1980er und 1990er Jahre traten jedoch zunehmend private Unternehmen als Datenverarbeiter auf die Bühne: Versicherungen bauten Warn- und Informationssysteme auf, die → SCHUFA und andere Kreditinformationssysteme erlangten eine zunehmende Bedeutung, die Arbeitgeberseite gewann durch Personal-

informationssysteme ein informationelles Übergewicht gegenüber den Beschäftigten. Die zunehmend personalisierte Werbung (Direktmarketing) wurde für viele zu einem lästigen Ärgernis.

Das Datenschutzrecht versuchte und versucht hier Regelungen zu finden, die die Interessen von Betroffenen und Datenverarbeitern zu einem Ausgleich bringen. Eine einseitige Betonung der Betroffeneninteressen ist dabei allerdings ausgeschlossen, weil auch die datenverarbeitenden Unternehmen dem Schutz der Verfassung unterliegen und sich auf ihre Berufs- und Handlungsfreiheit berufen können. Sie betrachten – immaterialgüterrechtlich auch nicht ganz zu Unrecht – die bei ihnen gespeicherten personenbezogenen Daten als ihr Eigentum.[15] Eine grundsätzliche Klärung des Verhältnisses zwischen dem Recht der Daten-»Besitzer« und dem Anspruch auf »informationelle Selbstbestimmung« der Betroffenen steht noch immer aus.

8 Internet und Datenschutz im Informationszeitalter

Seit Ende des letzten Jahrhunderts stellt das Internet den Datenschutz vor neue Herausforderungen. Das weltweite Netz hat die bisherige Konzeption des Datenschutzrechts mit seinen detaillierten Pflichten der verarbeitenden Stellen an Grenzen geführt (siehe auch den Beitrag von Roßnagel in diesem Band, S. 331 ff.). Zum einen setzt das herkömmliche Datenschutzrecht voraus, dass die datenverarbeitenden Stellen auch dem jeweiligen nationalen Recht unterliegen. Bei Datenverarbeitungen im Ausland ist das deutsche Datenschutzrecht nicht anwendbar, jedenfalls kaum effektiv durchsetzbar. Auch hat die allgemeine Verbreitung von Datenverarbeitungsmöglichkeiten die Zahl derjenigen, die Daten verarbeiten, potenziert. Der weltweite Zugriff auf personenbezogene Daten und deren problemlose (Weiter-)Verbreitung über das Internet lassen die überkommenen Regelungskonzepte (Meldepflichten, behördliche Aufsicht, betriebliche Datenschutzbeauftragte) weitgehend wirkungslos verpuffen.

Die neuartigen Verhaltensweisen in der Informationsgesellschaft führen außerdem zu neuen Gefährdungspotenzialen des Persönlichkeitsrechts. Das sogenannte → Web 2.0 mit seinen → Netzwerkplattformen (Soziale Netzwerke) lebt von der freiwilligen Preisgabe persönlicher Informationen (siehe auch den Beitrag von Schmidt in diesem Band, S. 215 ff.). Das herkömmliche Datenschutzrecht mit seinem Ideal der → Anonymität kann diesen Verhaltensweisen nicht mehr gerecht werden. Weitere Herausforderungen für den Datenschutz ergeben sich aus der zunehmenden Orts-

bezogenheit (mobiles Internet) und einer permanenten, allgegenwärtigen Datenverarbeitung (→ *Ubiquitous Computing*). Die Geräte dieser neuen Generation der Datenverarbeitung (etwa → *Smartphones*) erheben nicht mehr nur punktuell Daten, sondern generieren komplette Datenspuren, die über bisherige Grenzen der verschiedenen Lebensbereiche hinweg verknüpft werden können.

9 Datenschutz als Begrenzung von Machtungleichgewichten

Auch wenn es aus juristischer Perspektive meist so gesehen wird: Datenschutz ist nicht allein eine Frage der Grundrechte und damit ein individuelles Persönlichkeits- und Abwehrrecht gegenüber dem Staat. Datenschutz verfolgt vielmehr auch ein über-individuelles, strukturelles Ziel: die Begrenzung jener Machtungleichgewichte, die durch die Informationsballung bei einzelnen Akteuren bestehen.

Diese Aufgabe des Datenschutzes ist zudem keine statische. Vielmehr setzt der Datenschutz bei den veränderlichen kulturellen und sozialen Anschauungen über Privatheit an und muss auf den (informations-)technischen Wandel reagieren. Beides ist mit dem Eintritt in das Informationszeitalter stark in Bewegung geraten. Deshalb müssen nicht nur die Instrumente des Datenschutzes angepasst werden. Auch die sich wandelnde Einstellung der Gesellschaft zum Umgang mit personenbezogenen Daten ist bei einer neuen Konzeption des Datenschutzrechts zu berücksichtigen.

Wie unterschiedlich dabei der Schutz der Privatsphäre gedacht und konzipiert werden kann und mit welchem Grad an Veränderung, aber auch mit welchen Kontinuitäten in der Zukunft gerechnet werden muss, zeigt – wie in vielen anderen Bereichen auch – ein Blick in die Vergangenheit.

Anmerkungen

1 Guter Überblick bei Alfred Büllesbach/Hansjürgen Garstka, Meilensteine auf dem Weg zu einer datenschutzgerechten Gesellschaft, in: Computer und Recht (CR) 2005, S. 720 ff.

2 Kai v. Lewinski, Geschichte des Datenschutzrechts von 1600 bis 1977, in: Arndt u. a., Freiheit – Sicherheit – Öffentlichkeit, Baden-Baden 2009, S. 196 ff.

3 Allgemein zu Bürokratisierung des Staates Cornelia Vismann, Akten, Frankfurt/M. 2000.

4 Hierzu allgemein Klaus Martin, Das allgemeine Persönlichkeitsrecht in seiner historischen Entwicklung, Hamburg 2007.
5 Gisa Austermühle, Zur Entstehung und Entwicklung eines persönlichen Geheimsphärenschutzes vom Spätabsolutismus bis zur Gesetzgebung des Deutschen Reiches, Berlin 2002, S. 25 ff. et passim.
6 Umfassend dazu Wolfgang van Rienen, Frühformen des Datenschutzes?, Bonn 1984.
7 George Orwell, 1984, London 1949 (Originalausgabe). Der »Große Bruder« ist der Diktator im Staat »Ozeanien«, in dem eine absolute Kontrolle der Bevölkerung herrscht (Anm. d. Red.).
8 Samuel D. Warren/Louis D. Brandeis, The Right to Privacy, in: Harvard Law Review Bd. IV (Nr. 5/1890), im Internet unter http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (20.11.2011).
9 Götz Aly/Karl Heinz Roth, Restlose Erfassung, 2. Aufl., Frankfurt/M. 2000, S. 44–48.
10 Arthur R. Miller, The Assault on Privacy, Ann Arbor 1971 (dt.: Der Einbruch in die Privatsphäre, Neuwied 1973).
11 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD): Interviews zur Geschichte und Programmatik des Datenschutzes in Deutschland, im Internet unter https://www.datenschutzzentrum.de/interviews (20.11.2011).
12 BVerfGE 65, 1; Az. 1 BvR 209/83 u. a.
13 George Orwell, 1984. London 1949.
14 Wilhelm Steinmüller, Das informationelle Selbstbestimmungsrecht – Wie es entstand und was man daraus lernen kann, in: Recht der Datenverarbeitung (RDV) 2007, S. 158 ff.
15 Zur Kontroverse um die Eigentumsrechte an persönlichen Daten siehe den Beitrag von Papier in diesem Band, S. 67 ff.

Christoph Bieber

Datenschutz als politisches Thema – von der Volkszählung zur Piratenpartei

Der Beginn der politischen Themenkarriere des Datenschutz-Begriffs lässt sich recht deutlich auf die Debatten rund um die Volkszählung von 1987 zurückführen. Ursprünglich war diese umfassende Erhebung statistischer Bevölkerungsdaten bereits für 1983 vorgesehen, doch aufgrund massiver Proteste verzögerte sich das Verfahren um mehrere Jahre. Eine wesentliche Folge dieser Auseinandersetzung war die umfassende Neuregelung der rechtlichen Rahmenbedingungen – als Folge der Volkszählungskontroverse entstand der Begriff der »informationellen Selbstbestimmung« (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.). Auch danach wurden zahlreiche Datenschutzdebatten als Kontroversen geführt, die bisweilen erstaunliche Ähnlichkeiten aufweisen. Die aktuelle Konjunktur des Themas zeigt sich an Beispielen wie der Debatte zum → *Street View*-Projekt der US-Firma *Google* oder dem öffentlichen Umgang mit den Enthüllungen auf der Informationsplattform → *WikiLeaks*.

Der nachfolgende Beitrag skizziert kurz die Geschichte der politischen Datenschutzdebatten in Deutschland, benennt die wichtigsten Akteure und arbeitet wiederkehrende Merkmale der politischen Verarbeitung solcher Konflikte durch Parteien und Parlamente heraus. Abschließend werden aktuelle Entwicklungen wie die Debatte um die Einführung von »Internetsperren« sowie die damit verbundene Entstehung der Piratenpartei skizziert.

1 Die Ursprünge des Datenschutz-Begriffs

Datenschutz beschäftigt – nicht nur – die deutsche Politik bereits über einen längeren Zeitraum als gemeinhin angenommen. Die Verabschiedung des ersten Datenschutzgesetzes datiert zurück auf den 7. Oktober 1970: In Wiesbaden trat mit dem »Hessischen Landesdatenschutzgesetz« die erste Regelsammlung dieser Art in Kraft (siehe hierzu auch den Beitrag von Lewinski in diesem Band, S. 23 ff.). Gut eineinhalb Jahre später gab der erste Tätigkeitsbericht des Datenschutzbeauftragten Aufschluss über die Inhalte der Arbeit auf einem damals noch unbestellten Politikfeld. Das gleiche Thema

sorgt vier Jahrzehnte später regelmäßig für Ratlosigkeit, Irritation und hektische Aktivität auf unterschiedlichen administrativen Ebenen. Der SPD-Politiker Willi Birkelbach wurde am 8. Juni 1971 von der hessischen Landesregierung zum Datenschutzbeauftragten ernannt und hatte Pionierarbeit zu leisten.[1]

Die Entwicklung eines Datenschutzgesetzes und die Schaffung einer formalisierten Verwaltungsstruktur ist als Reaktion auf die allmähliche Nutzung von Computern in der öffentlichen Verwaltung zu verstehen. Die wesentliche Regelungsperspektive war zunächst jedoch ein Ausgleich zwischen Exekutive und Legislative. Die einzelnen Bürgerinnen und Bürger spielten in diesem Prozess zwar durchaus eine Rolle, jedoch eher als Objekte einer mit den Mitteln der »elektronischen Datenverarbeitung« arbeitenden Verwaltung und weniger als Subjekte, die zu einem selbstständigen politischen Handeln gegenüber behördlichen Akteuren in der Lage seien.[2]

