Jan-Hinrik Schmidt/Thilo Weichert (Hrsg.)
Datenschutz

Schriftenreihe Band 1190

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.

Wiebke Loosen

(Massen-)Medien und Privatheit

1 Veröffentlichte Privatheit in den Medien

Massenmedien schaffen *öffentliche* Kommunikation. Daher sind Privatheit und Massenmedien auf den ersten Blick zwei Begriffe, die sich gegenseitig ausschließen: Was über die Massenmedien verbreitet wird, ist öffentlich und damit nicht privat. Wohl aber wird Privates und Intimes massenhaft Gegenstand öffentlicher Kommunikation. Privatheit in den Medien ist daher stets als »medialisierte Privatheit«[1], als Thematisierung oder Inszenierung von Privatheit zu begreifen. Dies gilt ebenso für traditionelle Medien wie für das Internet und insbesondere für soziale Medien, die auf dem Prinzip Selbstoffenbarung basieren und eine zunehmende Verfügbarkeit privater Informationen mit sich bringen.

Das, was wir in den Medien wahrnehmen, ist also stets eine mediale Konstruktion von Privatheit, genauer gesagt: von Themen, die beispielsweise von einem Medienkritiker, einer Politikerin, einem Nutzer etc. als (eigentlich) privat, nicht öffentlich relevant oder als die Privatsphäre verletzend qualifiziert werden. Dies deutet darauf hin, dass derartige Einschätzungen und Bewertungen individuell höchst unterschiedlich sein können, und daher die Darstellung von Privatem in den Medien häufig Gegenstand kontroverser Debatten in unterschiedlichen Kontexten ist (etwa in der Medienpädagogik, der Medienpolitik, im Medienrecht, in den Medien selbst etc.).

Damit stellen sich auch Fragen danach, wie Privatheit in den Medien dargestellt wird, welche Inszenierungsstrategien dabei eine Rolle spielen, welche Konsequenzen sich hieraus für das Verhältnis von Privatheit und Öffentlichkeit ergeben und welche Bewertungsmaßstäbe dabei zugrunde gelegt werden. Hierbei ist zu berücksichtigen, dass Bedeutung, Wert und Schutz des Privaten eng verbunden sind mit der kulturellen, normativen und sozialen Verfasstheit einer Gesellschaft.

Die Unterscheidung von Privatheit und Öffentlichkeit ist konstitutiv für das Selbstverständnis moderner Gesellschaften.[2] Dieses Selbstverständnis – und der dazu gehörende Selbstverständigungsprozess – wird heute maßgeblich von Massenmedien und Journalismus geprägt und ist konstituierend für das, was in einer Gesellschaft unter »Öffentlichkeit«

verstanden wird. Bedeutung und Verhältnis von Privatheit und Öffentlichkeit sind ohne (Massen-)Medien und Journalismus also nicht zu bestimmen.

2 Privatheit in der Fernsehkultur

Eine besondere Rolle nimmt hierbei das Fernsehen ein, und die Darstellung von Privatheit in den Medien wird häufig beschrieben als ein Phänomen der Fernsehkultur.[3] Orientiert ist die Diskussion vielfach an spezifischen Programmformaten (wie *Daily Talks*) oder speziellen Sendungen (wie »Big Brother« oder »Ich bin ein Star – holt mich hier raus!«), die gesellschaftliche (zum Teil wiederum in den Medien ausgetragene) Debatten nicht nur um die Grenzen des guten Geschmacks, sondern auch um die Verschiebungen des Verhältnisses zwischen Privatheit und Öffentlichkeit auslösen.

Das Fernsehen gibt in diversen Programmformen unterschiedlich gestaltete Einblicke in private Lebensräume:[4] fiktionale Sendeformen, die Alltagssituationen und -konflikte dramaturgisch verdichten; Dokumentationen, die beispielsweise Lebensausschnitte zeigen sowie Werbespots, Gameshows und Talkshows. Ergänzen lassen sich hier zum Beispiel noch Formate des sogenannten →*Reality-TV* wie Doku-/*Real-Life-Soaps* und *Reality*-Spiel-/*Casting-Shows*. Sie verhelfen einer zunehmenden Zahl »normaler Menschen« um den Preis der Selbstoffenbarung zu einer mehr oder weniger flüchtigen Medienprominenz.

Mit dem Begriff *Scripted Reality* werden schließlich Sendungen bezeichnet, die mit verschiedenen dieser Elemente arbeiten, auf einem fiktionalen Drehbuch basieren und von Laiendarstellern präsentiert werden. Spätestens hierbei sind die Grenzen zwischen Fakten und Fiktion (für die Zuschauerinnen und Zuschauer) kaum mehr auszumachen. Darüber hinaus findet die Darstellung von Privatem nicht nur in derartigen eher unterhaltenden Programmformen statt, sondern auch in nachrichtlich ausgerichteten Programmen und Medien, etwa im Zusammenhang mit der Berichterstattung über Gerichtsprozesse und Politiker- oder sonstige Prominenten-Affären.

Die Schnittstellen zwischen Privatheit und Öffentlichkeit zeigen sich aber nicht nur am Massenmedium Fernsehen, sondern insgesamt an der Vielfalt von Medientechnologien und Medienangeboten, die in einer Gesellschaft genutzt werden. So hat es beispielsweise die Verbreitung von Mobiltelefonen mit sich gebracht, dass Telefongespräche als private Handlung zunehmend im öffentlichen Raum stattfinden[5] und als solche Distanz von anderen in der Öffentlichkeit erfordern:[6] Mithören gilt als unhöflich,

lässt sich mitunter aber nicht vermeiden. Mindestens als ambivalent zu bewerten sind auch Videoüberwachungen von öffentlichen Plätzen (von denen man unter Umständen nichts weiß und an die man sein Verhalten nicht entsprechend anpassen kann) sowie das anders gelagerte Beispiel der Web-Cams (oder der digitalen Fototechnologie), die eine »Sichtbarmachung des Privaten«[7] im Internet ermöglichen und eine Form der Selbstoffenbarung mit Hilfe von Medien(-technologien) darstellen.

3 Der Nachrichtenwert von Privatheit

Das Gegenteil von Selbstoffenbarung privater Informationen und Selbstinszenierung ist die »Fremdoffenbarung« und Inszenierung von Privatheit durch andere, beispielsweise durch journalistische Berichterstattung: Auch in journalistischen Printmedien hat die Darstellung und Thematisierung des Privaten einen hohen Nachrichtenwert – besonders in Verbindung mit dem Nachrichtenfaktor Prominenz. Derartige Ereignisse und Themen bilden den Schwerpunkt der reichweitenstarken sogenannten »Promi-Berichterstattung«, die sich überwiegend (aber nicht ausschließlich) in Boulevardmedien finden lässt und bis hin zur Skandalisierung und öffentlichen Disqualifizierung (vermeintlichen) Fehlverhaltens führen kann.[8]

In dieser Hinsicht lässt sich Privatheit durchaus auch als *Nachrichtenfaktor* charakterisieren, der Ähnlichkeiten zu klassischen journalistischen Nachrichtenfaktoren wie Personalisierung, Elitepersonen, Prominenz, kulturelle Nähe, soziale Relevanz, *Human Touch* und Sex/Erotik aufweist. Insbesondere Personalisierung ist eine gängige journalistische Strategie, Themen (auch mit Hilfe der Einbindung von sozialen Medien und weiteren Formen der Publikumsbeteiligung) anhand von Einzelpersonen/-schicksalen zu illustrieren. Dabei können »private Nachrichten« bzw. Nachrichten von/über Privatpersonen ein hohes Maß an Authentizität aufweisen. Sie ermöglichen eine Identifikation und (parasoziale) Interaktion sowie Anschlusskommunikation.

Die Frage »Privatangelegenheit oder von öffentlichem Interesse?« und der dahinter stehende grundlegende Konflikt zwischen den Rechtsgütern Persönlichkeitsschutz und Berichterstattungsfreiheit[9] macht im Journalismus eine kontinuierliche Güterabwägung erforderlich. Beide Rechtsgüter sind auf unterschiedlichen Ebenen angesiedelt, haben unterschiedliche Bezugsgrößen: Im einen Fall ist das Individuum, eine Gruppe oder Organisation angesprochen, die ein berechtigtes Interesse haben können, dass private Informationen unveröffentlicht bleiben. Im anderen Fall ist die Bezugsgröße die Gesellschaft, die wiederum ein berechtigtes Interesse an der

Enthüllung haben kann. In beiden Fällen hat die Veröffentlichung privater Informationen unterschiedliche Bedeutung, Relevanz und Konsequenzen.

Daher ist die Abwägung zwischen eben diesen unterschiedlichen Interessen komplex und insbesondere dann Gegenstand medienkritischer, medienethischer Diskussionen und bisweilen auch juristischer Auseinandersetzungen, wenn Medien in Aufsehen erregender Weise ethische und/oder juristische Grenzen zugunsten einer Veröffentlichung überschreiten (zum Beispiel die Fotos des toten Uwe Barschel, die Berichterstattung über die Unglücke von Borken und Ramstein oder der »Fall des kleinen Josephs aus Sebnitz«). Über derartige Grenzüberschreitungen wird dann wiederum in den Medien in Form des Medienjournalismus berichtet und diskutiert.

Zwischen Enthüllung und Selbstoffenbarung

Eine neue Unübersichtlichkeit bekommt die Situation durch die zunehmende Verbreitung sozialer Medien, denn diese und die dort verfügbaren Informationen sind immer öfter auch Gegenstand journalistischer Recherche und Berichterstattung und eröffnen damit neue Potenziale, aber auch neue ethische Probleme.[10] Denn in den sozialen Medien treffen die Prinzipien »Enthüllung durch den Journalismus« und »Selbstoffenbarung durch das Publikum« aufeinander: Inhalte, die im → *Social Web* ursprünglich für eine private bzw. »persönliche Öffentlichkeit« (siehe auch den Beitrag von Schmidt in diesem Band, S. 215 ff.) gedacht waren, können über die massenmediale Zirkulation einer sehr viel breiteren Öffentlichkeit bekannt werden. Das *Social Web* bringt also besondere Herausforderungen in Bezug auf die Unterscheidung und den Umgang mit Privatheit und (unterschiedlichen Formen von) Öffentlichkeit mit sich.

Das zeigt auch das sogenannte *Privacy-Paradox*.[11] Damit wird der vielfach beobachtete Umstand bezeichnet, dass zwar eine Mehrheit der Nutzenden des *Social Web* ein individuelles Bedürfnis nach Privatsphäre äußert und überdies angibt, sich der potentiellen Gefahren der Selbstoffenbarung im Web bewusst zu sein, dieses Wissen aber offenbar nicht zwangsläufig zu entsprechenden Vorsichtsmaßnahmen zum Schutz der eigenen Privatsphäre führt (siehe auch den Beitrag von Trepte in diesem Band, S. 59 ff.).

Eine (Teil-)Erklärung für diesen widersprüchlichen Befund lässt sich in einer Einschätzung der Philosophin Beate Rössler finden, die der vielfach geäußerten These einer generellen Entgrenzung zwischen Privatheit und Öffentlichkeit eher kritisch gegenübersteht.[12] Sie konstatiert vielmehr eine »Änderung des Grenzverlaufs zwischen dem Privaten und dem Öffentlichen, ein Grenzverlauf der ohnehin nie feststand und feststeht, sondern immer umstritten und immer im Umbau ist (…).« Damit finde, so Rössler weiter,

aber noch keine Aufhebung, kein Verfall der Trennung zwischen öffentlich und privat statt, vielmehr veränderten sich die Funktionen des Öffentlichen und Privaten, ohne dass die »Menschen ihren Sinn fürs Private oder ihren Sinn für die Differenzierung zwischen öffentlich und privat verlieren«.[13] So jedenfalls ließe sich auch die öffentliche Diskussion um → *Google Street View* lesen, bei der vor allem Hauseigentümer ihre Privatsphäre durch das Fotografieren ihrer Häuser verletzt sahen. Wenn der Sinn für die Unterscheidung privat/öffentlich nicht verloren gegangen ist, dann bedeutet dies für den Umgang mit sozialen Medien: Die neuen Technologien, ihre Nutzungsbedingungen und -konsequenzen müssen auch und gerade in Bezug auf die Unterscheidung privat/(teil-)öffentlich erst erlernt und berechenbar werden.

4 Die Ambivalenz öffentlicher Privatheit

Auch wenn immer wieder konstatiert werden muss, dass die Grenzziehung zwischen Privatheit und Öffentlichkeit nicht statisch sein kann, also Wandlungsprozessen unterworfen ist, wird die *Privatisierung der Öffentlichkeit* vielfach als Verfallsgeschichte beschrieben. Sie sei getrieben von dem »bizarren Drang, dem Privaten und Intimen den Rang eines öffentlichen Ereignisses zu geben«[14] – einhergehend mit der Gefahr der Entpolitisierung des öffentlichen Raums.[15] Demgegenüber stehen die Befürworter der »transparenten Gesellschaft«[16] (siehe auch den Beitrag von Seemann in diesem Band, S. 243 ff.): Sie betonen – auch unter Rekurs auf die Geschlechterforschung und der feministischen Kritik am Privatheitsbegriff (»Das Private ist politisch!«) – die Vorzüge und Notwendigkeiten der Durchdringung der Öffentlichkeit mit privaten und alltagsrelevanten Themen[17], zum Beispiel im Zusammenhang mit häuslicher Gewalt oder der Vernachlässigung von Kindern. Die Diskussionen und Wertungen rund um das Verhältnis von Privatheit und Öffentlichkeit und die Rolle der Medien sind damit mindestens ebenso ambivalent wie die Unterscheidung zwischen den beiden Sphären selbst.