Nichtsdestotrotz war bereits in den frühen Grundlagendokumenten das Bewusstsein für die Notwendigkeit des Schutzes einzelner Bürgerinnen und Bürger vor einem tendenziell allwissenden Verwaltungsapparat erkennbar, ebenso wurde häufig auch ein individuelles »Recht auf Privatheit« dargelegt. Wie das hessische Beispiel zeigt, haben die damals verwendeten Formulierungen ihre Gültigkeit bis heute behalten und dokumentieren eine erstaunlich kohärente Entwicklung der Datenschutz-Thematik im politischen Kontext.[3]

Auszug aus dem Ersten Tätigkeitsbericht des Hessischen Datenschutzbeauftragten 1972[4]

»Dem einzelnen (muss) um der freien und selbstverantwortlichen Erhaltung seiner Persönlichkeit willen ein ›Innenraum‹ verbleiben (…), in dem er ›sich selbst‹ besitzt und in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt.«

Nach der hessischen Initialzündung folgte in den 1970er Jahren auf dem Gebiet der Bundesrepublik der flächendeckende Ausbau einer Datenschutzgesetzgebung auf Landes- wie auf Bundesebene. Die Verabschiedung des ersten Bundesdatenschutzgesetzes (BDSG) am 27. Januar 1977 sowie die Ernennung des ersten Bundesdatenschutzbeauftragten Hans-Peter Bull am 14. Februar 1978 markierten hier die wesentlichen Meilensteine für die Verankerung der Thematik innerhalb des politischen Systems.[5]

Die formale Etablierung von Datenschutzgesetzgebungen verlief demnach vor allem innerhalb der politischen Institutionen und sorgte neben der grundsätzlichen politisch-juristischen Erschließung des Themenfeldes auch für einen Ausgleich innerhalb des politischen Systems. Die Figur des Datenschutzbeauftragten ist in dieser Zeit stark durch Kontroll-, Beratungs- und Vermittlungstätigkeiten innerhalb des Verwaltungsapparates geprägt. Die ebenfalls vorhandene »Ombudsman-Aufgabe« als Ansprechperson für die Bevölkerung wurde zwar genutzt. Aufgrund der noch nicht allzu weit verbreiteten Praxis der elektronischen Datenverarbeitung war die Thematik aber nur für einen kleinen Teil der Öffentlichkeit präsent.[6]

2 Volkszählungsprotest und informationelle Selbstbestimmung

Einen wesentlichen Entwicklungsschub und eine »Popularisierung« erfuhr die Datenschutzgesetzgebung während der Volkszählungs-Boykotte (»VoBos«) in den 1980er Jahren – von diesem Zeitpunkt an rückten die Bürgerinnen und Bürger als politische Subjekte in den Mittelpunkt der Datenschutz-Kontroversen. Zur Aktualisierung der bereits lange veralteten statistischen Datenbestände war 1982 im Bundestag die Durchführung einer umfassenden Volkszählung beschlossen worden, wobei erstmalig Daten im großen Maßstab zur maschinellen Weiterverarbeitung durch Behördenapparate erhoben werden sollten. Doch dieser Zensus stand unter keinem guten Stern – in die Zeit der Vorbereitung der Datenerhebung fielen zunächst das Misstrauensvotum gegen Helmut Schmidt, Neuwahlen und der Wechsel zur christlich-liberalen Regierung unter Helmut Kohl. Zudem meldeten sich zahlreiche Protestgruppen zu Wort, die schließlich eine Verschiebung der Volkszählung um vier Jahre bewirkten.

Begünstigt wurden die Proteste durch ein aktives »Bewegungsmilieu« im Umfeld der Neuen Sozialen Bewegungen sowie der 1983 in den Bundestag eingezogenen Partei Die Grünen.[7] In inhaltlicher Hinsicht spielte das Aufkommen der ersten Heimcomputer zur gleichen Zeit eine wichtige Rolle – bis dahin wurde die »elektronische Datenverarbeitung« in Rechenzentren und mittels technisch limitierter Eingabegeräte (»Terminals«) vollzogen. Erst für wenige Menschen war die neue Technologie auch im Alltag sichtbar. Neben der allmählichen »Computerisierung« der Lebenswelt hatten die raschen Entwicklungssprünge zu Überarbeitungsbedarf bei den Datenschutzgesetzen geführt – die wachsende Aktivität des Gesetzgebers begünstigte die Wahrnehmung einer Front-

stellung zwischen »Datenschutz-Aktivisten« und staatlichen Akteuren. Nicht zuletzt sorgte die Verschärfung staatlicher Sicherheits- und Überwachungsansprüche nach den Erfahrungen der RAF-Morde im »Deutschen Herbst« von 1977 für Widerstände gegen eine massenhafte elektronische Datenerhebung.[8]

Das Resultat war schließlich eine breit ausgetragene Kontroverse, in deren Kern die Frage nach der Verletzung von Persönlichkeitsrechten aufgrund des staatlichen Informationsbedarfs stand. Deutlicher formuliert: Verletzt die Erhebung der für die Volkszählung benötigten Daten die Privatsphäre? Und legen staatliche Stellen dabei die nötige Sorgfalt im Umgang mit den Daten an den Tag? Die in den frühen 1980er Jahren herrschende Protestkonjunktur wurde belebt durch ein Netzwerk von »Bewegungsakteuren«, das sowohl Politikerinnen und Politiker (vor allem aus den Reihen der Grünen, aber auch in den übrigen Parteien erhoben sich kritische Stimmen), Fachleute (aus Verwaltungswissenschaft, Informatik und Rechtswissenschaft) sowie Bürgerinitiativen umfasste. Dabei meldete sich auch der 1981 gegründete Chaos Computer Club als zivilgesellschaftlicher Akteur zu Wort.[9]

Mit der Verlagerung der Debatte aus den abstrakten und unpersönlichen Verwaltungsverfahren hatte der Datenschutz als politisches Thema mehr als zehn Jahre nach Verabschiedung des ersten Datenschutzgesetzes die breite Bevölkerung erreicht. Im Mittelpunkt stand dabei der Rückzugsraum für Individuen, in den auch der Staat keine – oder zumindest nur eine klar begrenzte – Einsicht nehmen durfte. Wie sich auch anhand späterer Kontroversen zeigt, entstehen öffentliche Debatten um Datenschutz-Fragen erst in der Verbindung mit konkreten Bereichen der Lebenswelt – dieses Muster war bereits in den Volkszählungskontroversen angelegt.

Mit dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983[10] wurde das Verfahren zunächst ausgesetzt und auf 1986 verschoben, aufgrund organisatorischer Probleme ergab sich eine zusätzliche Verlegung auf den 25. Mai 1987. Die Karlsruher Entscheidung (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.) markierte zudem einen gravierenden Einschnitt für die Datenschutzgesetzgebung, denn das Urteil formulierte ein Grundrecht auf »informationelle Selbstbestimmung«[11]. Einer der Schlüsselsätze des Urteils bestätigte die Volkszählungsgegner und behält auch in Zeiten der Kommunikation in weltweiten Computernetzen seine Gültigkeit: »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.«[12]

3 Neue Anforderungen durch Computernetze

Auf die Zäsur des Volkszählungsurteils folgte die allmähliche Ausformung des Begriffs der informationellen Selbstbestimmung. Zunächst blieb die verfassungsrechtliche »Feststellung« eines neuen Grundrechts für weite Teile der Bevölkerung ohne große Relevanz. Nichtsdestotrotz ist die Phase nach dem Volkszählungsurteil gekennzeichnet von den Anpassungen und Überarbeitungen gesetzlicher Regelungen sowie von einer allmählichen Ausweitung datenschutzbezogener Staatstätigkeit. Mit Blick auf konkrete politische Auseinandersetzungen ist allerdings eine »Institutionalisierung« der Thematik zu konstatieren. Es sind die Parteien oder einzelne Politikerinnen und Politiker, die mit konkreten Vorschlägen für neue Datenschutz-Debatten sorgen, deren wesentlicher Austragungsort das Parlament ist – und nicht die »Straße«, wie im Falle der Volkszählungs-Boykotte. Im Vordergrund stehen dabei häufig Fragen, die sich an der Umsetzung computergestützter Ermittlungs- oder Überwachungsvorhaben orientieren.[13]

Der fortschreitende Bedeutungszuwachs von Computern in der Arbeitswelt, im Gesundheitswesen sowie die Nutzung zu Geschäfts- und Unterhaltungszwecken beförderte Informationstechnologien ans Licht der Öffentlichkeit. Eine erhebliche Rolle spielte dabei die Entstehung von Computernetzen, seit Mitte der 1990er Jahre veranschaulicht durch das Aufkommen des *World Wide Web* als sichtbare und für viele Menschen zugängliche Benutzeroberfläche des Internets.

Die Veränderung der technologischen Konstellation – vernetzte Computer statt Einzelplatzrechner oder Heimcomputer – wirft neue Datenschutzfragen auf. Schon zu Beginn der 1970er Jahre lieferte die Digitalisierung und Zusammenlegung von Registern und Datenbanken Impulse für die Entwicklung eines neuen Rechtsrahmens für den Umgang mit Informationen. Durch den globalen Siegeszug des Internets war diese Vernetzung zu einer Konstante bei der Computernutzung geworden, zudem entstanden bei immer neuen Aktivitäten in verschiedenen Lebensbereichen computerisierte, oft personenbezogene Daten. Die daraus resultierende Denkfigur der allgegenwärtigen Computernutzung (→ *Ubiquitous Computing*) stellte Datenschützer vor neue Herausforderungen.[14]

In diesem Zeitraum ist auch die Internationalisierung der Datenschutzpolitik (siehe auch die Beiträge von Hijmans/Langfeldt, S. 403 ff., und Körner, S. 426 ff., in diesem Band) zu verorten. Die Europäische Datenschutzrichtlinie von 1995 ist dabei lediglich der Ausgangspunkt für eine Harmonisierung der Vorschriften innerhalb der Mitgliedsstaaten – Konflikte mit großer Breitenwirkung entstanden dadurch nicht, allenfalls setz-

ten sich »Datenschutz-Eliten« mit den jeweiligen Folgen für die nationale Gesetzgebung auseinander. Besondere Kristallisationspunkte für »Datenschutzkontroversen« lieferten Abkommen auf internationaler Ebene wie etwa das EUROPOL-Informationssystem zur Weitergabe von Daten im Kampf gegen die organisierte Kriminalität oder das →Swift-Abkommen zum Austausch von Bankdaten.

Allerdings verblieben die Konfliktpotenziale in diesen Fällen auf der Institutionenebene; ein allgemeiner, breitenwirksamer Politisierungseffekt wie anlässlich der Volkszählungsboykotte wurde längst nicht erreicht. Auch die politischen Parteien nutzten diese Debatten kaum zu einer offensiven Positionierung in Sachen Datenschutz – die Thematik wurde innerhalb der üblichen programmatischen Ausrichtung als Teil der Innen- und Sicherheitspolitik verortet oder mit Verweis auf den Grundrechtsstatus der informationellen Selbstbestimmung als Gegenstand individueller bürgerlicher Freiheiten erwähnt.[15]

4 Internetsperren und die Entstehung der Piratenpartei

Dies änderte sich erst mit der Etablierung des Internets als Massenmedium um den Jahrtausendwechsel. An der Entstehung der Piratenpartei zeigen sich nun einige Parallelen zu den Volkszählungsboykotten der 1980er Jahre. Einerseits bildeten Organisationsformen und individuelle Aktivitäten jenseits der etablierten Parteien einen wichtigen Nährboden für ein politisches Engagement (Protestkultur), andererseits war die *Online*-Nutzung für viele Menschen zur Normalität geworden (Computerisierung). Diese Konstellation begünstigte erneut die Entstehung breiter Bürgerproteste gegen eine durch das politische System angestrebte Entscheidung im Themenbereich von Datenschutz und Informationsfreiheit.

Den konkreten Ansatzpunkt lieferte dabei jedoch kein Verfahren zur massenhaften Erhebung und Speicherung von Daten, sondern – ganz im Gegenteil – die staatlichen Versuche zu Kontrolle und Blockade *online* verfügbarer Informationen. Geburtshelfer einer neuen datenschutzorientierten Bürgerbewegung war das Anfang 2009 von der damaligen Bundesfamilienministerin Ursula von der Leyen (CDU) protegierte »Gesetz zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen«.[16]

Wie schon in den 1980er Jahren reagierte hier ein durch gesetzgeberische Aktivitäten aufgeschrecktes »Bewegungsmilieu«. Waren die damaligen »VoBo«-Gruppierungen noch auf analoge Koordination und

Kooperation angewiesen, so nutzten die Akteure im Umfeld der sogenannten »Zensursula«-Kampagne[17] die Möglichkeiten einer inzwischen vorhandenen interaktiven Kommunikationsumgebung aus. Das Resultat war ein enorm beschleunigter Verlauf der Datenschutzproteste. Kennzeichnend für die strukturelle Ähnlichkeit der gut drei Jahrzehnte auseinander liegenden Ereignisse ist aber die über unterschiedliche Einheiten verteilte Akteursstruktur, die sich in einer Vielzahl von individuell oder kollektiv verfassten Protestbeiträgen manifestierte.

Auch in Bezug auf die Kopplung an einen klassischen Akteur des politischen Systems bestehen Ähnlichkeiten: Lieferten bei den Volkszählungsboykotten Die Grünen als neue Parteiorganisation den Verbindungspunkt an parlamentarische Strukturen, so fungierte nun die ebenfalls noch junge Piratenpartei als Schnittstelle zum politischen System. Während allerdings Die Grünen zur Hochzeit der Volkszählungs-Proteste bereits den Einzug in den Bundestag realisiert hatten, durchläuft die Piratenpartei noch ihre Findungsphase. Auf ihre kaum beachtete Gründung (2006) folgte mit dem immensen Mitgliederzuwachs im Superwahljahr 2009 eine Etablierung als sichtbare Kleinpartei.[18] Die Ausrichtung auf Datenschutz und Informationsfreiheit war insbesondere in den frühen Programmentwürfen ersichtlich.[19] Nach den ersten Erfolgen bei Europa- und Bundestagswahl 2009 als »Ein-Themen-Partei« ist inzwischen eine Ausweitung der programmatischen Ausrichtung zu erkennen.[20] Im Jahr 2011 gelang der Piratenpartei der Einzug in das Berliner Abgeordnetenhaus, wo sie beweisen muss, ob sie sich zu weiteren Themen positionieren kann. 2012 erfolgte dann der Einzug in weitere Landesparlamente.

Nichtsdestotrotz stellt die Piratenpartei einen wichtigen Faktor für die aktuelle Popularisierung des Themas »Datenschutz« innerhalb des politischen Systems dar. Die allmähliche Ausdifferenzierung der konkreten Ansatzpunkte und Regelungsnotwendigkeiten von Datenschutzfragen hat – im Verbund mit dem allgemeinen Bedeutungsgewinn computerbasierter Kommunikation – zur Entwicklung des Politikfeldes »Netzpolitik« geführt.[21] Innerhalb dieses Themenkomplexes spielen Fragen des Schutzes personenbezogener Daten gegenüber staatlichen Stellen eine wichtige Rolle, unter den Bedingungen des → *Social Web* ist darüber hinaus das Grundrecht auf informationelle Selbstbestimmung zum wichtigen Faktor geworden. In Zeiten, in denen auf der eigenen Homepage, in sozialen Netzwerken oder mit den Mitteln der Echtzeitkommunikation beinahe jede Person einen aktiven Beitrag zur Gestaltung politischer Öffentlichkeiten leisten kann, spielen Medienkompetenz und das Verständnis der Konzepte von Datenschutz und (auch im analogen Leben garantierter) Privatheit eine wesentliche Rolle.

5 Bedeutungszuwachs der Thematik schafft Modernisierungsdruck

Die politische Geschichte des Datenschutzes nahm ihren Anfang in der zunächst verwaltungstechnisch begründeten Verabschiedung von Datenschutzgesetzen in den 1970er Jahren. Die erste »echte« Politisierung erfolgte in den massiven Datenschutzkonflikten um die Volkszählung von 1987. Die 1990er Jahre waren von der schrittweisen Präzisierung und Internationalisierung des gesetzlichen Rahmens bestimmt. Zugleich führte die weltweite Ausbreitung computerbasierter Kommunikation zu neuen Aufgabenbereichen für den Datenschutz und einem Perspektivwechsel.

Künftige Datenschutzkontroversen werden vor allem entlang der veränderten Kommunikationssituationen in Computernetzwerken geführt. Die unter dem Begriff → Web 2.0 zusammengefassten Entwicklungen von sozialen Netzwerken als zentralem Element der *Online*-Kommunikation, der mobilen, beschleunigten Datenübertragung und die Angebote ortsbezogener Dienstleistungen stellen dabei große Herausforderungen für die Modernisierung bestehender Datenschutzgesetze dar (siehe auch den Beitrag von Roßnagel in diesem Band, S. 331 ff.).

Die damit verbundene Ausweitung der Aufgabenbereiche für die politischen Institutionen des Datenschutzes hat in Deutschland bisher zu zahlreichen Aktivitäten von Regierungsbehörden geführt, die noch keine schlüssige Aufgabenverteilung erkennen lassen. Allein im Jahr 2010 haben das Innen-, Familien-, Verbraucher- und Wirtschaftsministerium Diskussionen im Bereich Datenschutz angestoßen, ohne dass dabei ein koordiniertes Vorgehen erkennbar gewesen wäre. Auf der föderalen Ebene war die hochgradig kontroverse Debatte um die Verabschiedung des Jugendmedienschutz-Staatsvertrages (JMStV) ein weiterer Schauplatz für politische Aushandlungsprozesse mit unklarem Ausgang, komplexer Beteiligungsstruktur und hohem Protest- und Konfliktpotenzial.

Darüber hinaus eröffnen immer häufiger externe Impulse neue Datenschutz-Kontroversen unter politischen Akteuren, was den Bedeutungszuwachs der Thematik unterstreicht: dazu zählen der intransparente Umgang mit personenbezogenen Daten durch international agierende Unternehmen wie *Facebook* oder die massenhafte Erhebung neuartigen Datenmaterials im Zuge des → *Google Street View*-Projektes. Schließlich haben auch die weltweit beachteten Veröffentlichungen der »Enthüllungs-Plattform« → *WikiLeaks* dazu beigetragen, den Umgang mit digitalisierten Daten als politisch brisantes Thema zu erkennen. Anhand solcher Beispiele deutet sich der außer-

ordentliche Modernisierungsdruck für aktuelle Regelwerke an. Dies gilt sowohl mit Blick auf Datenschutzaspekte, vor allem aber auch für das Grundrecht der informationellen Selbstbestimmung. Künftige Kontroversen dürften sich eher entlang des Begriffs der Informationsfreiheit entfalten, auch weil für immer mehr Menschen der Umgang mit Daten zu einer aktiven, produktiven Tätigkeit geworden ist und Datenschutzfragen die Bürgerinnen und Bürger längst nicht mehr nur im Umfeld von Verwaltungsverfahren erreichen.

Anmerkungen

1 Gut dokumentiert sind die Materialien auf den Seiten des »Zentralarchivs für Tätigkeitsberichte des Bundes- und der Landesdatenschutzbeauftragten und der Aufsichtsbehörden für den Datenschutz« (ZAfTDa), im Internet unter http://www.fh-giessen-friedberg.de/zaftda.
Der ausgebildete Kaufmann Birkelbach übernahm das Amt gewissermaßen aus einer »fachfremden« Perspektive. Sein heutiger Amtsnachfolger Michael Ronellenfitsch weist als Verwaltungsjurist ein typischeres Profil auf. Ein Blick in den ersten Tätigkeitsbericht ist auch insofern hilfreich, weil hier eine ausführliche Bestandsaufnahme der Überlegungen in anderen Bundesländern, auf Bundesebene sowie im internationalen Vergleich vorgenommen wird und sich daraus ein frühes, sehr detailliertes Porträt zur Datenschutzgesetzgebung ergibt. Darüber hinaus gilt das hessische Gesetz von 1970 als weltweit erste formelle Niederlegung von Regelungen zum Datenschutz (vgl. Alexander Genz, Datenschutz in Europa und den USA, Wiesbaden 2004).

2 Die möglichen Folgen einer Computerisierung der öffentlichen Verwaltung wurden bereits in den frühen 1970er Jahren auch hinsichtlich ihrer Wirkungen auf andere Gesellschaftsbereiche diskutiert. So kann die Darstellung der »Computer-Demokratie« (s. Helmut Krauch, Computer-Demokratie. Düsseldorf 1972) als früher Vorläufer der US-amerikanischen »Teledemocracy« aus den 1980er Jahren sowie der seit den 1990er Jahren populären »Cyberdemocracy« gelten.

3 Der hier skizzierte »persönliche Rückzugsraum« steht auch in den Debatten um den Begriff der »Post-Privacy« bzw. »Post-Privatheit« im Mittelpunkt. Allerdings bildet nun die Annahme, dass im Zuge der Bedeutungsverschiebung von Öffentlichkeit und Privatheit unter den Bedingungen digitaler, interaktiver Medien ein solches Refugium nicht mehr realisierbar sei, einen radikal formulierten Ausgangspunkt für künftige Datenschutzkontroversen (vgl. Abschnitt 5 dieses Beitrags).

4 Hessischer Datenschutzbeauftragter, Erster Tätigkeitsbericht, LT-Drs. 7/1495 vom 29.3.1972, Wiesbaden, S. 9 m. w. N.

5 Vgl. dazu ausführlich: Marie-Theres Tinnefeld/Eugen Ehmann/Rainer W. Gerling, Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in euro-

päischer Sicht, München 2011, S. 250 ff.; sowie Bundesbeauftragter für den Datenschutz, Tätigkeitsbericht, BT-Drs. 8/2460 vom 10.1.1979, Bonn.