Unter der *Privatisierung des Öffentlichen*[18] wird zudem auch eine Personalisierung des Politischen diskutiert, in deren Verlauf die Person des Politikers/der Politikerin wichtiger als die zu verhandelnden Themen zu werden scheint. Der Medientheoretiker Joshua Meyrowitz unterscheidet in diesem Zusammenhang zum Beispiel zwischen *privat-öffentlichen* und *öffentlich-öffentlichen* Ereignissen und führt als Beispiel die Veränderungen bei politischen Interviews an, die früher auch einen persönlichen und privaten Austausch zwischen Politiker und Journalist beinhalteten und damit

ein *privat-öffentliches* Ereignis waren, über das dann journalistisch im Nachgang berichtet wurde[19]. Das Fernsehinterview mache diese Situation zu einer *öffentlich-öffentlichen*, in der die Interaktionen zwischen Politiker und Journalist sowie zwischen Politiker und Öffentlichkeit vermischt werden. Eine derartige *Medialisierung der Politik*[20] kann bis zu einer medientauglichen Inszenierung des Privaten durch Politiker führen.

Eine solche Inszenierung des Privaten, die auch maßgeblich dramaturgisches Element vieler Formate des → *Reality-TV* ist,[21] lässt sich als *öffentlich-privates* Ereignis bezeichnen, welches immer schon im Hinblick auf seine Veröffentlichung gedacht und gemacht ist.[22] Werden sie von den Zuschauerinnen und Zuschauern als Inszenierung enttarnt, können sie durchaus auch zu nachteiligen Folgen, etwa zu Glaubwürdigkeitsverlusten bei Politikern, führen. Als *öffentlich-privat* lassen sich auch die vielen Ereignisse charakterisieren, die im Zentrum der Prominentenberichterstattung (nicht nur) in der Boulevardpresse stehen. Sie steht für den »Januskopf der Prominenz«[23]: Zwar beklagt (Medien-)Prominenz häufig den Verlust von Privatleben, inszeniert gleichzeitig öffentliche Privatheit aber zur Erhaltung des Prominentenstatus.

Aber auch unzählige (noch) nicht prominente Menschen sind offenbar für den Gegenwert medialer Aufmerksamkeit bereit, Privates und Intimes aus dem eigenen Leben und dem anderer in den Medien und über die vielfältigen Kanäle im Internet zu offenbaren. Das Verhältnis von Privatheit und Öffentlichkeit muss offensichtlich mit dem Aufkommen jedes neuen Mediums, jeder neuen Medientechnologie neu ausgehandelt werden.

Anmerkungen

1 Christian Pundt, Medien und Diskurs, Zur Skandalisierung von Privatheit in der Geschichte des Fernsehens, Bielefeld 2008, S. 234.
2 Vgl. Sandra Seubert, Privatheit und Öffentlichkeit heute. Ein Problemaufriss, in: Sandra Seubert/Peter Niesen (Hrsg.), Die Grenzen des Privaten, Band 16 der Schriftenreihe der Sektion Politische Theorien und Ideengeschichte in der Deutschen Vereinigung für Politische Wissenschaft, Baden-Baden 2010.
3 Vgl. Pundt 2008 (Anm. 1); Ralph Weiß/Jo Groebel (Hrsg.), Privatheit im öffentlichen Raum, Medienhandeln zwischen Individualisierung und Entgrenzung, Opladen 2002.
4 Vgl. Joan Kristin Bleicher, Formatiertes Privatleben: Muster der Inszenierung von Privatem in der Programmgeschichte des deutschen Fernsehens, in: Ralph Weiß/Jo Groebel (Hrsg.), Privatheit im öffentlichen Raum, Medienhandeln zwischen Individualisierung und Entgrenzung, Opladen 2002, S. 208 f.
5 Vgl. Günter Burkart, Das Mobiltelefon: Grenzverschiebungen zwischen Privatsphäre und Öffentlichkeit durch technisch vermittelte Kommunikation, in: Korne-

lia Hahn (Hrsg.), Öffentlichkeit und Offenbarung, Eine interdisziplinäre Mediendiskussion, Konstanz 2002.

6 Vgl. Beate Rössler, Der Wert des Privaten, Frankfurt/M. 2001, S. 311.

7 Klaus Neumann-Braun, Internet Kameras/Web Cams – die digitale Veröffentlichung des Privaten, in: Kornelia Hahn (Hrsg.), Öffentlichkeit und Offenbarung, Eine interdisziplinäre Mediendiskussion, Konstanz 2002, S. 117.

8 Vgl. Steffen Burkhardt, »Wir stürzen ab.« Mediale Selbstbespiegelung zwischen Integrität und Indiskretion am Beispiel Michel Friedmann, in: Michael Beuthner/Stephan Alexander Weichert (Hrsg.), Die Selbstbeobachtungsfalle. Grenzen und Grenzgänge des Medienjournalismus, Wiesbaden 2005.

9 Vgl. Udo Branahl, Medienrecht, Eine Einführung, Wiesbaden 2009.

10 Vgl. Tobias Eberwein/Horst Pöttker, Journalistische Recherche im Social Web: Neue Potenziale, neue Probleme?, in: Zeitschrift für Kommunikationsökologie und Medienethik, 11 (1/2009), S. 23–32.

11 Susan Barnes, A privacy paradox: Social networking in the United States, in: First Monday, 11 (2006) 9, im Internet unter http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/issue/view/203 (13.11.2011).

12 S. Rössler 2001 (Anm. 6), S. 309.

13 Ebd., S. 312.

14 Thomas Jung/Stefan Müller-Doohm, Das Tabu, das Geheimnis und das Private – Vom Verlust der Diskretion, in: Kurt Imhof/Peter Schulz (Hrsg.), Die Veröffentlichung des Privaten – Die Privatisierung des Öffentlichen, Opladen 1998, S. 14.

15 Vgl. Richard Sennett, Verfall und Ende des öffentlichen Lebens. Die Tyrannei der Intimität, Frankfurt/M. 1983.

16 Gianni Vattimo, Die transparente Gesellschaft, Wien 1992.

17 Vgl. Frederike Herrmann/Margret Lünenborg (Hrsg.), Tabubruch als Programm. Privates und Intimes in den Medien, Opladen 2001; Elisabeth Klaus, Das Öffentliche im Privaten – Das Private im Öffentlichen. Ein kommunikationstheoretischer Ansatz, in: Herrmann/Lünenborg 2001 (ebd.).

18 Vgl. Imhof/Schulz, Opladen 1998 (Anm. 14).

19 S. Joshua Meyrowitz, Der Politische Held wird vom Sockel gestoßen, in: Joshua Meyrowitz, Die Fernseh-Gesellschaft. Wirklichkeit und Identität im Medienzeitalter, Weinheim/Basel 1987, S. 193.

20 Vgl. unter anderem Ulrich Sarcinelli, Politische Kommunikation in Deutschland : Zur Politikvermittlung im demokratischen System, Wiesbaden 2009, S. 109 ff.

21 Vgl. Elisabeth Klaus, Fernsehreifer Alltag: Reality TV als neue, gesellschaftsgebundene Angebotsform des Fernsehens, in: Tanja Thomas (Hrsg.), Medienkultur und soziales Handeln, Wiesbaden 2008.

22 Vgl. Paula Diehl, Zwischen dem Privaten und dem Politischen – Die neue Körperinszenierung der Politiker, in: Seubert/Niesen 2010 (Anm. 2).

23 Ulrich F. Schneider, Der Januskopf der Prominenz, Zum ambivalenten Verhältnis von Privatheit und Öffentlichkeit, Wiesbaden 2004.

Sabine Trepte

Privatsphäre aus psychologischer Sicht

Eine wichtige Funktion des Datenschutzes ist, dass Menschen selbstbestimmt über die Weitergabe und Verwendung ihrer persönlichen Daten entscheiden können – auch und insbesondere, um ihre Privatsphäre zu wahren. Privatsphäre wird oft als »das Recht, allein gelassen zu werden« bezeichnet. Dieses Recht können Menschen heute nur in Anspruch nehmen, wenn ein ausreichender Datenschutz gewährleistet ist.

Privatsphäre ist psychologisch gesehen lebensnotwendig. Kinder brauchen Privatsphäre, um ohne Bewertungsangst etwas auszuprobieren. Sie erwerben auf diesem Weg wichtige motorische und kognitive Fertigkeiten. Jugendliche brauchen Privatsphäre, um eigenständig denken und selbstbewusst handeln zu lernen. Erwachsene brauchen Privatsphäre, um sich persönlich und beruflich weiter zu entwickeln. Erholung, Muße und Kreativität können nur entstehen, wenn Menschen ein für sie optimales Maß an Privatsphäre herstellen können.

Gleichzeitig brauchen wir jedoch den Kontakt und die Beziehungen zu anderen Menschen. Menschliche Beziehungen sind nur möglich, wenn wir uns selbst offenbaren, indem wir etwas von uns preisgeben. Wenn zwei Menschen aufeinandertreffen, so ist ihre Begegnung und ihr Austausch dadurch bestimmt, wie viel beide voneinander berichten. Die Selbstoffenbarung ist so gesehen der Treibstoff jeder Beziehung und damit ebenso lebensnotwendig wie Privatsphäre. Privatsphäre und Selbstoffenbarung sind zwei gegensätzliche Pole, zwischen denen wir uns tagtäglich bewegen. Ständig handeln wir – oft auch unbewusst – die Grenzen unserer Privatsphäre und unserer Selbstoffenbarung mit anderen, aber auch mit uns selbst aus.

Bis in die 1960er Jahre hinein hat sich die Psychologie kaum mit dem Thema Privatsphäre beschäftigt. Aufgrund der seitdem vollzogenen technischen und politischen Entwicklungen wurde das Thema immer relevanter.[1] In diesem Beitrag wird die Essenz der psychologischen Forschung zusammengefasst. Dabei sollen folgende Fragen beantwortet werden: Was ist eigentlich Privatsphäre? Gibt es ein optimales Maß an Privatsphäre? Welche Folgen hat es, wenn die Privatsphäre gestört wird? Wie gehen Menschen im → *Social Web*, zum Beispiel in → sozialen Netzwerken wie *Facebook*, mit ihrer Privatsphäre um?

1 Was ist Privatsphäre?

Privatsphäre beschreibt, inwieweit ein Mensch anderen Menschen Zutritt zu seiner eigenen Welt gewährt.[2] Es geht also darum, Grenzen auszuhandeln. Privatsphäre ist die Bezeichnung für einen Optimierungsprozess, der während der Interaktion mit anderen Menschen abläuft. Besonders wichtig wird Menschen dieses Aushandeln von Privatsphäre, wenn sie andere Menschen neu kennenlernen. Aber auch in bestehenden Beziehungen kommen immer wieder die Fragen auf: Wie viel möchte ich von mir preisgeben? Was möchte ich lieber für mich behalten?

Um Privatsphäre zu erlangen und aufrecht zu erhalten, wird verbales (Sprache), paraverbales (Mimik, Gestik) und territoriales Verhalten (physische oder architektonische Gestaltung von Räumen) angewandt. Anne Vinsel und ihre Kollegen haben in den USA 1980 in einem Studentenwohnheim untersucht, mit welchen Methoden dort Studierende ihre Privatsphäre aufrecht erhalten.[3] Ihre Untersuchung zeigt, dass die mit Blick auf die eigene Privatsphäre zufriedeneren Studierenden sich vor allem dadurch auszeichneten, dass sie in der Lage waren, ihre Privatsphäre zu regulieren. Sie suchten zwar insgesamt mehr Kontakt zu anderen Kommilitonen, wandten aber zugleich auch mehr Techniken an, um Kontakte zu vermeiden (etwa durch das Verschließen ihrer Zimmertür, Alleine-Spaziergänge oder die Nutzung der Gemeinschaftsräume zu Zeiten, in denen wenige andere Personen dort waren). Das entscheidende Kriterium für die erfolgreiche Regulierung der Privatsphäre ist also auf der einen Seite die Offenheit und die Preisgabe von Informationen an andere, und zum anderen der gezielte Rückzug und die Einsamkeit.

Das ideale Ausmaß von Privatsphäre ist von Mensch zu Mensch (*inter*individuell) sehr unterschiedlich. Manche Menschen brauchen weniger Zeit der Zurückgezogenheit und andere mehr, um sich zu erholen. Manche Menschen müssen sich anderen öffnen, um ein Problem zu lösen, und andere finden bessere Lösungen, wenn sie allein darüber nachdenken. Auch für ein und dieselbe Person ist das ideale Ausmaß an Privatsphäre zu verschiedenen Zeitpunkten (*intra*individuell) unterschiedlich. An manchen Tagen und in manchen Situationen ist mehr Privatsphäre wohltuend, an anderen Tagen weniger.

Wenn umgangssprachlich von »Privatsphäre« gesprochen wird, dann bezieht sich der Begriff auf unterschiedliche Situationen. Kinder hängen beispielsweise ein Schild an die Türklinke ihres Zimmers, wenn sie von ihren Eltern nicht gestört werden möchten. Erwachsene fühlen sich in ihrer Privatsphäre verletzt, wenn ein Nachbar in der U-Bahn ihrer Unterhaltung zuhört oder sie ein Foto von sich im Internet entdecken, das sie nicht freigegeben haben.