6 Vgl. Bundesbeauftragter für den Datenschutz 1979 (Anm. 5), S. 5 f.

7 Vgl. Nicole Bergmann, Volkszählung und Datenschutz. Proteste zur Volkszählung 1983 und 1987 in der Bundesrepublik Deutschland, Hamburg 2009, S. 17.

8 Die Erfahrung des RAF-Terrorismus und der daraus folgende Ausbau staatlicher Sicherheitsstrukturen ähneln durchaus den US-amerikanischen Maßnahmen nach den Anschlägen vom 11. September 2001 – auch wenn in der Bundesrepublik keine zentrale »Heimatschutzbehörde« mit weit in die Privatsphäre hinein reichenden Befugnissen etabliert wurde.

9 Vgl. dazu ausführlich Bergmann 2009 (Anm. 7), a. a. O., S. 32 f. Interessant ist in der Rückschau auch die Rhetorik des Widerstands. So nannte sich beispielsweise eine lokale Hamburger Widerstandsgruppe »Datenpiraten« (s. »Datenschrott für eine Milliarde?«, in: Der Spiegel vom 16.3.1987, S. 30–52 [35], im Internet unter http://www.spiegel.de/spiegel/print/d-13522320.html).

10 BVerfGE 65, 1; Az. 1 BvR 209, 269, 362, 420, 440, 484/83.

11 Vgl. Hansjürgen Garstka, Informationelle Selbstbestimmung und Datenschutz. Das Recht auf Privatsphäre, in: Christiane Schulzki-Haddouti (Hrsg.), Bürgerrechte im Netz, Bonn 2003, S. 48–70, sowie den Beitrag von Papier in diesem Band, S. 67 ff.

12 BVerfGE 65, 1; Az. 1 BvR u. a., Rn. 155.

13 Thematische Ansatzpunkte sind z. B. verschiedene Überwachungstechnologien, die Diskussion um den »Großen Lauschangriff«, computerbezogene Kriminaldelikte (»Cyber-Crimes«) oder *Online*-Durchsuchungen. Im Rahmen des vorliegenden Beitrags können diese Aspekte jedoch nicht näher diskutiert werden, der Schwerpunkt liegt auf jenen Datenschutzkontroversen, die eine große öffentliche Reichweite erzielt und politische Beteiligungsprozesse ausgelöst haben.

14 Vgl. Alexander Roßnagel, Datenschutz im 21. Jahrhundert, in: Aus Politik und Zeitgeschichte, Nr. 5–6/2006, S. 9–15, im Internet unter http://www.bpb.de/publikationen/9GGQGR,0,Datenschutz_im_21_Jahrhundert.html.

15 In den programmatischen Entwicklungsprozessen der Parteien ist allerdings ein langsamer Bedeutungszuwachs der Thematik zu erkennen. Sämtliche Grundsatzprogramme, die seit den 1990er Jahren beschlossen wurden, enthalten Passagen zur Informationsgesellschaft. Dabei werden auch die Bereiche des Datenschutzes berührt, allerdings nehmen diese Abschnitte keinen großen Raum ein und werden auch nicht an prominenter Stelle behandelt. Der Begriff der »informationellen Selbstbestimmung« findet sich einzig im Grundsatzprogramm von 2002 der Partei Bündnis 90/Die Grünen.

16 Vgl. dazu ausführlich Christoph Bieber, NoBailout und Zensursula. *Online*-Kampagnen in der Referendums-Demokratie, in: Klaus Kamps/Heike Scholten/Guido Schommer/Ingo Seeligmüller (Hrsg.), Politische Kampagnen in der Referendums-Demokratie, Wiesbaden i. E.

17 Unter diesem Etikett werden die unterschiedlichen *Online*-Aktivitäten der Gegner des Zugangserschwerungsgesetzes zusammengefasst, dazu zählten verschiedene

Webseiten mit Informationen zur Gesetzesinitiative, *Facebook*-Aktivitäten oder auch die massenhafte Beteiligung an einer *Online*-Petition beim deutschen Bundestag. Als visuelles Signet diente ein digital bearbeitetes Portraitfoto von Ursula von der Leyen, das mit einem »Zensursula«-Schriftzug versehen war (vgl. dazu ausführlich Bieber 2012, Anm. 16). Das Rauten-Symbol findet im Rahmen der *Twitter*-Kommunikation Verwendung und dient dabei zur Markierung bzw. Indizierung bestimmter Inhalte.

18 Vgl. dazu ausführlich Christoph Bieber, Der Wahlkampf als Onlinespiel. Die Piratenpartei als Innovationsträger im Bundestagswahlkampf 2009, in: Martin Eifert/Wolfgang Hoffmann-Riehm (Hrsg.), Innovation, Recht, öffentliche Kommunikation. Baden-Baden 2010, S. 233–254.

19 Das Programm der Piratenpartei ist im »Piratenwiki« einsehbar (vgl. http://wiki.piratenpartei.de/Parteiprogramm), die entsprechenden Absätze zu »Privatsphäre und Datenschutz« finden sich in Abschnitt 3. Konsequenter Weise beteiligt sich die Piratenpartei selbst auch an Kampagnen gegen die für 2011 geplante Volkszählung (vgl. http://wiki.piratenpartei.de/Volkszählung).

20 Vgl. hierzu die Beschlüsse der Landesmitgliederversammlung vom 23./24.10.2010 in Berlin zur Überarbeitung des Grundsatzprogramms, im Internet unter http://wiki.piratenpartei.de/BE:Parteitag/2010.2/Beschlüsse/Grundsatzprogramm_Bausteine.

21 Vgl. ausführlich Bieber 2010 (Anm. 18) und Bieber 2012 (Anm. 16).

Franziska Heine

Mobilisierung und politischer Protest im Internet

Es ist ungemütlich draußen, kalt und windig. Hier und da kommen Regentropfen vom Himmel. Seit drei Tagen berichtet das Radio von Blockaden und Polizeieinsätzen im Zusammenhang mit den Castor-Transporten. Das Radio? Nein, das Internet. »Radio Freies Wendland« sendet fast ausschließlich im Netz. Auf einer Wiese in Dannenberg steht die Sendezentrale. Das Internet ist der Dreh- und Angelpunkt für aktuelle Informationen. Kein anderes Medium kann eine so hohe Informationsdichte liefern. Ein Castor-Ticker gibt in Form von Kurznachrichten die neuesten Geschehnisse auf einer Webseite wieder. Daneben wird das Internet-Radio genutzt, um die Proteste zu koordinieren. Das Netz ermöglicht den Protestierenden die Unabhängigkeit von Massenmedien. Noch nie konnte ihre Botschaft so viele Menschen erreichen wie in den letzten Jahren.

Durch das Netz scheint der Erfolg von David gegen Goliath nicht mehr unmöglich zu sein. Doch welche Potenziale bietet das Netz wirklich, um auf politische Entscheidungen Einfluss zu nehmen? Und was macht erfolgreiche Netzkampagnen aus?

1 Das Zugangserschwerungsgesetz

Das Netz ist eine Transparenzmaschine. Sie zeigt den Polizisten, der die Kontrolle verliert, ebenso wie den Protestierenden, der Steine schmeißt. Auch die abgeschottete parlamentarische Demokratie wird durchsichtig, wenn Bürgerinnen und Bürger bei öffentlichen Ausschusssitzungen präsent sind, das Geschehen kommentieren und im Netz sichtbar machen.

Das musste die Bundesministerin für Familie, Senioren, Frauen und Jugend, Ursula von der Leyen, im Jahr 2009 schmerzlich erfahren. Sie schlug die Einrichtung sogenannter Netzsperren vor, um den sexuellen Missbrauch von Kindern und Jugendlichen zu bekämpfen, und erntete eine Welle der Empörung. Nach ihrem Vorschlag sollte das Bundeskriminalamt (BKA) Adresslisten von jenen Webseiten erstellen, auf denen sich kinderpornografische Abbildungen finden. Diese Listen würden an die Internet-Service-Provider übermittelt, die beim Aufruf der entsprechenden

Internetadressen (→ URL) ein Stoppschild präsentieren und den Zugang zu den Seiten versperren sollten. Zudem sollten die Verbindungsdaten (→ IP-Adressen) jener Nutzenden gespeichert werden, die versuchen, auf Webseiten der Sperrliste zuzugreifen. Dem Gesetzentwurf zufolge spielte es dabei keine Rolle, wie die Nutzenden auf die gesperrte Webseite gelangten – ob bewusst, aus Unwissenheit oder als Folge einer Täuschung.

2 Erfolgreiche Kampagnen benötigen ein breites Netzwerk

Die Initiative gegen die Netzsperren begann mit einer Frage beim Kurznachrichtendienst → *Twitter.* Sie lautete sinngemäß: Wollen wir einfach zwei Monate wegen des Gesetzes jammern oder wirklich etwas dagegen unternehmen? Die Antworten zeugten einerseits von Frustration über die realitätsferne Netzpolitik, enthielten aber auch den Vorschlag, es mit einer *Online*-Petition zu versuchen. Gesagt, getan. Nachdem die Petition zum Mitzeichnen freigeschaltet wurde, war wiederum *Twitter* der erste Verbreitungskanal. Der Link zur Petition wurde weitergegeben, mit der Aufforderung dort mitzuzeichnen. Gleichzeitig waren sehr schnell Organisationen bereit, die Kampagne zu unterstützen. Fachleute aus den unterschiedlichsten Bereichen analysierten die Probleme des Gesetzes, veröffentlichten Blogposts, standen für Interviews zur Verfügung, redeten mit Politikverantwortlichen, organisierten Demonstrationen und Mahnwachen.

Wenn man die Netzsperren-Debatte betrachtet, so beruhen erfolgreiche politische Kampagnen vor allem auf einem breiten Netzwerk von Unterstützerinnen und Unterstützern. Ihnen gelang es, auf vier Ebenen zu wirken: in die Breite, um möglichst viele Menschen (auch außerhalb der Datenschutzbewegung) zu erreichen; in die Politik und bei den Entscheidungsträgern; in die Medien, um Sichtbarkeit für ihr Anliegen zu erzeugen; in Wissenschaft und Forschung, um ihre Forderungen mit harten Daten und Fakten belegen zu können. Die Kampagne wurde während des gesamten Prozesses wahlweise von Einzelpersonen, lose verbundenen Kleingruppen bis hin zu etablierten Vereinen und Arbeitskreisen getragen.

3 Das Internet verändert den Meinungsbildungsprozess

Was unterscheidet nun den Castor-Ticker, das »Radio Freies Wendland« und die Kampagne gegen das Netzsperrengesetz von früheren Protesten? Heute nutzen mehr Aktivistinnen und Aktivisten das Internet für die Durchsetzung ihrer politischen Ziele. Sie haben gelernt, die unterschiedlichsten Medien *online* zu bedienen: kurze Statusmeldungen per → *Twitter*, Video-Uploads zu *YouTube*, Bilder aktueller Geschehnisse bei *Flickr*. Das konkrete Geschehen vor Ort ist auf das engste verknüpft mit der Berichterstattung darüber im Netz. Im Jahre 2009, zur Zeit der Netzsperren-Petition, gab es mehr als doppelt so viele Menschen, die in Deutschland das Internet nutzten als noch 2001 (circa 56 Millionen zu 24 Millionen).[1] Das heißt auch, dass wesentlich mehr Menschen von der gefährlichen Vermischung von Netzregulierung und polizeilichem Vorgehen (BKA) betroffen waren. Außerdem gab es 2001 weder Dienste wie *Twitter* noch → *Blogging*-Plattformen. Die Möglichkeiten des Internets haben die Quellen und Prozesse der Meinungsbildung in den vergangenen zehn Jahren dramatisch verändert.

Die klassischen Medien haben das Monopol auf die Distribution von Informationen verloren. Jeder von uns kann mit Hilfe neuer Kanäle mehr Menschen erreichen als jemals zuvor. Beispiele wie die Petition »Keine Indizierung und Sperrung von Internetseiten« zeigen, dass es möglich ist, innerhalb kürzester Zeit Menschen nicht nur zu informieren, sondern sie zu einem aktiven Eingreifen in politische Prozesse zu motivieren. Die Netzsperren-Debatte hat bewiesen, dass es möglich ist, ohne etablierte politische Akteure wie NGO oder Parteien eine politische Kraft zu entwickeln, die so stark ist, dass ein zunächst gelobtes und von den großen Parteien gewolltes Gesetz nicht zur Anwendung kommt.

Am Ende jedoch ist das Netz nichts als ein Werkzeug, ein Medium. Es ist nichts ohne das unermüdliche Engagement vieler Menschen – sie machen eine erfolgreiche Kampagne aus. Es sind die, die in ihrer Kritik des Bestehenden Visionen für sinnvolle und gute Alternativen entwickeln.

Anmerkung

1 Eurostat, Internet usage in 2009 – Households and Individuals, in: Data in Focus 46/2009, im Internet unter http://www.eds-destatis.de/de/publications/select.php?th=4&k=2.

Markus Beckedahl

Die neue Datenschutzbewegung

In den Jahren nach dem 11. September 2001 ging es politisch in der Datenschutzdebatte nur noch um einen Abbau von Grundrechten. Dem hatte die zersplitterte Datenschutzbewegung mit einer Vielzahl kleiner und mittelgroßer Initiativen wie dem Chaos Computer Club, FoeBuD (Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e. V.), dem Forum der InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FifF), netzpolitik.org und anderen wenig entgegen zu setzen.

Das Frühjahr 2005 markierte einen Wandel in der deutschen Datenschutzbewegung. Auf europäischer Ebene wurde die →Vorratsdatenspeicherung als Richtlinie beschlossen. Kurz vorher versuchte das europäische Netzwerk *European Digital Rights (EDRi)* mit einer europaweiten Kampagne noch zu retten, was zu retten war. Erfolglos. Auf dem *Chaos Communications Congress* des Chaos Computer Club trafen sich Ende 2005 Vertreterinnen und Vertreter der einzelnen Gruppen, um den Arbeitskreis Vorratsdatenspeicherung zu gründen. Die Idee: Gemeinsam eine Kampagne entwickeln und Ressourcen zusammenzutragen, um auf nationaler Ebene dieses Gesetz zu verhindern. Für alle Beteiligten war die Vorratsdatenspeicherung ein Dammbruch, mit dem alle europäischen Bürgerinnen und Bürger unter Generalverdacht gestellt und flächendeckend unser Kommunikationsverhalten protokolliert würde. Besonders viele Ressourcen zum Zusammenlegen gab es nicht. Ein *Wiki* (→ *Wikipedia*) und eine Mailingliste wurden ins Leben gerufen; alle Interessierten waren eingeladen, sich zu beteiligen.

1 Entwicklung einer neuen Öffentlichkeit im Netz

Eine mediale Öffentlichkeit gab es für dieses Thema nicht, als die Richtlinie auf europäischer Ebene angenommen wurde. Einige Medien wie die Tagesschau berichteten kurz darüber. Im weiteren Verlauf schien ein deutsches Gesetz in der allgemeinen Terrorhysterie niemanden besonders zu interessieren. Aber im Netz entwickelten sich neue Öffentlichkeiten in der →Blogosphäre. Und der Arbeitskreis Vorratsdatenspeicherung wurde schnell zum zentralen Anlaufpunkt für all jene, die sich für Datenschutz interessierten und sich gemeinsam mit Gleichgesinnten gegen einen Abbau ihrer Privatsphäre engagieren wollten.

In Gesprächen mit vielen Politikverantwortlichen wurde uns zwar Sympathie entgegen gebracht, aber immer hieß es: ›Was ihr da im Netz macht, kommt bei der Politik nicht an. Ihr müsst auf die Straße gehen!‹ Im Sommer 2006 wurde in Berlin die erste Demonstration »Freiheit statt Angst« ins Leben gerufen. 200 Menschen trafen sich am Alexanderplatz, um gemeinsam durch Berlin-Mitte zu ziehen. Medien interessierten sich nicht dafür.

Anfang 2007 erreichte dann die vorher weitgehend netzintern erfolgte Debatte über Sinn und Unsinn der Vorratsdatenspeicherung auch die klassischen Massenmedien. Die Oppositionsparteien entdeckten plötzlich das Potenzial dieser Diskussion, und schließlich erkannten auch Journalisten- und Medienverbände, dass eine Vorratsdatenspeicherung ihren Quellenschutz und damit die Pressefreiheit betreffen würde. Im September 2007 fanden sich auf einmal 15 000 Menschen vor dem Brandenburger Tor zu einer weiteren »Freiheit statt Angst«-Demonstration ein. Die Mobilisierung hatte fast ausschließlich im Netz stattgefunden. Freiwillige bastelten *Online*- wie *Offline*-Banner, Kreative gestalteten Mobilisierungsvideos und die zentrale Webseite www.vorratsdatenspeicherung.de wurde immer mehr zur zentralen Informations- und Mobilisierungsplattform.

2 Massenaktion gegen die Vorratsdatenspeicherung

Aber es half erst einmal nichts: Kurz nach der Demonstration wurde von der damaligen Großen Koalition die Vorratsdatenspeicherung beschlossen. Sie sollte Anfang 2008 in Kraft treten. Die Zeit bis dahin wurde für weitere Aktionen genutzt: Alle waren sich sicher, dass dieses Gesetz nicht verfassungskonform sein konnte. Unser Ziel war es deshalb, mit einer Massenaktion viele Unterstützer zu sammeln, die gemeinsam mit uns vor das Bundesverfassungsgericht ziehen würden, um gegen die Vorratsdatenspeicherung zu klagen.

Im Gegensatz zu üblichen Netz-Petitionen bestand die Herausforderung darin, dass wir schriftliche Einwilligungserklärungen benötigten, die uns per Post zugeschickt werden mussten. Innerhalb eines Jahres sammelten wir tatsächlich mehr als 34 000 Unterschriften und konnten so die größte Massenbeschwerde in der Geschichte des Bundesverfassungsgerichts starten. Im Jahr 2008 gab es zwei weitere Großereignisse, die dabei halfen: Im Frühsommer probierte der Arbeitskreis Vorratsdatenspeicherung einen dezentralen Aktionstag aus. In mehr als 40 Städten gingen gleichzeitig über 30 000 Aktivistinnen und Aktivisten auf die Straße. Im Herbst fand erneut die »Freiheit statt Angst«-Demonstration in Berlin statt, die ihre Teilnehmerzahl wieder

verdoppeln konnte. So viele Menschen und Organisationen waren noch nie in Deutschland für den Datenschutz auf die Straße gegangen. Spätestens jetzt stand fest: Nach der Volkszählungsdebatte in den 1980er Jahren gab es eine neue Datenschutzbewegung in Deutschland. Jetzt konnte man auch nicht mehr davon sprechen, dass es sich nur um einige wenige »Computerfreaks« handelte, denn an der Kundgebung und den begleitenden Aktivitäten im Netz nahmen längst auch andere gesellschaftliche Gruppen teil. Zu den Organisationen, die aktiv dafür eintraten, zählten beispielsweise die Naturfreundejugend Deutschlands, PRO ASYL, der Deutsche Gewerkschaftsbund und die Freie Ärzteschaft.

Anfang 2009 wurden die vielen Aktenordner mit den Unterstützerunterschriften dem Bundesverfassungsgericht in Karlsruhe übergeben; zusammen mit einigen anderen Beschwerden von Parteien und Verbänden begann das Verfahren. Es sollte sich über das gesamte Jahr 2009 hinziehen. Die Fachleute vom Chaos Computer Club wurden vom Bundesverfassungsgericht als Sachverständige eingeladen. Im März 2010 erging schließlich das Urteil: Das Gesetz zur Vorratsdatenspeicherung war verfassungswidrig. Leider teilte der Senat nicht komplett unsere Linie, wonach die Vorratsdatenspeicherung generell abzulehnen sei. Es wurde aber ein sehr enger Rahmen vorgegeben, innerhalb dessen eine neue Regelung zur Vorratsdatenspeicherung möglich wäre. Trotzdem hatte die neue Datenschutzbewegung einen Sieg errungen, den 2005 zwar alle erträumt hatten, von dem aber niemand überzeugt war, dass wir ihn tatsächlich erreichen würden.

3 Die Debatte geht weiter

Die Debatte um die Vorratsdatenspeicherung geht auch im Jahr 2012 weiter (siehe auch den Beitrag von Ziercke in diesem Band, S. 129 ff.). Während sich die mittlerweile mitregierende FDP dagegen sträubt, versucht die Union immer wieder, das Gesetz zur Vorratsdatenspeicherung neu zu beleben. Aber etwas hat sich verändert: Das Thema ist in den Massenmedien angekommen. Jede Äußerung eines Politikers oder einer Politikerin für oder gegen die Vorratsdatenspeicherung ist zur Nachricht geworden. Ohne den Arbeitskreis Vorratsdatenspeicherung und die neuen Möglichkeiten des Netzes zu Organisation und Mobilisierung wäre das nicht passiert.

II. Brennpunkte und Kontroversen

Einleitung

Die achtzehn Beiträge des zweiten Abschnitts widmen sich unterschiedlichen gesellschaftlichen Bereichen, in denen derzeit das Thema »Datenschutz« kontrovers diskutiert wird. Zu Beginn stehen Beiträge, die sich mit der Abwägung zwischen Sicherheit und Datenschutz befassen.

Marion Albers zeigt einleitend das Präventionsdilemma auf. Bei ihr wird deutlich, dass Datenschutz einerseits präventiven Charakter hat, andererseits aber übertriebene Vorsorgemaßnahmen verhindern soll.