Wissenschaftlich unterscheidet man verschiedene Formen der Privatsphäre: physische, psychologische, soziale und informationsbezogene Privatsphäre. Diese Kategorisierung dient der Vereinfachung des komplexen Konstrukts Privatsphäre, um besser zu verdeutlichen, in welchen Lebensbereichen sich Menschen mit Privatsphäre befassen und diese aushandeln.[4]

- *Physische Privatsphäre* beschreibt, inwieweit Menschen für andere physisch zugänglich sind. Es gibt zahlreiche Experimente, die belegen, dass die physische Privatsphäre starke Auswirkungen auf das individuelle Wohlbefinden, auf das Empfinden von Stress und auf die körperliche Gesundheit hat. Das Ausmaß der physischen Privatsphäre wird durch verschiedene Aspekte beeinflusst. Dazu gehört der Umfang des Territoriums, das eine Person kontrollieren kann, für das sie also bestimmen kann, welche Bedingungen der Privatsphäre dort gelten und mit welcher Wahrscheinlichkeit diese Regeln eingehalten werden. In unserer Gesellschaft bilden unser »Zuhause«, also der von uns selbst gestaltete Wohnraum, zu dem wir nur ausgewählten Personen Zutritt gestatten, und unser Körper sowie seine unmittelbare Umgebung den Kern dessen, was wir als physische Privatsphäre ansehen.
- *Psychologische Privatsphäre* beschreibt unsere Kontrolle über emotionalen und gedanklichen In- und Output. Wenn also ein hohes Maß an psychologischer Privatsphäre vorhanden ist, so können wir frei denken, unsere Meinungen und Werte frei formulieren. Wir können entscheiden, wann und mit wem wir Gefühle teilen möchten, wen wir um Unterstützung und Rat bitten möchten. Psychologische Privatsphäre hat viele funktionale Komponenten. Sie trägt beispielsweise entscheidend dazu bei, wie Menschen ihre eigene Identität entwickeln. Dazu grenzen sie sich von anderen ab. Sie emanzipieren sich sowohl von ihren Eltern als auch zeitweise von ihren Freundinnen und Freunden. Nur diese Emanzipation trägt dazu bei, dass Menschen das Eigene und Besondere ihrer Identität in Abgrenzung zu anderen kennenlernen. Metaphorisch kann man sich dieses Aushandeln zwischen Nähe und Privatsphäre vorstellen wie die Arbeit eines Schauspielers. »Hinter der Bühne« (*backstage*) entwickeln Menschen unter den Bedingungen psychologischer Privatsphäre ihre Identität und ihre Rolle. Dabei greifen sie auf den Rat und die Hilfe anderer vertrauter Menschen zurück. »Auf der Bühne« (*on stage*) interagieren sie mit anderen. So wichtig die psychologische Privatsphäre zur Identitätsentwicklung auch ist, ein Leben ohne »Publikum«, also ohne andere Menschen, hätte gesundheitlich und emotional ebenso negative Folgen wie ein Leben ohne Privatsphäre.
- *Soziale Privatsphäre* umfasst den dialektischen Prozess, Nähe zu bestimmten Menschen herzustellen und Distanz zu anderen aufzubauen. Sie ist

erreicht, wenn man die Kontrolle über die Form und das Ausmaß sozialer Interaktionen hat. Unter Bedingungen sozialer Privatsphäre können sich Menschen von anderen zurückziehen und somit von den Erwartungen und Anforderungen anderer befreien. Dies ist manchmal erforderlich, um gedanklich zu planen oder Verhaltensweisen auszuprobieren. Ebenso wie die psychologische und physische beeinflusst auch die soziale Privatsphäre das individuelle Wohlbefinden. Darüber hinaus trägt das harmonische Aushandeln sozialer Privatsphäre dazu bei, dass Gemeinschaften und Gesellschaften funktionieren.

- *Informationsbezogene Privatsphäre* bezieht sich darauf, ob ein Mensch Kontrolle darüber hat, welche und wie viel Informationen an andere Personen weitergegeben werden. Gerade die informationsbezogene Privatsphäre ist seit den 1960er Jahren gesellschaftlich zunehmend bedeutsam geworden, weil auf elektronischem Weg Daten gesammelt und gespeichert werden, ohne dass die Betroffenen davon wissen. Jeder Zahlungsvorgang mit einer Kreditkarte, die Teilnahme an einem Preisausschreiben oder die Verwendung einer Kundenkarte führen dazu, dass personenbezogene Daten gesammelt werden. Häufig werden diese Daten sogar ohne Wissen der Personen weiterverwendet.

2 Warum brauchen Menschen Privatsphäre?

Welchen Nutzen hat nun die Privatsphäre für Menschen? Warum möchten und müssen wir manchmal allein oder im engsten Freundes- oder Familienkreis sein? Die Fragen hat Westin 1967 als einer der ersten Forscher zur Privatsphäre sehr gut beantwortet[5] (siehe Infokasten).

Funktionen der Privatsphäre

1. Autonomie: soziale Normen durchbrechen, mit neuem Verhalten und Gedanken experimentieren
2. Emotionale Erleichterung: in wertfreier Umgebung – allein oder mit anderen – sich den Anforderungen und der Stimulation der Umwelt entziehen
3. Selbstevaluation: aufrichtig zwischen den persönlichen Idealen und der eigenen Leistung abwägen
4. Geschützte Kommunikation: eine Situation, in der anderen Einblicke in das „wahre Ich" gewährt werden und in denen die mentale Distanz gering ist

Eigene Zusammenfassung nach Alan F. Westin, Privacy and Freedom, New York 1967.

Inzwischen haben viele weitere Wissenschaftlerinnen und Wissenschaftler seine Erkenntnisse um Studien erweitert, in denen Menschen genau danach gefragt wurden, welchen Nutzen Privatsphäre für sie hat. Dabei kamen sie zu folgenden Ergebnissen:

Allein oder unter befreundeten Personen ist es möglich, bewertungs- und angstfrei neue Gedanken oder Ideen auszudrücken. Dieses Empfinden der Autonomie ermöglicht das gedankliche und gefühlsmäßige Experimentieren, das ein menschliches Grundbedürfnis darstellt. Sich in einer wertfreien Umgebung ausprobieren und seinen Gedanken freien Lauf lassen zu können, ist eine Voraussetzung für die Entwicklung des eigenständigen Denkens und Handelns. Jugendliche und Erwachsene brauchen eine geschützte Umgebung, um sich selbst zu bewerten und ihre Gedanken und Gefühle ohne sozialen Druck äußern zu können. Privatsphäre ist erforderlich, um die eigene Identität und Individualität zu entwickeln, sie ist eine Voraussetzung für Freiheit.

Eine private Umgebung verschafft darüber hinaus emotionale Erleichterung, da Menschen darin unterschiedliche Rollen, die sie im beruflichen und privaten Austausch spielen, sowie aufgezwungene Masken ablegen können. Im Rahmen der Privatsphäre können sie sich in notwendigen Erholungspausen vom emotionalen Druck entlasten, den sie bisweilen in beruflichen und privaten Beziehungen erfahren.

Privatsphäre dient auch als Raum des Rückzugs der Verarbeitung vergangener Ereignisse. Unter ihrem Schutz kann jene Selbstevaluation stattfinden, die hilfreich sein kann, das eigene Verhalten zu reflektieren und gegebenenfalls zu ändern. Studien zur Kreativität zeigen sehr anschaulich, dass gerade in einem Zustand der Einsamkeit, des Rückzugs und des Tagträumens kreative Gedanken möglich sind.

Eine weitere wichtige Funktion der Privatsphäre ist die geschützte Kommunikation. So paradox es klingt: Die zentrale Funktion der Privatsphäre ist hier die Selbstoffenbarung. Gerade in krisenhaften Situationen kann es wichtig sein, dass wir allein (zum Beispiel in einem Tagebuch) oder im Beisein von vertrauten Menschen uns etwas »von der Seele reden« können. Für die Rückgewinnung der Handlungsfreiheit kann es von Bedeutung sein, etwa moralisch fragwürdige Gedanken oder ambivalente Gefühle anderen Menschen anzuvertrauen, mit ihnen frei – ohne Angst vor Abwertung oder Ausgrenzung – darüber sprechen zu können.

Ein weiterer Nutzen der Privatsphäre liegt darin, dass wir uns verschiedene Verhaltensoptionen offen halten, wenn wir zunächst weniger von uns preisgeben. Es ist ein gut fundiertes psychologisches Prinzip, dass Menschen in ihrem Denken und Handeln nach Konsistenz streben. Wenn eine

Person also bestimmte Gedanken äußert, so wird von ihr auch erwartet, dass sie sich dementsprechend verhält, ihr Handeln und Reden also konsistent sind. Dies nur privat zu offenbaren, hält den Menschen mehr Verhaltensoptionen offen, sie fühlen sich weniger verletzbar.

3 Warum möchten Menschen etwas von sich preisgeben?

Bisher haben wir uns vor allem der Frage gewidmet, welchen Nutzen und welche Funktion die Aufrechterhaltung der Privatsphäre hat. Welchen Nutzen kann es im Gegenzug haben, sich selbst zu offenbaren? Wie bereits erwähnt, können Beziehungen nur entstehen und aufrechterhalten werden, wenn Menschen etwas von sich preisgeben.

Darüber hinaus spielt die Selbstoffenbarung bei der Suche nach Identität eine wichtige Rolle. Nur wenn andere an den eigenen Gedanken teilhaben, können diese auch erprobt und einer Realitätsprüfung unterzogen werden. So zeigte sich in einer Studie von Meifen Wei, einer Professorin aus den USA, dass College-Studierende, die nichts von sich preisgaben, einsamer und trauriger waren als vergleichsweise offene Menschen.[6] Menschen, die ein überdurchschnittlich hohes Bedürfnis nach Privatsphäre haben, werden in der Interaktion von anderen als angespannt oder unnatürlich wahrgenommen. Obwohl Personen mit einem stärkeren Bedürfnis nach Privatsphäre sehr gern andere Menschen kennenlernen möchten, fällt es ihnen manchmal schwer, in einem Gespräch positive Signale zu setzen und so eine »belohnende« Gesprächssituation für das Gegenüber zu schaffen. Die Selbstoffenbarung eigener psychischer Belastungen fördert laut aktuellen Studien den Zugang zu sozialer Unterstützung und erhöht das Selbstvertrauen sowie die allgemeine Lebenszufriedenheit der betroffenen Personen.[7]

4 Privatsphäre im Internet

In jüngerer Zeit hat das Thema Privatsphäre vor allem im Kontext der Veröffentlichung privater Daten im Internet (zum Beispiel in →sozialen Netzwerken wie *Facebook* oder StudiVZ) gesellschaftliche und politische Debatten angeregt. Viele Menschen fragen sich, wie viel Selbstoffenbarung für sie gut ist und ab wann ihre Privatsphäre verletzt wird. Auch dazu wurden wissenschaftliche Studien durchgeführt.[8] In diesem Zusammenhang wird die Frage relevant, ob sich Menschen gerade deshalb bei der Inter-

netnutzung wohl fühlen, weil sie dort die Möglichkeit haben, etwas von sich preiszugeben. Tatsächlich zeigt die Forschung, dass Menschen, die viel von sich offenbaren, besonders gern *online* sind. Doch was bedeutet es für die Gesellschaft, wenn alle zunehmend mehr von sich preisgeben und die individuellen Grenzen sich zusehends verschieben?

Internationale Studien zeigen, dass sich Menschen heute wesentlich mehr um ihre Privatsphäre sorgen, als dies noch vor zehn oder 30 Jahren der Fall war.[9] Die Privatsphäre sehen viele vor allem durch den Informationsfluss im Internet bedroht oder verletzt. Die meisten privaten Informationen verbreiten freilich die Nutzenden selbst auf sozialen Netzwerken oder anderen Angeboten des → *Social Web*, in das sie ihre Inhalte einstellen und – mehr oder weniger öffentlich – mit anderen kommunizieren (siehe auch die Beiträge von Schmidt, S. 215 ff. und Wagner/Gebel/Brüggen, S. 226 ff. in diesem Band). Studien belegen, dass gerade die Kontaktaufnahme zu anderen und der Austausch mit ihnen das Motiv für eine Beteiligung in den sozialen Netzwerken ist, was die Veröffentlichung privater bis zum Teil intimer Details einschließt. Viele Profile sind öffentlich, also über das Internet frei recherchierbar, ohne dass ein Einloggen in die Netzwerke erforderlich wäre. Auch im *Social Web* gilt, dass nur Personen, die etwas von sich offenbaren, mit anderen in Kontakt treten und mit ihnen Beziehungen aufbauen können. Dementsprechend sind vor allem solche Menschen im Netz aktiv, die – wie bereits oben erwähnt – dort gern etwas von sich preisgeben möchten.[10]

5 Wandel der Privatsphäre?

Aus psychologischer Sicht hat die Balance zwischen Privatsphäre und Selbstoffenbarung einen nennenswerten Einfluss auf unsere Beziehungen zu anderen Menschen. Praktische Relevanz erhält das Thema Privatsphäre zunehmend dadurch, dass die psychologische und physische Privatsphäre durch die Verarbeitung und Weitergabe von Daten beeinflusst wird. In Zukunft wird dieses Thema gerade deshalb relevant bleiben, weil neue Formen der Datenverarbeitung verfügbar sind, mit denen mehr private Informationen als bisher preisgegeben werden können. Mit den zahlreichen Angeboten der Vernetzung und des ständigen Austauschs wird unser bisher gültiges Konzept der Privatsphäre in Frage gestellt.

Anmerkungen

1 Irwin Altman, Privacy: A conceptual analysis, in: Environment and Behavior, Bd. 8 (1/1976), S. 7–29.
2 Ebd.; sowie Irwin Altman, The environment and social behavior: Privacy, personal space, territory, crowding, Monterey 1975.
3 Anne Vinsel u. a., Privacy regulation, territorial displays, and effectiveness of individual functioning, in: Journal of Personality and Social Psychology, Bd. 39 (6/1980), S. 1104–1115.
4 Judee K. Burgoon, Privacy and communication, in: Michael Burgoon (Hrsg.), Communication yearbook Bd. 6, Beverly Hills 1982, S. 206–249.
5 Alan F. Westin, Privacy and Freedom, New York 1967.
6 Meifen Wei/Daniel W. Russel/Robyn A. Zakalik, Adult attachment, social self-efficacy, self-disclosure, loneliness, and subsequent depression for freshman college students: A longitudinal study, in: Journal of Counseling Psychology, Bd. 52 (4/2005), S. 602–614.
7 Joseph P. Forgas, Affective influences on self-disclosure: Mood effects on the intimacy and reciprocity of disclosing personal information, in: Journal of Personality and Social Psychology, Bd. 100 (3/2011), S. 449–461.
8 Sabine Trepte/Leonard Reinecke (Hrsg.), Privacy online: Perspectives on privacy and self-disclosure in the social web, Heidelberg 2011.
9 European Commission: Eurobarometer. Attitudes on data protection and electronic identity in the European Union, Brüssel 2011, im Internet unter http://ec.europa.eu/public_opinion/archives/ebs/ebs_335_en.pdf.
10 Siehe Trepte/Reinecke 2011 (Anm. 8).