Thomas Petri stellt die Grundzüge der Datenverarbeitung bei Sicherheitsbehörden dar. Die Texte von *Jörg Ziercke* und *Bettina Sokol* sind als explizite Meinungstexte dazu gedacht, die Positionen in der Kontroverse zwischen Sicherheit und Privatheit zu verdeutlichen.

Es folgen Beiträge, die Aspekte des Datenschutzes in unterschiedlichen gesellschaftlichen Kontexten aufgreifen: *Sven Polenz* stellt die Rolle der Datenverarbeitung in der Finanzverwaltung dar.

Der Beitrag von *Falk Lüke* beschreibt grundlegende datenschutzrechtliche Probleme aus Verbrauchersicht, während *Christoph Fiedler* und *Gerd Billen* das Verhältnis von Datenschutz und Verbraucherschutz aus kontroversen Perspektiven beschreiben.

Franz-Joseph Bartmann skizziert die Relevanz von personenbezogenen Daten und von Datenschutz im Gesundheitssystem.

Schließlich widmet sich *Wolfgang Däubler* der Frage von Datenerfassung im Bereich der Arbeitsverhältnisse. In Form einer weiteren Kontroverse zur Notwendigkeit eines Beschäftigtendatenschutzgesetzes werden die Positionen von *Roland Wolf* und *Martina Perreng* gegenübergestellt.

Den Abschnitt beschließen Beiträge, die sich mit dem Zusammenhang von Datenschutz, Privatsphäre und digitalen Medien beschäftigen. *Jan-Hinrik Schmidt* beschreibt die Veränderung von Öffentlichkeit, die Plattformen wie *Facebook* oder *Twitter* mit sich bringen.

Ulrike Wagner, *Christa Gebel* und *Niels Brüggen* zeigen auf, wie Jugendliche mit den Möglichkeiten und Zwängen der Selbstdarstellung im Internet umgehen.

Zwei aktive und bekannte Persönlichkeiten aus der →Blogosphäre, Bloggerin *Franziska Bluhm* und Blogger *Michael Seemann*, schildern in der dritten Kontroverse das Pro und Kontra von Privatsphäre und ihrem Verlust im digitalen Alltag.

Aus der Praxis von Fortbildungsveranstaltungen für Schülerinnen und Schüler zum Thema »Datenschutz und digitale Kommunikation« berichten *Frank Spaeing* und *Thomas Spaeing*.

Schließlich wird ein Interview mit Richard Allen dokumentiert, der die Internetplattform *Facebook* als oberster Datenschützer des Unternehmens in Europa vertritt.

III. Datenschutzrecht – Bestandsaufnahme und Perspektiven

Einleitung

Als der Datenschutz in den 1970er Jahren des letzten Jahrhunderts als Antwort auf die informationstechnische Entwicklung aufkam, wurde er als regulatorisches Problem verstanden, das mit Gesetzen in den Griff gebracht werden muss und kann. Inzwischen ist klar, welche Rolle Organisation, Technik und Wettbewerb für den Schutz informationeller Selbstbestimmung spielen. Doch auch hierfür ist ein rechtlicher Rahmen nötig, der in den folgenden acht Beiträgen dargestellt wird.

Dirk Heckmann stellt die allgemeinen Grundlagen und mit dem Bundesdatenschutzgesetz die nationale rechtliche Basis der Regulierung des Datenschutzes dar. *Dagmar Hartge* widmet sich dann dem ursprünglichen Ordnungsansatz mit materiell-rechtlichen Ge- und Verboten. Wie Betroffene ihre Rechte – vom Auskunftsanspruch über die Datenkorrektur bis zum Recht auf Schadenersatz – geltend machen können, beschreibt *Alexander Dix*.

Die Organisation der für den Datenschutz tätigen Stellen und deren Handlungsabläufe werden von *Sarah Thomé* und *Meike Kamp* vorgestellt. Die modernen Wettbewerbsinstrumente finden durch *Kirsten Bock* ihre Darstellung.

Peter Hustinx beschreibt, in welchem Spannungsverhältnis Datenschutz und Informationsfreiheit zueinander stehen und sich zugleich gegenseitig ergänzen.

Alexander Roßnagel und *Thilo Weichert* blicken in die nähere und in die fernere Zukunft – auf den aktuellen Änderungsbedarf des Datenschutzrechts und auf die darüber hinausgehenden langfristigen normativen Perspektiven.

IV. Technischer und organisatorischer Datenschutz

Einleitung

Spätestens seit Mitte der 1990er Jahre ist klar, dass Datenschutz auch eine Aufgabe für Fachkräfte aus den Bereichen Informatik und Management ist. Die Gestaltung der Informationstechnik und deren kontrollierte Anwendung bestimmen, ob die Betroffenen ihre Rechte tatsächlich wahrnehmen können. In den folgenden fünf Beiträgen werden hierzu die grundlegenden Informationen gegeben.

Welche Schutzziele der Datenschutz verfolgt und in welchem Verhältnis diese zueinander stehen, beschreibt *Martin Rost*.

Peter Schaar wird dann konkret und nennt die wichtigsten Methoden und Stellschrauben des technischen Datenschutzes.

Welche praktischen Hilfsmittel und Verhaltensregeln die Nutzerinnen und Nutzer zur Wahrung ihrer informationellen Rechte im Internet anwenden können, ist das Thema von *Martin Schallbruch*.

Sven Thomsen stellt auch für Informatikfremde verständlich dar, welche Grundtechnologie – nämlich die Kryptographie – zur Sicherung von Daten und von Kommunikationsvorgängen zum Einsatz kommt.

Dass und wie Datenschutz langfristig und nachhaltig in Organisationen integrierbar ist, beschreibt *Angelika Martin*.

V. Datenschutz international

Einleitung

Im fünften Teil des Bandes wird die Perspektive auf Datenschutz über Deutschland hinaus geöffnet.

Hielke Hijmans und *Owe Langfeldt* stellen die Grundzüge des Datenschutzes in der Europäischen Union vor.

Lars Reppesgaard gibt einen Einblick in die datenschutzbezogenen Vorstellungen und Strategien von *Global Players* der Internetwirtschaft wie *Google, Apple, Facebook* oder *Amazon*.

Thilo Weichert beschreibt exemplarisch die Situation von Datenschutz und Überwachung in den USA, China und Iran.

Marita Körner diskutiert schließlich die Frage, wie weit die internationale Staatengemeinschaft auf dem Weg zum globalen Datenschutz bereits ist.

VI. Anhang

Glossar

Allgegenwärtiges Rechnen: → *Ubiquitous Computing.*

Anonym: → Anonymität.

Anonymität: Der Personenbezug der Daten kann nicht mehr hergestellt werden, wie etwa bei statistischen Daten (§ 3 Absatz 6a BDSG).

Artikel-29-Gruppe: Die Gruppe (»Datenschutzgruppe«) wurde aufgrund Artikel 29 der Richtlinie 95/46/EG (Datenschutzrichtlinie) vom 24. Oktober 1995 eingesetzt. Sie ist das unabhängige Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes.

Auskunfteien: Private Dienstleistungsunternehmen, die Informationen über die Zahlungsfähigkeit von Personen sammeln und diese Daten auf Anfrage entgeltlich zur Verfügung stellen.

Blog: → *Weblog*.

Blogger/Bloggerin: Person, die ein → *Weblog* betreibt.

Blogosphäre: → *Weblog.*

Blog-RSS-Feeds: → RSS und → Feeds.

Blogging-Plattform: Software zum Betreiben eines → *Weblogs*.

Bluetooth: Ein in den 1990er Jahren entwickelter Industriestandard für die Datenübertragung zwischen Geräten über kurze Distanz per Funktechnik. B. ist eine wichtige Kommunikationsschnittstelle für mobile Kleingeräte wie Mobiltelefone. Hauptzweck von B. ist das Ersetzen von Kabelverbindungen zwischen Geräten. Der Begriff B. (dt. Blauzahn) soll an den dänischen Wikingerkönig Harald Blauzahn erinnern, der als kommunikativer Mensch galt.

Botnet-Attacken: Eine Vielzahl von Rechnern (oft mehrere Tausend) werden zunächst mit einem Schadprogramm infiziert und können dann mittels einer zentralen Steuerung (Comand and Control-Server) für den Angriff auf ein gemeinsames Ziel (z. B. den Webserver eines Unternehmens) genutzt werden (siehe auch den Beitrag von Schallbruch in diesem Band, S. 372 ff.).

Cloud: (dt. Wolke) → *Cloud Computing*.

Cloud Computing: Konzept für die Organisation von IT-Infrastrukturen, bei der Daten, aber auch Rechnerkapazität oder Programme nicht auf lokalen Rechnern, sondern in verteilten Netzwerken (metaphorisch: in der Wolke) bereit gehalten und bei Bedarf genutzt werden können.

Compliance: (dt. Einhaltung/Erfüllung) Die Bemühungen um die Einhaltung gesetzlicher Vorschriften innerhalb von Unternehmen. Durch eine geeignete Unternehmensführung sollen Mitarbeiterinnen und Mitarbeiter eines Unternehmens dazu angehalten werden, auf strafbares oder pflichtwidriges Handeln zu verzichten (siehe auch den Beitrag von Wolf in diesem Band, S. 199 ff.).

Cookie: (dt. Keks) Datenpaket, das beim Besuch von Webseiten erzeugt und auf dem Computer der Nutzenden gespeichert wird. Enthält Informationen über frühere Seitenabrufe, Browsereinstellungen sowie Systemmerkmale und dient der Wiedererkennung.

Customer Relationship Management-System: (dt. Verwaltungssystem für Kundenbeziehungen) Softwaresysteme, mit denen sich Kundendaten sowie Kontakte, Vertragsabschlüsse und andere Geschäftsbeziehungen mit (potentiellen) Kunden erfassen und auswerten lassen.

Cyberspace: (griech.-engl. Ursprungs, dt. kybernetischer Raum) Von Computern erzeugte virtuelle Scheinwelt. Der Begriff wird umgangssprachlich auch benutzt, um alle Anwendungen des Internets zu beschreiben.

Datamining: Sammelbegriff für mathematisch-statistische Verfahren, um in großen Datenbeständen Muster zu erkennen.

Datenschutzaudit: Bei einem D. lassen die Anbieter von Datenverarbeitungsanlagen ihre (technischen) Abläufe und ihre Datenschutzregeln durch unabhängige Begutachtung freiwillig darauf prüfen, ob ihr Konzept und ihre Technik mit den Datenschutzgesetzen im Einklang sind. Die Ergebnisse werden veröffentlicht. Rechtliche Grundlage für das D. ist § 9a BDSG, jedoch fehlt das entsprechende Datenschutzauditgesetz (siehe auch den Beitrag von Bock in diesem Band, S. 310 ff.).