Hans-Jürgen Papier

Verfassungsrechtliche Grundlegung des Datenschutzes

Stellt man sich die Frage nach den verfassungsrechtlichen Vorgaben für das Datenschutzrecht, schaut man selbstverständlich zunächst im Grundgesetz (GG) nach. In dessen ersten Abschnitt finden sich zwar einige Grundrechte, die sich mit speziellen Fragen des Datenschutzes beschäftigen. So regelt Artikel 10 GG das Post- und Fernmeldegeheimnis und Artikel 13 GG enthält Vorgaben für die Überwachung von Wohnungen. Diese Grundrechte betreffen aber nur einen sehr kleinen Ausschnitt der möglichen datenschutzrechtlich relevanten Maßnahmen des Staates. Ein ausdrückliches allgemeines »Grundrecht auf Datenschutz« – wie es nunmehr auf europäischer Ebene in Artikel 8 der Charta der Grundrechte der Europäischen Union enthalten ist – sucht man jedoch im Grundgesetz vergeblich.

Eine verfassungsrechtliche Grundlegung des Datenschutzes muss deshalb mit einer der bedeutendsten Entscheidungen des Bundesverfassungsgerichts beginnen, dem sogenannten Volkszählungsurteil vom 15. Dezember 1983[1]. Dort entwickelte das Bundesverfassungsgericht aus dem allgemeinen Persönlichkeitsrecht (Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG) das sogenannte Recht auf informationelle Selbstbestimmung. Erst seit dieser Entscheidung lässt sich folglich von einem »Grundrecht auf informationelle Selbstbestimmung« sprechen. Das Volkszählungsurteil stellt – mit den Worten des ehemaligen Richters des Bundesverfassungsgerichts Wolfgang Hoffmann-Riem – die *Magna Charta* des deutschen Datenschutzrechts dar.

Als Ausgangspunkt der verfassungsrechtlichen Grundlegung des Datenschutzrechts soll deshalb als erstes dieses Urteil genauer betrachtet werden.

1 Grundaussagen des Volkszählungsurteils

Hintergrund und Ergebnis der Entscheidung zum Volkszählungsurteil

Worüber hatte das Bundesverfassungsgericht 1983 in tatsächlicher Hinsicht zu entscheiden? In jenem Jahr sollte in der Bundesrepublik Deutschland eine umfassende Volkszählung durchgeführt werden. Das zu diesem

Zweck erlassene Volkszählungsgesetz hatte das Bundesverfassungsgericht zu überprüfen. Eine tatsächliche Besonderheit des Falles bestand darin, dass die durch das Gesetz angeordnete Volkszählung politisch und gesellschaftlich höchst umstritten war. Dies war vor allem auf die damals neuartigen Möglichkeiten der modernen Datenverarbeitung zurückzuführen, die in Teilen der Bevölkerung Angst vor einer unkontrollierbaren und totalen Erfassung ihrer persönlichen Daten auslöste – ein Szenario, wie es George Orwell in seinem berühmten Roman »1984« für das darauf folgende Jahr prognostiziert hatte.

In rechtlicher Hinsicht bestand das Problem in erster Linie darin, dass die für die Volkszählung erhobenen personenbezogenen Daten zugleich für andere Zwecke benutzt werden sollten: Die Melderegister sollten bei dieser Gelegenheit auf ihre Richtigkeit und Vollständigkeit hin überprüft und gegebenenfalls korrigiert werden. Das Bundesverfassungsgericht hielt dann auch die Datenerhebung für die Volkszählung als solche im Großen und Ganzen für verfassungskonform. Als verfassungswidrig befand es lediglich die Verwendung der Daten zu einem weiteren Zweck, der mit dem ersten nicht unmittelbar etwas zu tun hatte.

Um zu diesem Urteil zu gelangen, musste das Bundesverfassungsgericht aber zuerst einmal allgemeine verfassungsrechtliche Maßstäbe für den staatlichen Umgang mit personenbezogenen Daten entwickeln. Dies führte zu dem bereits eingangs beschriebenen »Recht auf informationelle Selbstbestimmung«, dessen Herleitung nun detaillierter untersucht werden soll.

Herleitung des Rechts auf informationelle Selbstbestimmung

Das Bundesverfassungsgericht verankerte das mit dem Volkszählungsurteil anerkannte »Recht auf informationelle Selbstbestimmung« im Mittelpunkt unserer grundgesetzlichen Ordnung, nämlich im Wert und der Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt. Sie wird durch das allgemeine Persönlichkeitsrecht aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG geschützt, das unter anderem auch das Recht am eigenen Bild oder vor verfälschenden oder entstellenden Darstellungen der eigenen Person schützt.[2]

Die Grenzen der zulässigen staatlichen Informationserhebung und -verarbeitung unter Bezug auf die Menschenwürde und das allgemeine Persönlichkeitsrecht zu bestimmen, diese Methode war freilich nicht neu. So hatte das Bundesverfassungsgericht bereits im Jahr 1970 in seiner Entscheidung zum sogenannten Mikrozensus – das ist die Erstellung einer Repräsentativstatistik der Bevölkerung und des Erwerbslebens – festge-

stellt, dass es mit der Menschenwürde nicht zu vereinbaren wäre, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich sei.[3]

Neu war im Volkszählungsurteil vielmehr, dass das Bundesverfassungsgericht die Vorgaben des allgemeinen Persönlichkeitsrechts an die modernen Bedingungen der automatischen Datenverarbeitung anpasste.[4] Die freie Entfaltung der Persönlichkeit setzt unter diesen Bedingungen voraus, die persönlichen Daten des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe zu schützen. Das Grundrecht auf informationelle Selbstbestimmung gewährleistet daher dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[5] Damit wurde die zuvor vom Bundesverfassungsgericht verwendete »Sphärenkonzeption«[6] zum Teil aufgegeben.[7]

Seit dem Volkszählungsurteil hängt die Beurteilung der Frage, inwieweit ein Datum als sensibel zu beurteilen ist, nicht mehr allein davon ab, ob es einen intimen Vorgang betrifft. Unter den Bedingungen der modernen Informationstechnologie gibt es nämlich kein von vornherein »belangloses Datum« mehr. Vielmehr bedarf es nun zur Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines Verwendungszusammenhangs.[8]

Die modernen Mittel der Datenverarbeitung erlauben zudem die beliebige Zusammenführung einmal erlangter Informationen, ohne dass der Einzelne die Richtigkeit und Verwendung kontrollieren könnte. Wer jedoch nicht mehr überschauen kann, wer in einer Gesellschaft was, wann und bei welcher Gelegenheit über einen weiß, wird in der freien Entfaltung seiner Persönlichkeit und in der Ausübung von Freiheitsrechten, die auch für die Mitwirkung in einem demokratischen Gemeinwesen von Bedeutung sind, gefährdet.[9]

Das Recht auf informationelle Selbstbestimmung hat nach dem Volkszählungsurteil allerdings nicht zur Folge, dass der Einzelne ein eigentumsgleiches Recht an »seinen Daten« hat.[10] Denn der Mensch ist Teil einer miteinander kommunizierenden Gemeinschaft. Eine Information, auch soweit sie personenbezogen ist, stellt ein Stück soziale Realität dar. Diese soziale Realität kann nicht ausschließlich dem Betroffenen zugeordnet werden, sie gehört ihm nicht allein. Aus diesem Grund muss die/der Einzelne auch Einschränkungen ihres/seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen.[11]

Datenschutzrechtliche Folgerungen

Welche konkreten Folgerungen zog das Volkszählungsurteil aus der genannten Einordnung des Datenschutzes als Grundrechtsschutz?[12] Eingriffe in das Recht auf informationelle Selbstbestimmung bedürfen nach dem Volkszählungsurteil zunächst einer hinreichend bestimmten gesetzlichen Grundlage.[13] Dabei muss der Gesetzgeber den Verwendungszweck der zu erhebenden Daten bereichsspezifisch, das heißt für den jeweiligen Verwendungsbereich wie etwa das Polizeirecht, und präzise festlegen.[14] Eine Weitergabe von Daten kommt grundsätzlich nur zu dem gleichen Zweck in Betracht, zu dem die Daten erhoben wurden. Die öffentliche Verwaltung ist keine »Informationseinheit«, innerhalb derer im Wege der Amtshilfe jede Information beschafft werden darf.[15] Zwar schließt die Zweckbindung einmal erhobener Daten eine nachträgliche Zweckänderung nicht aus. Diese Zweckänderung und die Übertragung der Daten an eine neue Stelle bedarf jedoch ihrerseits einer verfassungskonformen gesetzlichen Grundlage.[16] Erforderlich sind zudem verfahrensrechtliche Schutzvorkehrungen – wie Aufklärungs-, Auskunfts- und Löschungspflichten – sowie im Interesse eines vorgezogenen Rechtsschutzes die Beteiligung eines unabhängigen Datenschutzbeauftragten.[17]

2 Weitere Entwicklung des Rechts auf informationelle Selbstbestimmung

Die Vorgaben des Volkszählungsurteils führten im Jahr 1990 zu einer Novellierung des 13 Jahre alten Bundesdatenschutzgesetzes. Damit war die Entwicklung des Datenschutzes freilich nicht abgeschlossen. Das Bundesverfassungsgericht erließ auch in den folgenden Jahren zahlreiche zentrale Entscheidungen zum Recht auf informationelle Selbstbestimmung. Sie ergingen vor allem im Bereich der inneren Sicherheit und konzentrierten sich damit auf das Verhältnis zwischen dem Staat auf der einen und den Bürgerinnen und Bürgern auf der anderen Seite. Die Weiterentwicklung dieser sogenannten Abwehrdimension des Rechts auf informationelle Selbstbestimmung soll deshalb als erstes in den Blick genommen werden. Im Anschluss daran wird auf die sogenannte Schutzdimension des Grundrechts eingegangen. Sie betrifft die staatliche Ausgestaltung des Datenschutzes für das Verhältnis der Bürgerinnen und Bürger untereinander und gewinnt aktuell an Bedeutung.

Recht auf informationelle Selbstbestimmung als Abwehrrecht

Entsprechend dem klassischen Verständnis der Grundrechte hat auch das Recht auf informationelle Selbstbestimmung in erster Linie eine Abwehrfunktion. Bürgerinnen und Bürger können sich auf das Grundrecht berufen, um verfassungsrechtlich nicht gerechtfertigte Eingriffe in dessen Schutzbereich abzuwehren.

Die Abwehrdimension bildete den Schwerpunkt der Entscheidungen des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung seit dem Volkszählungsurteil. Dies lag vor allem daran, dass der Staat immer mehr Möglichkeiten zur Erfassung der personenbezogenen Daten Einzelner bekam. So wurden in den 1990er Jahren insbesondere zur Bekämpfung der organisierten Kriminalität neue Ermittlungsmethoden eingeführt, wie der »Kleine« und der →»Große Lauschangriff«,[18] und die erweiterten Befugnisse des Bundesnachrichtendienstes zur Überwachung der Telekommunikation.[19]

Nach den Terroranschlägen vom 11. September 2001 in den USA und vom 11. März 2004 in Madrid wurden in Deutschland sowie auf EU-Ebene weitere Maßnahmen beschlossen und durchgeführt, wie die präventive polizeiliche Rasterfahndung nach sogenannten »Schläfern«[20], die »*Online*-Durchsuchung«[21] von Computern oder die Vorratsspeicherung von Telekommunikationsverbindungsdaten.[22]

Damit steht das Recht auf informationelle Selbstbestimmung im Vergleich zur Zeit des Volkszählungsurteils vor neuen Herausforderungen. Sie haben ihren Grund allerdings nicht nur in neuen Gefahren, sondern auch in den revolutionären Veränderungen der Informations- und Kommunikationstechnologie. Dabei ist anzuerkennen: Der Staat kann diese technischen Veränderungen – schon um seiner grundrechtlichen Pflicht zum Schutz von Leib, Leben oder Freiheit seiner Bürgerinnen und Bürger aus Artikel 2 Absatz 2 GG zu genügen – bei der Gefahrenbekämpfung und Verfolgung von Straftaten nicht unberücksichtigt lassen.[23] Gleichwohl dürfen bei der Ausbalancierung von Freiheit und Sicherheit die Gewichte nicht grundlegend verschoben werden.[24]

Für Eingriffe in das Recht auf informationelle Selbstbestimmung ist zunächst, wie bei allen Grundrechten, der →Verhältnismäßigkeitsgrundsatz zu beachten, der ein angemessenes Verhältnis zwischen der Schwere des Eingriffs in das Grundrecht und dem Gewicht des Eingriffszwecks gebietet. Wegen der Bedeutung des Rechts auf informationelle Selbstbestimmung stellt er besondere Anforderungen an den Rang der zu schützenden Rechtsgüter sowie die Art und Intensität ihrer Gefährdung.[25] So sind

beispielsweise präventive polizeiliche Rasterfahndungen ohne Vorliegen einer konkreten Gefahr für hochrangige Rechtsgüter oder automatische Kraftfahrzeug-Kennzeichenüberwachungen ohne konkreten Anlass und ohne jede Konkretisierung der Verwendungszwecke mit dem Verhältnismäßigkeitsgrundsatz nicht zu vereinbaren[26] (siehe auch den Beitrag von Petri in diesem Band, S. 115 ff.).

Darüber hinaus darf – dies hat das Bundesverfassungsgericht seit seiner Anfangszeit immer wieder betont[27] – der Kernbereich privater Lebensgestaltung, der sich letztlich aus der Menschenwürdegarantie des Artikels 1 Absatz 1 GG ableitet, durch staatliche Überwachungsmaßnahmen nicht angetastet werden. Die Menschenwürde und der Menschenwürdegehalt spezieller Freiheitsrechte sind nämlich nicht gegenüber anderen Freiheitsrechten und den aus ihnen folgenden Schutzpflichten des Staates abwägbar oder gar »wegwägbar«. Demgegenüber müssen die anderen Grundrechte außerhalb ihres Menschenwürdekerns im Einzelfall zum Schutz kollidierender vorrangiger Grundrechtspositionen zurücktreten.

Entscheidung zur Vorratsdatenspeicherung

Einen weiteren verfassungsrechtlichen »Grenzpfahl« hat das Bundesverfassungsgericht mit seiner Entscheidung zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten vom März 2010 errichtet: Eine flächendeckende, vorsorgliche Erfassung und Speicherung von Daten, die praktisch alle Aktivitäten der Bürgerinnen und Bürger rekonstruierbar macht, ist mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar.[28] Selbst wenn eine lückenlose, staatliche Datensammlung vielleicht ein zusätzliches Maß an Sicherheit bedeutete, ist sie nicht mit unserer Verfassung in Einklang zu bringen, denn sie würde die Freiheitsausübung der Bürgerinnen und Bürger empfindlich einschränken. Die vorgesehene anlasslose Speicherung aller Telekommunikationsverkehrsdaten für den Zeitraum von sechs Monaten ist nur deshalb noch mit dem Grundgesetz vereinbar, weil sie eben nur die Verkehrsdaten (wer, wann mit wem kommuniziert), nicht aber die Inhalte der Kommunikation umfasst. Zugleich hob das Bundesverfassungsgericht hervor, dass die Existenz dieser Art der Vorratsdatenspeicherung den Spielraum für weitere ähnliche Datensammlungen aus dem oben genannten Grund stark beschränkt; derartige Vorratsdatenspeicherungen müssen die Ausnahme bleiben.

Darüber hinaus hat das Bundesverfassungsgericht in der Entscheidung zur Vorratsdatenspeicherung nochmals präzisiert, unter welchen Bedingungen in das Recht auf informationelle Selbstbestimmung eingegriffen

werden darf: Angesichts der Schwere des Eingriffs muss erstens ein besonders hoher Standard der Datensicherheit gewährleistet sein.[29] Zweitens dürfen die Daten nur zur Ahndung von Straftaten, die überragend wichtige Rechtsgüter verletzen oder bedrohen, oder zur Abwehr von Gefahren für solche Rechtsgüter verwendet werden.[30] Drittens muss der Gesetzgeber hinreichende Vorkehrungen zur Transparenz der Datenverwendung sowie zur Gewährleistung eines effektiven Rechtsschutzes treffen.[31] Die Entscheidung zur Vorratsdatenspeicherung betraf zwar den Anwendungsbereich von Artikel 10 GG (Brief-, Post- und Fernmeldegeheimnis); dieser stellt aber insoweit nur eine spezielle Normierung des Rechts auf informationelle Selbstbestimmung für den Bereich des Telekommunikationsverkehrs dar, so dass sich die verfassungsrechtlichen Vorgaben des Bundesverfassungsgerichts auf das allgemeine Recht auf informationelle Selbstbestimmung übertragen lassen.[32]

Entscheidung zur »*Online*-Durchsuchung«

Schließlich ist noch darauf hinzuweisen, dass das Recht auf informationelle Selbstbestimmung nach Maßgabe des Volkszählungsurteils mit der Entscheidung zur »*Online*-Durchsuchung« gewissermaßen eine »Schwester« bekommen hat, nämlich das »Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme«. Die Geburt dieser neuen »Tochter« des allgemeinen Persönlichkeitsrechts war notwendig, weil weder die speziellen Freiheitsrechte noch die übrigen Ausprägungen des allgemeinen Persönlichkeitsrechts gegen die Gefahren hinreichend Schutz gewähren, die sich aus der zunehmenden Nutzung der Informationstechnik ergeben.[33] Das Grundrecht in dieser neuen Ausprägung sichert den persönlichen Bereich nämlich auch dann, wenn auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten.[34] Die Vertraulichkeit und Integrität dieser Systeme erscheint inzwischen besonders schützenswert, weil der Einzelne wegen ihrer technischen Komplexität gar nicht mehr in der Lage ist, diese selbst beurteilen zu können – und dennoch darauf angewiesen ist.[35] Das Recht auf informationelle Selbstbestimmung liefe hier ins Leere, weil es nur die Daten und ihre Kommunikation, nicht aber das informationsverarbeitende System schützt.

Online-Durchsuchungen stellen einen schwerwiegenden Eingriff in die Vertraulichkeit und Integrität von IT-Systemen dar. Die Betroffenen können in der Regel die verdeckte Manipulation ihrer Systeme nicht bemerken. Deshalb gelten für die Zulässigkeit von *Online*-Durchsuchungen

besondere Vorgaben: Es müssen tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut wie Leib, Leben oder Freiheit der Person vorliegen und sie dürfen grundsätzlich nur auf richterliche Anordnung erfolgen.[36]

Gefahren für den Datenschutz durch Private – Grundrecht auf informationelle Selbstbestimmung als Grundlage staatlicher Schutzpflicht

Abschließend soll auf die Entwicklungen der Schutzdimension des Grundrechts auf informationelle Selbstbestimmung eingegangen werden. Wie bereits erwähnt, werden die Grundrechte traditionell als Abwehrrechte gegen den Staat verstanden. Bereits früh entwickelte das Bundesverfassungsgericht aus den Grundrechten aber auch gewisse Schutzpflichten des Staates. Der Staat ist aufgrund der mit den Grundrechten geschaffenen Wertordnung in bestimmtem Umfang dazu verpflichtet, die Bürgerinnen und Bürger vor einer Beeinträchtigung durch Private zu schützen. Das gilt auch im Schutzbereich des Rechts auf informationelle Selbstbestimmung.

Angesichts des andauernden technischen Fortschritts der Informations- und Kommunikationstechnologie und der internationalen Vernetzung der Informationswege liegt hier aktuell vielleicht die größte Herausforderung des Rechts auf informationelle Selbstbestimmung. Würden alle die irgendwo auf der Welt von privater Seite gespeicherten Informationen zusammengeführt, ließe sich sehr leicht ein »Persönlichkeitsprofil« von jeder Person erstellen. Dadurch würde der im Volkszählungsurteil für unzulässig befundene »Super-Gau des Datenschutzes« Wirklichkeit werden,[37] allerdings herbeigeführt durch die Hände Privater. Auch eine weitere, bereits eingangs zitierte Aussage des Volkszählungsurteils scheint im privaten Sektor neue Aktualität zu bekommen: »Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer, was, wann und bei welcher Gelegenheit über einen weiß«.

Das Grundrecht auf informationelle Selbstbestimmung im Sinne des Volkszählungsurteils fordert auch diesbezüglich den Schutz der Bürgerinnen und Bürger. Es verpflichtet den Staat, im Ausgleich mit konkurrierenden Freiheitsrechten ein angemessenes Schutzregime zu schaffen und durchzusetzen sowie sich auf internationaler Ebene für ein solches Regime einzusetzen.[38] Im Bereich der Schutzpflichten hat der Staat selbstverständlich eine größere Ausgestaltungsfreiheit als es bei der oben dargestellten Abwehrdimension des Rechts auf informationelle Selbstbestimmung der Fall ist. Dennoch muss er einen effektiven Schutz gegen Eingriffe von

privater Seite sicherstellen. Mindestanforderungen sind dabei insbesondere, dass der Zweck der Datenerhebung in einem angemessenen Verhältnis zu der Eingriffsintensität steht und dass die zu diesem bestimmten Zweck erhobenen Daten nicht ohne weiteres zu einem anderen Zweck benutzt werden dürfen. Darüber hinaus hat der Staat Private dazu zu verpflichten, die Sicherheit erhobener personenbezogener Daten zu gewährleisten. Schließlich muss bei heimlicher Datenerhebung grundsätzlich ein Anspruch des betroffenen Bürgers auf Benachrichtigung bzw. auf Auskunft bestehen, das heißt es muss für eine hinreichende Transparenz der Datenerhebung gesorgt werden.

Um einen ausreichenden Schutz des Rechts auf informationelle Selbstbestimmung auch in diesem Bereich zu sichern, wird sich der Staat häufig nicht mit bloßen Selbstverpflichtungen Privater begnügen dürfen. Er wird selbst eine verbindliche Ordnung konstituieren müssen, um der grundrechtlichen Werteordnung auch im Privatrechtsverkehr Geltung zu verschaffen. Denn nur auf der Grundlage gesetzlicher Regelungen sind effiziente Rechtsschutzmöglichkeiten gegeben. Bezeichnenderweise bezogen sich die letzten Novellen des Bundesdatenschutzgesetzes aus dem Jahr 2009 ganz überwiegend auf den privaten Bereich und haben beispielsweise den Adresshandel erschwert.

3 Zusammenfassung

Das Grundrecht auf informationelle Selbstbestimmung ergibt sich nicht unmittelbar aus dem Text der Verfassung. Es wurde vom Bundesverfassungsgericht im Volkszählungsurteil aus dem allgemeinen Persönlichkeitsrecht aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG hergeleitet. Das Bundesverfassungsgericht hat dort bereits detaillierte Anforderungen an die Ausgestaltung staatlicher Eingriffe in das Recht auf informationelle Selbstbestimmung entwickelt. Die späteren Entscheidungen des Bundesverfassungsgerichts, die in erster Linie das Recht auf informationelle Selbstbestimmung als Abwehrrecht gegen den Staat betrafen und im Bereich der inneren Sicherheit ergingen, haben die verfassungsgerichtlichen Vorgaben dieses jungen Grundrechts weiter präzisiert. Neue Herausforderungen für das Recht auf informationelle Selbstbestimmung betreffen vor allem die staatliche Schutzdimension, weil aktuell immer größere Gefährdungen des Datenschutzes von privaten Akteuren ausgehen. Hier muss der Staat in Zukunft seine verfassungsrechtliche Schutzverpflichtung aktiv wahrnehmen.

Anmerkungen

1 BVerfGE 65, 1 (41 ff.); Az. 1 BvR 209/83 u. a.
2 Vgl. jüngst: BVerfGE 119, 1 (24); Az. 1 BvR 1783/05.
3 Vgl. BVerfGE 27, 1 (6); Az. 1 BvL 19/63. Weitere Entscheidungen: BVerfGE 27, 344 (350 f.); Az. 1 BvR 13/68; 32, 373 (379); 44, 353 (372 f.).
4 Vgl. BVerfGE 65, 1 (42); 1 BvR 209/83 u. a.
5 Ebd., Rn. 43
6 Dieser Begriff verweist auf die sogenannte »Sphärentheorie« des Bundesverfassungsgerichts, die zur Bestimmung des Schutzbereichs von Art. 2 Abs. 1 GG entwickelt wurde. Vor dem Volkszählungsurteil wurden persönliche Daten abhängig davon geschützt, welcher »Sphäre« sie entstammten. Je nachdem, ob es sich um Bereiche der Intim-, Privat- oder Öffentlichkeitsphäre handelte, wurde ein weitergehender Schutz persönlicher Daten gewährleistet.
7 Nur »zum Teil« deshalb, weil das Bundesverfassungsgericht in der Folge daran festgehalten hat, dass wegen der besonderen Nähe zur Menschenwürde ein Kernbereich privater Lebensführung absolut geschützt bleibt, vgl. BVerfGE 109, 279 (310 ff.); Az. 1 BvR 2378/98; 1 BvR 1084/99; BVerfGE 119, 1 (29); Az. 1 BvR 1783/05.
8 Vgl. BVerfGE 65, 1 (45); Az. 1 BvR 209/83 u. a.; Trute, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, München 2003, 2.5 Rn. 10.
9 Vgl. BVerfGE 65, 1 (42f.); Az. 1 BvR 209/83 u .a.; zuletzt erneut bestätigt durch: BVerfGE 120, 274 (311f.).
10 Forderungen wie »Meine Daten gehören mir« (vgl. Renate Künast, »Meine Daten gehören mir« – und der Datenschutz ins Grundgesetz, Zeitschrift für Rechtspolitik (ZRP) 2008, S. 201) sind daher fragwürdig.
11 Vgl. BVerfGE 65, 1 (44); Az. 1 BvR 209/83 u. a.
12 Siehe dazu: Spiros Simitis, in: ders. (Hrsg.), BDSG, 6. Aufl., Baden-Baden 2006, Einleitung Rn. 30 ff.
13 Vgl. BVerfGE 65, 1 (44); Az. 1 BvR 209/83 u. a.
14 A. a. O.
15 A. a. O.
16 Vgl. BVerfGE 100, 313 (360); Az. 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95.
17 Vgl. BVerfGE 65, 1 (46); Az. 1 BvR 209/83 u. a.
18 Das heißt, die Überwachung von Gesprächen außerhalb (vgl. § 100c Abs. 1 Nr. 2 StPO in der Fassung des Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität vom 15.7.1992, BGBl I S. 1302) und innerhalb von Wohnungen (vgl. Art. 13 Abs. 3 bis 6 GG; § 100c in der Fassung des Gesetzes zur Verbesserung der Bekämpfung der Organisierten Kriminalität vom 4.5.1998, BGBl I S. 845, dazu: BVerfGE 109, 279; Az. 1 BvR 2378/98, 1084/99).
19 Vgl. das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses vom 13.8.1968, BGBl I S. 949 in der Fassung des Begleitgesetzes zum Telekommunikationsgesetz vom 17.12.1997, BGBl I S. 3108, vgl. dazu: BVerfGE 100, 313; Az. 1 BvR 2226/94, 1 BvR 2420/95, 1 BvR 2437/95.

20 Vgl. BVerfGE 115, 320.
21 Vgl. BVerfGE 120, 274.
22 Vgl. Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15.3.2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. Nr. L 105 vom 13.4.2006, S. 54; vgl. dazu: BVerfGE 122, 120.
23 Vgl. BVerfGE 120, 274 (319 f.); BVerfGE 120, 378 (428 f.).
24 Vgl. BVerfGE 115, 320 (360), siehe auch: Christine Hohmann-Dennhardt, Informationeller Selbstschutz als Bestandteil des Persönlichkeitsrechts, in: Recht der Datenverarbeitung (RDV) 2008, S. 1 ff.; Ulf Buermeyer, Verfassungsrechtliche Grenzen der »Online«-Durchsuchung, in: RDV 2008, S. 8 ff.
25 Vgl. BVerfGE 115, 320 (360).
26 Vgl. ebd., S. 320 (360 ff.); BVerfGE 120, 378 (430).
27 Vgl. BVerfGE 6, 32 (41); 27, 1 (6); 109, 279 (311 ff.).
28 BVerfGE 125, 260 (324 f.).
29 Ebd., S. 325.
30 Ebd., S. 377 ff.
31 Ebd., S. 334 ff.
32 Ebd., S. 310 ff.
33 Vgl. BVerfGE 120, 274 (303 ff.).
34 Ebd., S. 313 ff.
35 Vgl. Wolfgang Hoffmann-Riem, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JuristenZeitung (JZ) 2008, S. 1009 (1013, 1018).
36 BVerfGE 120, 274 (328 ff.).
37 Vgl. BVerfGE 65, 1 (42). S. dazu auch BVerfG in: NJW 2010, 833 (839).
38 Vgl. auch Wolfgang Hoffmann-Riem 2008 (Anm. 35), S. 1009 (1011 f., 1013); ders., Informationelle Selbstbestimmung in der Informationsgesellschaft – Auf dem Weg zu einem neuen Konzept des Datenschutzes, in: Archiv des öffentlichen Rechts (AöR) 123 (1998), S. 513 (524 ff.); Thomas Petri, Das Urteil des Bundesverfassungsgerichts zur »Online-Durchsuchung«, in: Datenschutz und Datensicherheit (DuD) 2008, S. 443 (446 f.); Winfried Hassemer, Partner Staat, in: Frankfurter Allgemeine Zeitung vom 4.7.2007, S. 6, im Internet unter: http://www.faz.net/themenarchiv/2.1198/recht-und-politik-partner-staat-1436365.html; Michael Ronellenfitsch, Von der informationellen Selbstbestimmung zum Mediengeheimnis – Zur Dynamik der Grundrechtsordnung, in: RDV 2008, S. 55 (58).