De-Mail: Ein nationaler Standard zur verbindlichen und vertraulichen Versendung von Dokumenten und Nachrichten über das Internet. Er soll die Signierung und Verschlüsselung auch für Laien zugänglich machen. De-Mail wird vom Bundesministerium des Innern koordiniert, das zertifizierte Anbieter (De-Mail-Provider bzw. -Anbieter) zulässt (siehe auch den Beitrag von Schallbruch in diesem Band, S. 372 ff.).

Digital Natives: Bezeichnung von Personen, die mit digitalen Technologien wie Computer, Internet, Mobiltelefon etc. aufgewachsen sind.

DNA: (Abk. für Desoxyribonukleinsäure) Ein in allen Lebewesen vorkommendes Biomolekül und Trägerin der Erbinformationen. Einzelne Abschnitte der DNA gelten als Marker für spezielle Eigenschaften des Lebewesens (etwa Krankheiten), aus ihnen lassen sich Abstammungs-/Verwandtschaftsverhältnisse rekonstruieren. Abgesehen von eineiigen Mehrlingen ist die DNA eines Menschen mit sehr hoher Wahrscheinlichkeit eineindeutig, das heißt jeder Mensch lässt sich anhand seiner DNA eindeutig identifizieren.

Einschreitschwelle: Mindestanforderungen, die erfüllt sein müssen, damit ein staatliches Handeln erfolgen darf.

Ende-zu-Ende-Verschlüsselung: Verfahren der Kryptografie, bei dem Nachrichten vom Sender verschlüsselt und erst beim Empfänger wieder entschlüsselt werden. Die Information ist während der gesamten Übertragung gegen Zugriffe von Außen gesichert (siehe auch den Beitrag von Thomsen in diesem Band, S. 381 ff.).

Europol: Europäisches Polizeiamt, 1995 begründet mit Sitz in Den Haag. Die Behörde soll die Arbeit der nationalen Polizeibehörden Europas im Bereich der grenzüberschreitenden organisierten Kriminalität (OK) koordinieren und den Informationsaustausch zwischen den nationalen Polizeibehörden fördern. Seit 1.1.2010 ist Europol eine offizielle Agentur der EU.

Feed Reader: Sammelbegriff für Programme, die das Abonnieren und zeitversetzte Abrufen von → RSS-*Feeds* unterstützen.

Firewall: (dt. Brandmauer) Software-System zur Sicherung gegen unbefugte Netzwerkzugriffe.

Geodaten: Digitale Standortangaben, mit denen die genaue Position auf der Erdoberfläche beschrieben wird. G. sind die Voraussetzung für → *Location Based Services*.

GIZ: (Abk. für Gemeinsames Internetzentrum) In dem in Berlin ansässigen GIZ arbeiten nach dem Vorbild des → GTAZ das Bundesamt für Verfassungsschutz, das Bundeskriminalamt

(BKA), der Bundesnachrichtendienst (BND), der Militärische Abschirmdienst (MAD) sowie die Generalbundesanwaltschaft zusammen, um die Arbeitsweise islamistischer Terrorgruppen im Netz zu beobachten. Das GIZ wurde 2007 mit Erlass des Bundesinnenministers begründet, eine gesetzliche Grundlage für seine Arbeit besteht nicht.

Global Positioning System (GPS): Satellitengestütztes System zur Positionsbestimmung und Zeitmessung. Die vom GPS-System ausgesandten Signale können Endgeräte (z. B. in → *Smartphones*, Navigationssystemen) weltweit zur Standortbestimmung nutzen.

Google Street View: *Online*dienst der Firma *Google Inc.*, für den großflächig Panoramabilder aufgenommen, digitalisiert und mit Kartographie- und Geodaten verknüpft wurden. Internetnutzende können digitalisierte Gebiete in videorealistischen Ansichten betrachten.

GPS: → *Global Positioning System*.

Großer Lauschangriff: Akustische Wohnraumüberwachung, bei der Strafverfolgungsbehörden mit Hilfe von technischen Mitteln heimlich Gespräche abhören, die in geschlossenen Räumen (Wohnungen, Geschäftsräume usw.) geführt werden. Davon zu unterscheiden ist der »Kleine Lauschangriff«, der sich nur auf Gespräche außerhalb von Wohnungen, also an öffentlichen Örtlichkeiten oder auch in allgemein zugänglichen Büro- und Geschäftsräumen, bezieht.

GTAZ: (Abk. für Gemeinsames Terrorismusabwehrzentrum) Eine in Berlin ansässige Koordinierungsstelle der deutschen Sicherheitsbehörden des Bundes und der Länder zur Bekämpfung des islamistischen Terrorismus. Im GTAZ tauschen Polizeibehörden, Nachrichtendienste, das Bundesamt für Migration und Flüchtlinge sowie die Generalbundesanwaltschaft ihre Informationen aus. Die Einrichtung wurde am 14.12.2004 mit Erlass des Bundesinnenministers begründet, eine gesetzliche Grundlage für die Arbeit des GTAZ besteht nicht.

Hash/Hashwert: Prüfsumme (von engl. *hash total*), mit der die Unversehrtheit von Daten vor/nach einer Übertragung oder einer Verschlüsselung/Entschlüsselung kontrolliert werden kann.

Hashfunktion: Mathematische Vorschrift bzw. Algorithmus, mit deren Hilfe → Hashwerte berechnet werden.

Identity Theft: (dt. Identitätsdiebstahl) Missbräuchliche Nutzung der Identität einer Person durch Dritte.

Internet der Dinge: Bezeichnung für Techniken der zunehmenden informationellen Vernetzung von Gegenständen, die über Sensor- und Aktorensysteme (etwa → RFID oder *Barcodes*) miteinander kommunizieren. Bisher vor allem in der Logistik angewandt, beispielsweise bei der Paketverfolgung im Internet.

IP: Abk. für *Internet Protocol*, umgangssprachlich für → IP-Adresse.

IP-Adresse: Internetprotokoll-Adresse für alle Geräte (PCs, Webserver, Mailserver, → *Smartphones*, → *Router* etc.), die über das IP-Netzwerk, den geläufigsten Netzwerkstandard, miteinander verbunden sind. Die IP-Adresse wird zur Identifizierung aller beteiligten Geräte sowie zur Festlegung der Übertragungsrouten aller Informationen genutzt. Sie besteht aus einer 32- (IPv4) bzw. 128-bittigen Ziffer (IPv6) und wird üblicherweise in Oktettschreibweise dargestellt (Beispiel: 192.168.0.1). Mit der Einführung der IP Version 6 (IPv6) wird eine nahezu unbegrenzte Anzahl von I.n für internetfähige Geräte und damit eine wichtige Voraussetzung für das → Internet der Dinge geschaffen (siehe auch die Presse-

mitteilung des BfDI vom 5.6.2012 mit Verweis auf die Entschließungen der nationalen und internationalen Datenschutzkonferenzen sowie auf den BfDI-Tagungsband zum Symposium IPv6, im Internet unter www.bfdi.de).

ISO: (Abk. für *International Organization for Standardization*, dt. Internationale Organisation für Normung) 1947 begründete zwischenstaatliche Normungseinrichtung mit Sitz in Genf. Sie erarbeitet technische, klassifikatorische und Verfahrensstandards für nahezu alle Bereiche des industriellen Lebens. Der I. gehören derzeit über 150 Mitgliedsstaaten an, weitere Informationen im Internet unter http://www.iso.org.

Kryptografie: Verfahren der Verschlüsselung elektronischer Daten, um diese vor der unberechtigten Kenntnisnahme zu sichern.

Lauschangriff: Zum sogenannten Großen und Kleinen Lauschangriff → Großer Lauschangriff

Listenprivileg: In Listen zusammengefasst dürfen bestimmte Daten auch ohne Wissen und Zustimmung der Betroffenen anderen zur Verfügung gestellt werden, solange die Herkunft der Daten eindeutig aus der Liste hervorgeht (§ 28 Absatz 3 Nummer 3 BDSG).

Location Based Services (LBS): (dt. ortsbezogene Dienste) Standortbezogene Internetdienste, die Informationen in Abhängigkeit vom (aktuellen) Standort der Nutzenden bereitstellen. Beispiele für LBS sind Dienste, die Sehenswürdigkeiten und Restaurants (Qype), Verkehrsverbindungen (Öffi) oder *Online*-Freunde (Latitude, Foursquare) in der jeweiligen Umgebung markieren und empfehlen.

Messenger-Dienst: Internetbasierter Dienst zum Verschicken von Textnachrichten, Dateien oder (Video-) Telefonieren (beispielsweise *Skype*, ICQ oder MSN).

Microblog: → *Twitter.*

Monitoring: (dt. Beobachten) Überwachen des Verhaltens von Personen bei der Nutzung von Internetdiensten.

Netzwerkplattform (auch: *Social Media, Community Platform*, *Social Network* Site): Sammelbegriff für Internet-Anwendungen, bei denen Nutzende ausgehend von einer eigenen Profilseite soziale Beziehungen zu anderen Personen (als »Freunde« oder »Kontakte«) knüpfen und so den Kontakt mit ihrem erweiterten sozialen Umfeld halten können. Bekannte N. sind u. a. *Facebook*, studiVZ schuelerVZ, wer-kennt-wen, *Flickr,* XING, etc.

No-Fly-Liste: Liste von Personennamen, die vom US-amerikanischen *Terrorist Screening Center* (TSC) erstellt wird. Die in der Liste verzeichneten Personen dürfen sich nicht auf Flügen in die USA oder aus den USA heraus befinden.

Pervasive Computing: (dt. Rechnerdurchdringung) → *Ubiquitous Computing.*

Phishing: Sammelbegriff für betrügerische Methoden, um beispielsweise über gefälschte Anmeldeportale an die Daten von Internetnutzenden zu gelangen, um diese zu Zwecken des Identitätsdiebstahls zu nutzen.

Profiling: Das Erstellen von Profilen über eine bestimmte Person (von engl. *to profile*, dt. abgrenzen). Im *Online-Marketing* das Erstellen von Nutzerprofilen (zum Beispiel: welche Vorlieben oder Interessen hat eine Person) anhand von Informationen über das Surfverhalten der Nutzenden.

Privacy by Design: (dt. Privatsphäre durch Gestaltung) Beschreibung für das Prinzip des technologischen oder systemgestützten Datenschutzes. Prinzipien des Datenschutzes, allen voran die Datensparsamkeit, fließen dabei in die technische Gestaltung neuer Gerä-

te oder Programme ein (siehe auch die Beiträge von Schaar, S. 363 ff. und Roßnagel, S. 331 ff. in diesem Band).

Privacy International (PI): 1990 gegründete, international tätige Menschenrechtsorganisation mit Sitz in London. Sie versteht sich als Hüterin der Privatsphäre von Bürgerinnen und Bürgern gegenüber dem Staat und Wirtschaftsunternehmen. PI verleiht alljährlich den »Big Brother Award« an Organisationen, die die Privatsphäre von Menschen besonders eklatant verletzt haben.

Pseudonym: Name oder Kennwort zur Verschleierung der wahren Identität einer Person.