Marit Hansen

Überwachungstechnologie

1 Was ist Überwachung?

Überwachung bedeutet das zielgerichtete Beobachten einer Aktion, eines Objektes oder einer Person (Überwachungsziel) und das damit verbundene Sammeln von Informationen. Als »Überwachungstechnologien« werden dann all jene informationstechnischen Instrumente bezeichnet, die sich für diesen Zweck nutzen lassen. Auch Technik, die nicht als Überwachungsinstrument entwickelt wurde, kann ein solches Potenzial innehaben. So lassen sich zum Beispiel *Webcams* ebenso zur Beobachtung von Landschaften wie zur detaillierten Videoüberwachung von Personen nutzen.

Überwachung kommt in ganz unterschiedlichen Situationen zum Einsatz: So werden Überwachungsinstrumente verwendet, um Straftaten verhindern oder nachträglich leichter aufklären zu können. Detektive oder Geheimdienste setzen Überwachungsinstrumente ein, um das Verhalten von Menschen auszuspionieren. In Krankenhäusern dienen zahlreiche Instrumente dazu, die Lebensfunktionen und den Gesundheitszustand von Patienten zu überwachen. Ebenso werden beispielsweise in Kraftwerken die Betriebszustände von Maschinen kontrolliert. Überwachungsinstrumente zum sogenannten → *Tracking* ermöglichen es, die Bewegungen mobiler Kommunikationsgeräte (zum Beispiel Handys) bzw. deren Träger (Handynutzerinnen und -nutzer) nachzuverfolgen. Spezielle Programme zeichnen Nutzeraktionen im Internet auf, um aus derartigen Informationen beispielsweise Verhaltensmuster und Kundenprofile zu gewinnen und zielgerichtet Werbung einzublenden.

In vielen Fällen greift der Einsatz von Überwachungsinstrumenten in die Privatsphäre von Menschen ein.[1] Die Grenzen dessen, wer wen überwachen darf und wie weit eine (heimliche) Überwachung zulässig ist, werden vor allem durch das Recht auf informationelle Selbstbestimmung der überwachten Personen bestimmt. Auf der anderen Seite ist in einigen Fällen eine (nicht heimliche) Überwachung notwendig, um Datenschutzanforderungen zu erfüllen: So listet das Bundesdatenschutzgesetz in der Anlage zu § 9 Anforderungen an die Kontrolle der Verarbeitung personenbezogener Daten auf, beispielsweise »zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten

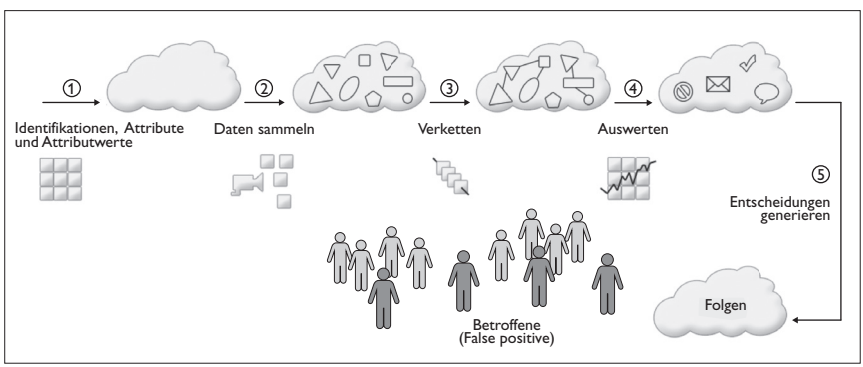
in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle)« (siehe dazu auch den Beitrag von Rost in diesem Band, S. 353 ff.). Dies bedeutet, dass für eine gewisse Zeit die Daten darüber vorgehalten werden müssen, welche Person an den entsprechenden Daten gearbeitet hat – also eine Art der Überwachung.

Doch selbst Einzelvorschriften zur Überwachung rechtfertigen keine Vollüberwachung der Menschen in all ihren Handlungen, sei es als Beschäftigte oder Konsumentinnen und Konsumenten. Dies hat das Bundesverfassungsgericht dazu bewogen, in seinem Urteil zur Volkszählung von 1983[2] vor den einschüchternden Effekten einer (möglichen) Überwachung zu warnen. Bei einer übermäßigen Überwachung bestünde die Gefahr, dass Bürgerinnen und Bürger ihre Grundrechte nicht mehr in Anspruch nehmen, weil sie negative Konsequenzen befürchten[3] (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.).

2 Verschiedene Phasen der Überwachung

Die Überwachung im engeren Sinn ist ein Bestandteil eines umfassenderen Prozesses von Informationsverarbeitung und -anreicherung: Wie man in Abbildung 1 sieht, werden Überwachungsinstrumente nicht nur beim unmittelbaren Beobachten und Datensammeln eingesetzt, sondern auch in anderen Phasen der Informationsanreicherung, etwa bei der Verkettung von Informationen oder in Entscheidungsprozessen.[4]

Abb. 1: Verschiedene Phasen der Informationsanreicherung



Quelle: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/Technische Universität Dresden, Verkettung digitaler Identitäten, Kiel 2007, S. 27.

Je nach Ziel und eingesetzten Instrumenten der Überwachung konzentriert sich die Informationserhebung auf verschiedene Daten, die beobachtet und gesammelt werden (Phase 1). In dieser ersten Phase werden Datenformate festgelegt und Werte zugeordnet: Dabei handelt es sich um Identifikatoren (IDs) und bestimmte Charakteristika (Attributwerte) zu bestimmten Personen oder zu Geräten in deren Besitz. Beispiele für Identifikatoren sind der Name einer Person, der in einer Datenbank einer Behörde oder eines Unternehmens gespeichert ist, Login-Namen, Computeradressen, Handy-Identifikationsnummern oder auch biometrische Merkmale der Person wie deren →DNA, Größe, Haarfarbe, Augenfarbe, Gesicht, Stimme usw. Einige dieser Daten sind unveränderlich, andere nicht; einige werden der betroffenen Person zugewiesen, andere kann sie selbst wählen.

Auf Basis dieses Datenmodells findet in Phase 2 die eigentliche Überwachung, nämlich die Beobachtung und Sammlung der vorhandenen Daten statt. Die erfassten Daten können wiederum mit anderen Informationen verkettet, das heißt in Beziehung gesetzt werden (Phase 3). Phase 4 dient der Auswertung der aus den vorherigen Phasen resultierenden Daten und bereitet damit den Entscheidungsprozess in Phase 5 mit möglichen Folgen für die betroffene Person vor. Eine polizeiliche Überwachung könnte beispielsweise darin resultieren, dass eine Person angeklagt wird oder eine Anklage sich als nicht begründet herausstellt. Ein Arbeitgeber könnte auf Basis der Überwachungsergebnisse eine Kündigung aussprechen oder mehr Leistung von dem Mitarbeiter oder der Mitarbeiterin einfordern. Ebenso ließen sich Einschätzungen bezüglich der Kreditwürdigkeit der Person, etwa vorliegenden Risiken aus Sicht eines Versicherungsunternehmens oder geeigneten Strategien für zielgruppenspezifische Produktwerbung treffen. Nicht immer wird die Überwachung über alle Phasen von einer einzigen Organisation vorgenommen, oft sind mehrere Akteure beteiligt.

3 Überwachung als visuelles Beobachten

Bereits die von Jeremy Bentham am Ende des 18. Jahrhunderts beschriebene Architektur eines »Panoptikums« stellt im weitesten Sinn eine Überwachungstechnologie dar.[5] Seine Idee bestand darin, eine effiziente Überwachung von Gefängnisinsassen oder Fabrikarbeitern durch wenige Wächter zu erreichen. Die Wächter (Überwacher) sind dafür in einem Beobachtungsturm in der Mitte des Gebäudes positioniert, von dem aus strahlenförmig gebaute Zelltrakte abgehen. So sind die Insassen beziehungsweise Arbeitenden jederzeit für ihre Überwacher einsehbar, während

von den Zellen aus nicht erkennbar wird, ob gerade ein Wächter anwesend ist. Die überwachten Menschen müssen also ständig damit rechnen, beobachtet zu werden. Dieses Prinzip der Ungewissheit gilt für viele Überwachungsinstrumente.

In dem Orwell'schen Klassiker »1984« bedient sich der »Big Brother« eines (fiktiven) Überwachungsinstruments namens »Telescreen«: ein Fernseher, der in beide Richtungen Bilder sendet und damit alles überträgt, was in den Wohnungen passiert.[6] Unsere heutigen Fernseher sind dazu – zum Glück – nicht geeignet. Allerdings sind zahlreiche technische Geräte verfügbar, um Wohnungen mit Video- und Akustiküberwachungsanlagen (sogenannte »Wanzen«) zu versehen (Phase 2 in Abbildung 1). Das entsprechende Detektivinstrumentarium ist günstig über das Internet oder in *Spy-Shops* (Spionage-Läden) zu beziehen. Selbst Spielzeug- und Elektronikläden führen inzwischen Technik im leicht versteckbaren Miniaturformat. Neben solchen Spezialgeräten verfügen schließlich alle aktuellen Handys über Funktionen für Ton-, Foto- oder Videoaufnahmen. Die allgemeine Verfügbarkeit und sinkende Anschaffungskosten haben dazu beigetragen, dass viele Institutionen, aber auch Privatpersonen inzwischen Videoüberwachungsanlagen und *Webcams* in Außenanlagen oder an anderen öffentlich zugänglichen Orten betreiben.

4 Datenauswertung mittels biometrischer Verfahren

Die Analyse von Bild- oder Tonaufnahmen kann mit Hilfe biometrischer Verfahren geschehen, die das Gesichtsbild, das Bild der Iris, Bilder von Finger- oder Handabdrücken, den Gang oder die Stimme abgleichen: Bei diesen Verfahren werden Referenzdaten (Muster) von einzelnen Personen gespeichert, gegen die später aktuelle Aufzeichnungen abgeglichen werden. Solche Verfahren der biometrischen Wiedererkennung werden beispielsweise für Zugangskontrollen eingesetzt, um nur berechtigte Personen passieren zu lassen. Eine biometrische Überwachung kann aber auch großflächig – beispielsweise in Bahnhöfen, Flughäfen oder Stadien – eingesetzt werden, um einzelne Personen aus einer unüberschaubaren Menge herauszusuchen und zu beobachten.

Daneben gibt es Verfahren der biometrischen Mustererkennung, die verdächtiges oder unnormales Verhalten melden sollen: Beispielsweise werten entsprechende Programme Aufzeichnungen von Videokameras aus und erkennen automatisch, welche der Bewegungen Menschen zuzurechnen sind und ob sich diese innerhalb der »normalen« Bewegungsmuster verhal-

ten. Geht beispielsweise eine Person auf einem Parkplatz nicht zielstrebig zu einem Auto, sondern in die Nähe verschiedener Fahrzeuge, könnte es sich um einen Autodieb oder um eine hilfsbedürftige Person handeln, die sich nicht mehr orientieren kann.

Zu den biometrischen Verfahren gehört auch die Genanalyse, bei der die →DNA eines Menschen auf der Basis von Speichel-, Blut- oder Haarproben untersucht wird. Dies kann mit Tatortspuren geschehen, die mit Spuren von anderen Tatorten, mit Datenbankeinträgen bereits bekannter Täter oder mit Erkenntnissen aus DNA-Reihenuntersuchungen (freiwillig oder auf Basis einer richterlichen Anordnung) verglichen werden. Daneben werden DNA-Analysen eingesetzt, um mögliche erbliche Vorbelastungen zu ermitteln, die zu schweren Krankheiten führen können. Viele Labors bieten DNA-Tests auch für Privatpersonen an, um etwa Verwandtschaftsfragen zu klären (siehe auch den Beitrag von Bartmann in diesem Band, S. 178 ff.).

5 Überwachung von Kommunikationsinhalten und Kommunikationsverhalten

Obwohl die Menschen an vielen Stellen Spuren wie Fingerabdrücke oder Haare hinterlassen, wäre heutzutage ein massenhaftes Auswerten dieser biometrischen Spuren sehr aufwändig und in der Regel nur zeitverzögert möglich. Anders sieht es bei der elektronischen Kommunikation aus: Bei jedem Telefonat, jeder Internetnutzung oder anderen Form der elektronischen Kommunikation hinterlässt man Spuren über die jeweilige Verbindung, zumindest beim Anbieter des Dienstes. Eigentlich wären diese Daten nach Abschluss der Verbindung nicht mehr erforderlich (außer gegebenenfalls zu Abrechnungszwecken) und damit schnellstmöglich zu löschen. Allerdings verpflichtete eine gesetzliche Regelung – entstanden durch Vorgaben auf europäischer Ebene – deutsche Telekommunikationsanbieter ab dem Jahr 2008 dazu, bestimmte Daten über die Verbindungen für sechs Monate auf Vorrat zu speichern (siehe auch die Beiträge von Papier, S. 67 ff., Sokol, S. 137 ff. und Ziercke, S. 129 ff. in diesem Band). Zwar betrifft diese Vorratsdatenspeicherung keine Kommunikationsinhalte, jedoch geben die gespeicherten Daten Auskunft über das Kommunikationsverhalten und die sozialen Kontakte der Bevölkerung: Mit wem, wann und wie wir kommunizieren, verrät viel über unser Leben. Das Bundesverfassungsgericht erklärte die deutsche Regelung zur anlasslosen Speicherung der Kommunikationsdaten im März 2010 für verfassungswidrig, da das Gesetz keine konkreten Maßnahmen zur Datensicherheit

vorsehe und die Hürden für den Abruf dieser Daten nicht hoch genug seien (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.). Eine Neufassung der Regelung zur Vorratsdatenspeicherung ist in Vorbereitung (Stand: Mitte 2012).