Pseudonymität: Liegt vor, wenn eine Zuordnungsregel existiert, mit welcher sich der Personenbezug von Daten wieder herstellen lässt.

Reality-TV: (dt. Realitätsfernsehen) Bezeichnung für ein Fernseh-Programmformat, bei dem der Eindruck einer dokumentarischen (»echten«) Darstellung erweckt wird, obwohl es sich um ein inszeniertes, teilweise fiktionales (»erfundenes«) Geschehen handelt .

RFID: (Abk. für *Radio Frequency Identification*, dt. Identifikation über Radiofrequenzen) Funkbasiertes System zur Identifizierung und Ortung von Objekten oder Lebewesen mit Hilfe von miniaturisierten Chips (RFID-*Tags*, RFID-Chips).

Router: Netzwerkgeräte, die die Schnittstelle zwischen Rechnernetzen darstellen. R. (von engl. *to route*, dt. leiten, befördern) analysieren die Zieladressen ankommender Datenpakete und blockieren deren Durchgang oder leiten sie zum gewünschten Subnetz weiter.

RSS: (Abk. für engl. *Really Simple Syndication*, dt. wirklich einfache Zusammenstellung) Format für die Darstellung von (Webseiten-)Informationen, das ein Lesen ohne Webbrowser ermöglicht. Mit Hilfe von →*Feed Reader*–Programmen können Nutzende jene Webseiten bzw. Nachrichtenkanäle, die →RSS anbieten, »abonnieren« und so über aktuelle Meldungen auf dem Laufenden bleiben.

Safe-Harbor-Abkommen: Eine Vereinbarung des *US Department of Commerce* mit der Europäischen Kommission. US-Unternehmen, die sich den *Safe-Harbor*-Prinzipien unterwerfen, verpflichten sich selbst, die wichtigsten europäischen Datenschutzstandards einzuhalten. Damit dürfen personenbezogene Daten an sie oder von ihnen aus der Europäischen Union in die USA übermittelt werden.

SCHUFA: (Abk. für Schutzgemeinschaft für allgemeine Kreditsicherung) Privatwirtschaftlich organisierte Auskunftei (Schufa Holding AG mit Sitz in Wiesbaden), die von Banken und anderen Finanzinstituten getragen wird. Die S. erfasst Daten zu Finanzdarlehen und Zahlungsverzügen, um daraus Prognosen zur Kreditwürdigkeit zu errechnen. Ihr Ziel ist es, ihre Vertragspartner (u. a. Banken, Vermieter) vor Kreditausfällen zu schützen. Nach eigenen Angaben hat sie 479 Millionen Einzeldaten von 66,2 Millionen Personen erfasst, die jährlich über 100 Millionen Mal abgerufen werden.

Scoring: (im Finanzsektor) Kreditwürdigkeitsprüfung anhand von analytisch-statistischen Verfahren (abgeleitet von engl. *to score* – punkten, *score* – Punktstand). Auf der Basis von Merkmalen werden Punkte (*Score*-Werte) vergeben, deren Zahlenwert die Kreditwürdigkeit einer Person repräsentiert.

Smart Metering: (dt. intelligentes Messen) Bezeichnung für Strom-, Gas- oder Wasserzähler, die den Zeitpunkt des Verbrauchs erfassen und eine Echtzeit-Anzeige der Verbrauchsmengen für die Verbraucherseite sowie die Berechnung zeitabhängiger Verbrauchstarife erlauben.

Smartphone: Neuere Generation von Mobiltelefonen, die über erweiterte Computereigenschaften und meist über einen Internetzugang verfügen. S. lassen sich durch Zusatz-Programme (Apps) in ihrer Funktionalität erweitern, bieten Möglichkeiten zur Texteingabe und multimediale Funktionen (Audio-/Videowiedergabe).

Smart Home Networks: (dt. Netzwerk für intelligentes Wohnen) Techniken der Vernetzung von Versorgungseinrichtungen (Heizung, Lüftung, Strom) und Haushaltsgeräten (Fernseher, Beleuchtung etc.). Sie sollen beim Energiesparen helfen, mehr Komfort bieten (einfache Steuerung) und die Sicherheit innerhalb der Wohnung für ältere und pflegebedürftige Menschen erhöhen (u. a. Rauchmelder, Alarmsysteme).

Social Media: (dt. soziale Medien) Bezeichnet digitale Kommunikationsdienste, -anwendungen und -plattformen, die es den Nutzenden erlauben, sich zu vernetzen und Informationen auszutauschen, → Netzwerkplattformen.

Social Web: (dt. soziales Netz), → Web 2.0.

Soziales Netzwerk: → Netzwerkplattformen.

SSL: (Abk. für *Secure Sockets Layer,* dt. sichere Übertragungs-Schicht) Protokollebene innerhalb des Internetprotokolls (→ IP) zur Verschlüsselung von Datenübertragungen. Sie wird vor allem genutzt, um Datenübertragungen zwischen Webservern und Internetnutzern zu schützen. Das SSL-Protokoll wird mittlerweile durch das TLS-Protokoll (*Transport Layer Security*) weiterentwickelt.

Streamen: Übertragen eines Datenstroms (zum Beispiel Audio- oder Videoübertragung) in Echtzeit.

Street View: → *Google Street View.*

Swift: (Abk. für *Society for Worldwide Interbank Financial Telecommunication*, dt. Gesellschaft für weltweiten Finanzdatenaustausch zwischen Geldinstituten) 1973 gegründete internationale Genossenschaft der Geldinstitute, über die deren Mitglieder Informationen zu transnationalen Finanzgeschäften austauschen, u. a. Standardüberweisungen, Wertpapierhandel, Kontoauszüge. S. hat seinen Sitz in La Hulpe (Belgien) und verarbeitet täglich circa 18,5 Millionen Meldungen (Stand: Juni 2012).

Targeting: Methode aus dem Marketing, um möglichst genau Zielgruppen beispielsweise mit Werbung anzusprechen (abgeleitet von engl. *target*, dt. Ziel). Das *Online*-T. basiert in der Regel auf → *Cookies* und/oder von Nutzenden bereit gestellten persönlichen Informationen, etwa auf Netzwerkplattformen.

Tracking: Sammelbegriff für Verfahren, mit denen Aktivitäten beispielsweise im Internet nachvollzogen und verfolgt werden können (von engl. *to track*, dt. verfolgen).

Trojaner: Ein Computerprogramm, das als unschädliche Anwendung getarnt ist, jedoch genutzt werden kann, um zum Beispiel den Datenverkehr von außen zu erfassen (so etwa bei der *Online*-Durchsuchung).

Twitter: Kurznachrichtendienst, digitale Anwendung zum *Microblogging*, vgl. → *Tweets*, → *Social Media*. Lesende, die die Beiträge einer Person abonniert haben, werden als *Follower* bezeichnet.

Tweets: Einträge auf der digitalen Kommunikationsplattform *Twitter* (dt. Gezwitscher; www.twitter.com). Bei dem *Microblogging*-Dienst dürfen nicht mehr als 200 Zeichen für eine Nachricht verwendet werden.

Ubiquitous Computing: (dt. Rechnerallgegenwart) Beschreibt den Umstand, dass computergestützte Dienste und Informationen nicht mehr nur auf speziellen PCs zur Verfügung stehen, sondern in nahezu alle alltäglichen Gegen-

stände und Aktivitäten eingebettet sind (→ Internet der Dinge).

URL: (Abk. für *uniform resource locator*, dt. einheitliche Quellenbezeichnung) Standard zur Bezeichnung von Adressen in einem Netzwerk. Die URL bezeichnet das verwendete Protokoll der Datenübertragung (z. B. http für Webseiten, ftp für Dateitransfer, mailto für Mailadressen), gefolgt von der Adresse (zum Beispiel http://www.bpb.de).

Verhältnismäßigkeit: Der Grundsatz bzw. das Prinzip der V. besagt, dass der Staat stets nur solche Mittel anwenden darf, die erforderlich, geeignet und angemessen sind, um ein bestimmtes legitimes Ziel zu erreichen. Möchte der Staat beispielsweise die Daten von bestimmten Personen erheben, um Verbrechen vorzubeugen, so muss die Erhebung der Daten diesen Grundsätzen entsprechen; die Verletzung des Rechts auf informationelle Selbstbestimmung, die durch den Eingriff erfolgt, darf nicht in einem unangemessenen Verhältnis zum Ziel der Verbrechensbekämpfung stehen.

Virtual Reality: Von Computern erzeugte virtuelle – im Gegensatz zur physischen – Realität.

Voice over IP: Telefonieren mittels *Internet Protocol* (→ IP), das heißt über Computer-Netzwerke (Internet-Telefonie).

Vorratsdatenspeicherung: Beschreibt allgemein die Speicherung von Daten zu einem noch unbekanntem Zweck (»auf Vorrat«). V. wird im engeren Sinn als Synonym für die präventive Speicherung der Telekommunikations-Verbindungsdaten aller Bürgerinnen und Bürger gebraucht (siehe auch die Beiträge von Beckedahl, S. 48 ff. und Papier, S. 67 ff. in diesem Band).

Web 2.0: Sammelbegriff für verschiedene technische Innovationen, die die Gestalt des *World Wide Web* seit Mitte der 2000er Jahre prägen. Das Web 2.0 zeichnet sich gegenüber dem »klassischen« Internet (Web 1.0) durch einen stärkeren Austausch zwischen Schreibenden und Lesenden bis hin zur Verwischung der Grenze zwischen Produzierenden und Konsumierenden der Netzinhalte aus.

Web 2.0-Anwendungen: → Netzwerkplattformen, → Web 2.0.

Weblog: Sammelbegriff für Webseiten, die relativ regelmäßig von einer oder mehreren Personen (»Blogger«) aktualisiert werden und deren Inhalte (meist Texte) rückwärts chronologisch angezeigt werden. In der Regel können einzelne W.-Einträge von anderen Nutzenden kommentiert werden. Die Gesamtheit aller W. wird als »Blogosphäre« bezeichnet.

Webtracking: → *Tracking*.

WikiLeaks: (häufig auch *Wikileaks*, von engl. *leak*, dt. undichte Stelle) Enthüllungsplattform im Internet, auf der Dokumente anonym veröffentlicht werden, die aufgrund von Geheimhaltung bisher nicht zugänglich waren.

Wikipedia: Die weltweit größte, auf dem Wiki-Prinzip basierende freie Enzyklopädie im Internet. Wikis sind Softwareplattformen für das gemeinsame Bearbeiten und Bereitstellen von Texten im Internet. An der W. können grundsätzlich alle Nutzerinnen und Nutzer mitschreiben. Sie existiert derzeit für über 270 Sprachen, allein die deutsche Version enthält zurzeit 1,4 Millionen Einträge (Stand: Juli 2012).

WLAN/W-LAN: (Abk. für *Wireless Local Area Network*, dt. drahtloses lokales Netzwerk) Bezeichnung eines lokalen Funknetzes.