Zusätzlich müssen die Telekommunikationsanbieter auf richterliche Anordnung das Mithören oder Mitlesen von Kommunikationsinhalten ermöglichen. Gegen eine solche Überwachung könnten sich die Kommunikationsteilnehmer durch den Einsatz von Verschlüsselungsverfahren schützen, weil dann nicht mehr auf die Inhalte ihres Austauschs zugegriffen werden kann. Während Verschlüsselungsverfahren für die computergestützte Kommunikation verfügbar sind (siehe unten sowie den Beitrag von Thomsen in diesem Band, S. 381 ff.), sind solche Maßnahmen in der herkömmlichen Telefonie nicht gängig.

6 Ortungstechniken

Der mobile Einsatz von Telekommunikationsgeräten wie Handys, → *Smartphones* oder *Notebooks* hat in der Vergangenheit stark zugenommen. Schon aus technischen Gründen lässt sich für den Telekommunikationsanbieter in der Regel die ungefähre Position des mobilen Geräts bestimmen. Bei einer Nutzung von ortsbezogenen Diensten (→ *Location-Based Services*) – beispielsweise um sich die Position von nahegelegenen Apotheken oder Tankstellen darstellen zu lassen oder bei der Verwendung eines Navigationssystems – bestimmt das Gerät seine Position selbst. Die Ortsbestimmung geschieht mit Hilfe des → GPS-Signals von Satelliten, über die Mobilfunknetzzellen und den Abstand zu verschiedenen Basisstationen oder anhand der → WLAN-*Access-Points (→ Router)*, die sich in der Nähe befinden und deren Position in anbieterseitigen Datenbanken gespeichert sind. Nur bei einer Positionsbestimmung ausschließlich per GPS-Empfänger lässt sich der Aufenthaltsort der Nutzenden für die Anbieter nicht verfolgen, da diese Geräte passiv arbeiten; bei den anderen Methoden – auch bei einer Kombination von passivem GPS-Empfänger mit einem aktiven Sender, der die Daten überträgt – kann der Betreiber der technischen Infrastruktur auf die Ortsdaten zugreifen.

Ermittlungsbehörden verwenden sogenannte »stille SMS«, um eine Ortung von eingeschalteten Handys zu erreichen: Dabei schicken sie SMS-Nachrichten an das zu ortende Handy, die dort weder auf dem Display noch als akustisches Signal dargestellt werden – der Besitzer des Handys weiß also nicht, dass er geortet wird. Dadurch fallen beim Mobilfunkanbieter Positionsdaten an, auf die die Behörden zugreifen.

Auch Unternehmen interessieren sich für solche Daten: Im Juni 2010 ergänzte der Telefonhersteller *Apple* in seiner Datenschutzerklärung, dass automatisch die Standortdaten seiner → *Smartphones* in die Unternehmensdatenbanken übertragen werden. Mit diesen Informationen wäre *Apple* ebenso wie den Mobilfunkanbietern ein → *Tracking* der Nutzenden möglich, solange diese ihre Handys nicht ausschalten. Dass Anbieter von ortsbasierten Diensten oft ebenfalls Informationen über die Nutzenden und ihre Standorte erhalten, soll nicht unerwähnt bleiben.

Daneben können *Tracking*-Dienste für Arbeitgeber interessant sein, um die Bewegungen ihrer Fahrzeuge und Mitarbeiter zu überwachen. Außerdem melden einige Navigationssysteme, die zusätzlich zu GPS über eine Mobilfunkanbindung verfügen, ihre Position an den Anbieter weiter, zum Beispiel um Hinweise auf Staus zu geben oder dynamisch aktuelle Verkehrsmeldungen zur Situation in der Umgebung abzurufen und bei der Routenplanung umzusetzen.

7 Überwachung im Internet

Zusätzlich zu den dargestellten Informationen auf der Ebene der Telekommunikation fallen bei der Internetnutzung weitere Daten an, die Grundlage einer Überwachung sein können. Dazu gehören die Inhaltsdaten jeder Nachricht im Internet, unabhängig davon, ob es sich um eine E-Mail, das Surfen im Web oder die Nutzung eines anderen Dienstes handelt. Zwar ist es möglich, die Inhaltsdaten auf der Übertragung zwischen den Endpunkten der Verbindung (also zum Beispiel Sender und Empfänger einer E-Mail) zu verschlüsseln (sogenannte Ende-zu-Ende-Verschlüsselung). Jedoch ist nur ein geringer Anteil heutiger E-Mail-Kommunikation verschlüsselt, und nicht alle Webserver unterstützen die mögliche Verschlüsselungstechnik →SSL für den Seitenabruf. Dies bedeutet, dass außer dem eigenen Internetanbieter auch alle Betreiber von Zwischenstationen auf der Strecke die übertragenen Daten mitlesen könnten – und das können leicht zwanzig Stationen im In- und Ausland sein. Ein derartiges Mitschneiden (*Sniffen*) des durchgeleiteten Datenverkehrs wäre nach deutschem Recht zwar rechtswidrig, jedoch genauso wenig nachweisbar wie das Mitlesen einer offen verschickten Postkarte. Dass es sich dabei nicht nur um eine theoretische Gefahr handelt, verdeutlicht eine Meldung aus dem Jahr 2008: Damals sorgten sich US-amerikanische Militärs darum, dass weniger Internetkommunikation über die USA geleitet würde (immer noch circa 25 Prozent des gesamten europäischen Datenverkehrs), was deren Überwachung erschweren würde.[7]

Neben den Inhaltsdaten bieten auch die Verbindungsdaten der Internetkommunikation ein großes Überwachungspotenzial. Sie verraten, wer sich wofür interessiert und mit wem kommuniziert. Besonders viele Auswertungsmöglichkeiten bieten sich denjenigen Anbietern, die häufig in die Kommunikation einbezogen sind: Betreiber von großen Suchmaschinen, von E-Mail-Diensten, von →sozialen Netzwerken, von Kartendiensten oder auch von verbreiteten Werbe-, Analyse- und *Tracking-Tools*, die – oft unbemerkt von den Nutzenden – mittlerweile in vielen Webseiten eingebaut sind und bei jedem Seitenaufruf Daten sammeln. Die größten Datenverarbeiter in dieser Hinsicht sind die Firmen *Google Incorporated (Inc.)* mit einer Vielzahl von Diensten einschließlich der Suchmaschine, die Einstiegsseite für viele Nutzerinnen und Nutzer ist, sowie *Facebook Inc.* mit dem größten sozialen Netzwerk, das immer mehr mit anderen Diensten wie *Online*-Spielen oder E-Shopping zusammenwächst. Sowohl *Google* als auch *Facebook* finanzieren sich durch Werbung und analysieren daher die Interessen und das Verhalten der Nutzenden so weit wie möglich (siehe auch den Beitrag von Reppesgaard in diesem Band, S. 412 ff.).

Die Datenbanken der Internetgiganten spielen eine große Rolle bei der Überwachung – in ihnen werden nicht nur die gesammelten Daten gespeichert, sondern sie ermöglichen auch eine Verkettung mit anderen Daten und weitergehende Auswertung der Informationen (in Abbildung 1: Phasen 2 bis 4). Der Umfang der Daten und die Möglichkeiten ihrer Auswertung sind wesentlich für die Abschätzung des Missbrauchspotenzials, das durch den Betreiber oder – unter Ausnutzung von Sicherheitslücken – durch Dritte besteht.

Dies gilt auch für staatliche Datenbanken: Dazu gehören in Deutschland neben polizeilichen Datenbanken beispielsweise staatliche Melderegister (zurzeit pro Bundesland in eigenen Datenbanken) sowie papierne oder elektronische Grundbücher. Für all diese Datensammlungen gibt es rechtliche Grundlagen, in denen der jeweilige Umfang der Daten und der Zweck ihrer Verarbeitung beschrieben werden.

8 Neuere Überwachungstechnologien

Zu den neueren Überwachungsinstrumenten gehören Drohnen, das heißt ohne Besatzung fliegende ferngesteuerte Fluggeräte, die zusammen mit Satelliten und Flugzeugen dem Gebiet der Fernüberwachung per Sicht zuzurechnen sind. Die kleinsten Drohnen sind wenige Millimeter groß; die großen Drohnen können 40 Meter Spannweite haben. Schon per Satellit kann eine

Auflösung unter einem Meter erzielt werden. Drohnen haben sogar die Möglichkeit, in Gebäuden Aufnahmen zu machen. In einigen Bundesländern werden Drohnen im Rahmen der polizeilichen Aufklärung zunächst experimentell eingesetzt. (siehe auch den Beitrag von Petri in diesem Band, S. 115 ff.).

Eine weitere Überwachungsmethode wird sich vermutlich durch den vermehrten Einsatz von →RFID-*Tags* etablieren, die Teil des →*Ubiquitous Computing* sind: das kontaktlose Auslesen von Daten per Lesegerät. Mittlerweile enthalten nicht nur Personalausweise und Reisepässe einen RFID-Chip, sondern auch einige Zugangssysteme für den öffentlichen Nahverkehr, für Discos, Fitness-Studios, Skigebiete, Casinos, Bibliotheken usw. Die wenigsten dieser RFID-Chips sind verschlüsselt, so dass sie sich als Identifikatoren zum →*Tracking* verwenden ließen, sofern an allen interessanten Stellen Auslesemöglichkeiten geschaffen würden. Für Ausweise bietet sich als Schutz ein Abschirmen der RFID-Chips per Alufolie an, jedoch funktioniert dies nicht besonders gut bei RFID-*Tags* in Kleidungsstücken oder Supermarktprodukten.

9 Künftige Herausforderungen

Der technische Fortschritt bringt ständig neue Überwachungsmöglichkeiten hervor. Zudem nehmen die Verarbeitungsgeschwindigkeit und die Miniaturisierung der Technologien zu. Gleichzeitig erhöht sich die Nachfrage, zum Beispiel vonseiten des Militärs, der Geheimdienste, der Strafverfolgung, aber auch von Arbeitgeberseite, Versicherungen oder staatlichen Stellen. Dass es gesellschaftlich gewollte Überwachung gibt, etwa um Straftaten aufzuklären oder bestenfalls zu verhindern, ist unbestritten. Jedoch dürfen die unbeabsichtigten Nebeneffekte nicht überhand nehmen.

Mittlerweile sind die Räume, in denen ein anonymes oder unbeobachtetes Handeln möglich ist, in erheblichem Maße eingeschränkt.[8] Dies kann sich negativ auf die Gesellschaft als Ganzes auswirken, indem die Menschen sich davor scheuen, von der Norm abzuweichen und ihre Rechte wahrzunehmen. Trends wie das →*Cloud Computing* verstärken die Gefahr eines Kontrollverlustes sowohl bei den Betroffenen als auch bei den verantwortlichen Stellen der Datenverarbeitung. Es wird künftig darauf ankommen, diesen Kontrollverlust und die damit verbundenen Eingriffe in die Privatsphäre umzukehren. Beispielsweise sollte Überwachungstechnik so gestaltet werden, dass zwar eine Überwachung von konkreten Einzelfällen möglich ist, jedoch nicht große Mengen unschuldiger Personen mit überwacht werden.

Anmerkungen

1 Für England siehe: David Murakami Wood (Hrsg.), A Report on the Surveillance Society for the Information Commissioner, by the Surveillance Studies Network, UK, September 2006, im Internet unter: http://www.libertysecurity.org/article1194.html.
2 BVerfGE 65, 1; Az. 1 BvR 209, 269, 362, 420, 440, 484/83.
3 Im Volkszählungsurteil (s. Anm. 2) heißt es dazu: »Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. […] Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.«
4 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein/Technische Universität Dresden, Verkettung digitaler Identitäten, Untersuchung für das Bundesministerium für Bildung und Forschung, Kiel 2007, im Internet unter https://www.datenschutzzentrum.de/projekte/verkettung/.
5 Michel Foucault, Überwachen und Strafen – Die Geburt des Gefängnisses, Frankfurt/M. 1977, Abschnitt III.3.
6 George Orwell, Nineteen Eighty-Four, London 1949.
7 Marit Hansen, Spuren im Netz – der Schutz der Privatsphäre, in: Dieter Korczak (Hrsg.), Spurensuche – Kulturwissenschaftliche Interpretationen und gesellschaftliche Rezeption, Kröning 2010, S. 105–128.
8 Christiane Schulzki-Haddouti (Hrsg.), Vom Ende der Anonymität. Die Globalisierung der Überwachung, 2. aktualisierte Aufl., Hannover 2000.

Edgar Wagner

Datenschutz als Bildungsaufgabe

1 Strategien des Datenschutzes

Der Datenschutz war bisher in erster Linie eine Aufgabe von Gesetzgebung und Kontrolle.[1] Bundestag und Landtage haben allgemeine und bereichsspezifische Datenschutzgesetze erlassen und die Datenschutzbeauftragten sollen dafür sorgen, dass diese Gesetze auch eingehalten werden. Das ging lange Zeit gut, auch weil das Bundesverfassungsgericht die Gesetzgeber oft genug auf den Pfad der Tugend, sprich des Datenschutzes zurückführte und die Medien zahllose Datenskandale an das Licht der Öffentlichkeit brachten. Erziehung zum Datenschutz war in diesem Konzept nicht vorgesehen und wurde deshalb auch nicht praktiziert. Wenn Bildung überhaupt eine Rolle spielte, dann ging es um Weiterbildung, allerdings nur um die der Mitarbeiterinnen und Mitarbeiter von datenverarbeitenden Stellen.

Dies war in gewisser Weise nachvollziehbar, denn die Bürgerinnen und Bürger hatten im analogen Zeitalter nur einen passiven Status. Sie waren »Betroffene« von Datenverarbeitungsprozessen, die besondere Rechte erhielten, um ihr informationelles Selbstbestimmungsrecht verteidigen zu können. Mehr war nicht vorgesehen und mehr wurde auch nicht für notwendig gehalten, auch weil die Betroffenen ohnehin von ihren Rechten kaum Gebrauch machten.

Seit dem Beginn des digitalen Zeitalters, also seit dem Ende des vergangenen Jahrhunderts, greift dieses Datenschutzkonzept zu kurz. Die Regelungsmöglichkeiten nationaler Gesetzgeber stoßen im *World Wide Web* an ihre Grenzen, die notwendigen internationalen Abkommen lassen auf sich warten. Datenschützer versuchen heute vergeblich, Regelungen, die für die analoge Datenverarbeitung gedacht waren, auf die digitalen Medien zu übertragen. Und die »Betroffenen« des elektronischen Zeitalters entwickeln sich zu einem guten Teil zu Aktivisten im → Web 2.0: Sie gestalten Inhalte, kommunizieren und vernetzen sich in sozialen Medien und werden damit zu Akteuren, die weit mehr als nur Betroffene nach der bisherigen Lesart sind.

Dieser Rollenwechsel trägt zusammen mit den neuen digitalen Möglichkeiten dazu bei, dass die Bürgerinnen und Bürger innerhalb wie außer-

halb des Netzes immer mehr Datenspuren hinterlassen (siehe auch die Beiträge von Schmidt, S. 215 ff., Wagner/Gebel/Brüggen, S. 226 ff. und Bluhm, S. 237 ff. in diesem Band). Nutzerinnen und Nutzer haben längst den Überblick darüber verloren, wann wer welche Daten zu welchem Zweck speichert, sie gegebenenfalls mit anderen Datensätzen verknüpft oder an Dritte weitergibt. Sie haben in der Regel auch keine Vorstellung davon, dass die Daten, die sie im Internet hinterlassen, dort noch in Jahrzehnten abgerufen werden können. Es fehlt ihnen weitgehend ein Bewusstsein für die Funktionsbedingungen des Internets und die Gefahren und Herausforderungen des digitalen Zeitalters. Mit einem Wort: Die digitale Welt überfordert ihre Bürgerinnen und Bürger.

Die großen Internetdienstleister zeigen sich davon unbeeindruckt. Schlimmer noch: Sie nutzen die digitale Überforderung aus und treiben eine totale Kommerzialisierung der Privatsphäre voran. Frank Schirrmacher, der Herausgeber der Frankfurter Allgemeinen Zeitung (FAZ), spricht sogar von deren Industrialisierung und meint damit den Versuch von *Google*, *Facebook* und Co., die Menschen virtuell abzubilden, einen digitalen Klon herzustellen, um diesen wirtschaftlich auszubeuten. Wer meint, dies sei übertrieben, sollte bedenken, dass die digitale Entwicklung und mit ihr die Speicherung menschlicher Aktivitäten noch lange nicht zu Ende ist: →RFID, intelligente Stromnetze, das →Internet der Dinge sind die nächsten Stufen dieser Entwicklung. Das digitale Ende ist nicht absehbar.

Mag sein, dass eine Gesellschaft, in der alle alles von allen wissen, großzügiger wird und toleranter mit den Mitmenschen umgeht. Vielleicht mutiert die digital vernetzte Gemeinschaft aber auch zu einer Art »sozialem Blockwart«, der eher kontrolliert als toleriert. Wir können weder vorhersagen noch können wir verordnen, in welche Richtung die Gesellschaft sich bewegt. Will man diese Entwicklung aber mitgestalten und beeinflussen, muss man sich kundig machen und ein Bewusstsein dafür entwickeln, dass die digitale Technologie Staat und Gesellschaft auf revolutionäre Weise umgestaltet und die Privatsphäre des Einzelnen infrage stellt. Aus diesem Grund darf der Datenschutz nicht mehr nur den Gesetzgebern und Datenschutzbeauftragten überlassen werden. Datenschutz ist auch als Bildungsaufgabe zu begreifen, er gehört in die Schulen, Hochschulen und Volkshochschulen sowie in die betriebliche Ausbildung.

Die Datenschutzbeauftragten des Bundes und der Länder haben dies mittlerweile erkannt. In ihrer Entschließung vom Oktober 2009 werden »Staat, Wirtschaft und Gesellschaft aufgefordert, ihre entsprechenden Bildungsanstrengungen zu verstärken«. Ziel müsse es sein, »die Fähigkeit und

Bereitschaft der Bürgerinnen und Bürger, insbesondere von Kindern und Jugendlichen, zu fördern, verantwortungsvoll mit ihren eigenen Daten und respektvoll mit den Daten anderer Menschen umzugehen«.[2]

Ihre Forderung ist mittlerweile bei den politisch Verantwortlichen angekommen. In Rheinland-Pfalz etwa verabschiedete das Landesparlament im März 2011 einstimmig eine Erklärung, die den Datenschutz ausdrücklich als Bildungsaufgabe bezeichnet.[3]

2 Gegenstand, Zielgruppen und Akteure der Datenschutzbildung

Welche inhaltlichen Konsequenzen folgen aus dieser Einsicht?

Bewusstsein für digitale Zusammenhänge entwickeln

Es geht sicherlich nicht darum, spezielle Kenntnisse vom Inhalt der allgemeinen und bereichsspezifischen Datenschutzregelungen zu vermitteln und jeden zu einem Datenschutzbeauftragten zu erziehen. Notwendig ist vielmehr, ein Bewusstsein für die digitalen Zusammenhänge zu entwickeln. Die Menschen müssen lernen, dass sie für ihre Kontakte in *Facebook*, die Aufmerksamkeit in SchülerVZ, die Nutzung der *Google*-Suchmaschine oder etwa die Rabatte auf Kundenkarten bezahlen müssen – nicht mit Geld, aber mit ihren Daten und mit ihrer Privatsphäre. Sie ist die Leitwährung im digitalen Zeitalter. Die Menschen müssen außerdem lernen, dass ihre digital gespeicherten Daten weder im Netz noch außerhalb sicher vor unbefugten Zugriffen sind. Die Enthüllungen von → *Wikileaks* haben dies in jüngster Zeit noch einmal deutlich gemacht.[4] Die Menschen müssen deshalb auch eine Vorstellung davon bekommen, dass sie im digitalen Zeitalter nicht erst dann gläsern werden, wenn sie durch einen Nacktscanner laufen. Das leisten *Google*, *Facebook* und Co. bereits mit Hilfe ihrer geheimen Algorithmen und den Milliarden von Daten, die sie von ihren Mitgliedern sowie Nutzerinnen und Nutzern erhalten.

Nur wenn die Menschen um jene Risiken wissen, die mit der Nutzung des Internets einhergehen, können sie auch selbstverantwortlich entscheiden, in welchem Umfang sie am digitalen Leben teilnehmen oder sich zurückhalten wollen. Damit wird kein digitaler Autismus gepredigt, sondern auf die Beachtung des Grundsatzes der Datenvermeidung und der Datensparsamkeit gepocht, der nicht nur für den Staat und die Wirtschaft gilt, sondern auch den Bürgerinnen und Bürgern gut tut.

Die Sensibilisierung für die Risiken im Netz muss einhergehen mit einer Aufklärung über die Werte und Prinzipien, die durch eine übermäßige Preisgabe privater Angelegenheiten gefährdet werden. Es muss den Menschen bewusst gemacht werden, dass es dabei um ihre Persönlichkeitsrechte und ihre Privatsphäre geht, und sie müssen wissen, warum diese schutzbedürftig sind. Insoweit geht es bei der Bildung zum Datenschutz auch um die Vermittlung von tradierten Werten, die schwer errungen wurden und deshalb nicht leichtfertig aufs Spiel gesetzt werden dürfen, zumal informationelle Selbstbestimmung nach der Rechtsprechung des Bundesverfassungsgerichts wesentlicher Bestandteil einer freiheitlichen Demokratie ist.[5] Erziehung zum Datenschutz läuft deshalb letztlich auf die Mobilisierung der freiheitssichernden Kraft des Datenschutzes hinaus.

Wissensvermittlung über Rechte und Selbstdatenschutz

Selbstverständlich muss ein Bildungskonzept zum Datenschutz auch die Rechte thematisieren, die den Bürgerinnen und Bürgern zur Wahrung ihres informationellen Selbstbestimmungsrechts zustehen. Diese Rechte (siehe hierzu auch den Beitrag von Dix in diesem Band, S. 290 ff.) reichen von Auskunfts- bis zu Löschungsansprüchen und schließen auch Widerspruchsrechte ein. Wie wichtig solche Rechte sind, wurde zuletzt bei → *Google Street View* deutlich, gegen das binnen weniger Wochen hunderttausende von Widersprüchen eingelegt wurden.

Hinzu kommen die Möglichkeiten des Selbstdatenschutzes, die im Mittelpunkt eines Bildungskonzepts zum Datenschutz stehen müssen. Der »digitale Bürger« ist ein »gläserner Bürger«, wenn er nicht selbst für ausreichenden Sichtschutz sorgt und sich vor neugierigen Blicken selbst schützt. Selbstdatenschutz reicht vom richtigen Verhalten in →sozialen Netzwerken bis zur sicheren Passwortgestaltung, dem passenden Identitätsmanagement oder der effektiven Verschlüsselung von E-Mails (siehe auch die Beiträge von Schallbruch, S. 372 ff. und Thomsen, S. 381 ff. in diesem Band).

Bildungskonzepte müssen flexibel sein

Die Beispiele zeigen, dass ein Bildungskonzept zum Datenschutz flexibel sein muss. Es hat sich am jeweiligen Stand der digitalen Entwicklung und an den aktuellen Datenschutzfragen zu orientieren. Es muss also ständig fortgeschrieben und angepasst werden, um selbst aktuell zu bleiben. Das unterscheidet die Erziehung zum Datenschutz beispielsweise von der Gesundheits- und der Verkehrserziehung, die ja ebenfalls in den Schu-

len stattfinden. Gesundheits- und Verkehrserziehung reagieren mehr oder weniger immer auf dieselben Risiken mit denselben Gegenstrategien. Beim Datenschutz ist dies anders. Das Internet bringt regelmäßig neue Angebote hervor und verändert sich ständig. Deshalb sind auch für die sich ändernden Risiken und Herausforderungen immer neue Strategien zu entwickeln und den Betroffenen zu vermitteln.

Generationsübergreifende Angebote

Es macht die Sache nicht einfacher, dass die permanente Notwendigkeit zur Aktualisierung des Bildungskonzeptes für alle Altersgruppen geleistet werden muss. Die Fähigkeit zu selbstverantwortlichem Verhalten muss bei allen Altersgruppen vorhanden sein. Eine generationen- und schichtenübergreifende Bildungs- und Erziehungsarbeit ist auch deshalb notwendig, weil das Datenschutzbewusstsein in allen Altersgruppen und unabhängig vom jeweiligen Bildungshintergrund zu wünschen übrig lässt (übrigens auch bei der jungen »Generation *Google*«).

Gesamtgesellschaftliche Aufgabe

Bildung zum Datenschutz kann deshalb nicht nur eine Aufgabe der Schulen sein. Diese tragen die Hauptverantwortung, auch deshalb, weil sie nach den Schulgesetzen zu Selbstbestimmung und eigenverantwortlichem Handeln zu erziehen haben. Dazu gehören eben auch die informationelle Selbstbestimmung und die informationelle Selbstverantwortung. Aber letztlich ist diese Aufgabe – wie die Vermittlung von Medienbildung überhaupt – eine gesamtgesellschaftliche Aufgabe, an der die Erziehungsberechtigten, die Träger der Jugendarbeit und der Erwachsenenbildung, die Hochschulen und Volkshochschulen sowie die Zentralen für politische Bildung zu beteiligen sind. Das gilt auch für die Wirtschaft, die Kammern und die Verbände. Junge Arbeitnehmerinnen und Arbeitnehmer lassen ihre oft laxe Haltung in Datenschutzfragen nicht am Werkstor zurück. Es liegt deshalb im eigenen Interesse der Wirtschaft, mit dazu beizutragen, dass ihre Mitarbeiterinnen und Mitarbeiter verantwortlich mit persönlichen, aber auch mit betrieblichen Geheimnissen umgehen. Es liegt auf der Hand, dass die entsprechenden Bildungsanstrengungen miteinander koordiniert werden müssen. Dies schließt die Zusammenarbeit der Schulen mit den Erziehungsberechtigten und den außerschulischen Einrichtungen mit ein, was wiederum die Bildung entsprechender Netzwerke unter Einbeziehung der Datenschutzbeauftragten notwendig macht.

3 Praxis der Datenschutzbildung

Soweit die Theorie. Aber wie sieht die Praxis aus? Welche Rolle spielt der Datenschutz als Bildungsaufgabe in der Realität, welchen Stellenwert hat er insbesondere im schulischen Unterricht?

Herausforderung für die Schulen

Die Schulen werden durch die digitale Entwicklung vor große Herausforderungen gestellt. Neue Unterrichtsinhalte können – schon aus zeitlichen Gründen – in der Regel nur auf Kosten anderer Inhalte behandelt werden, was zu schwierigen Prioritätsverschiebungen zwingt. Neue Unterrichtsinhalte setzen außerdem entsprechend qualifiziertes Lehrpersonal und hinreichend präzise Lehrpläne voraus. An all dem fehlt es aber, jedenfalls im notwendigen Umfang.

Es ist bezeichnend, dass die Kultusministerkonferenz das Thema Datenschutz im digitalen Zeitalter bisher noch nicht aufgegriffen und auch Fragen der Medienkompetenz in den letzten 15 Jahren nicht mehr behandelt hat. Ihre letzte Stellungnahme zu diesem Themenkreis stammt noch aus der Vor-Internetzeit. Dementsprechend fühlen sich offenbar nur wenige Lehrerinnen und Lehrer für den Datenschutz im schulischen Unterricht zuständig. Wenn es um das Internet geht, leben Lehrende und Lernende offenbar in verschiedenen Welten. Dies ist jedenfalls das Ergebnis einer Studie über »Medienkompetenz in der Schule«, die kürzlich von der nordrhein-westfälischen Landesanstalt für Medien vorgestellt wurde.[6] Auch dies muss nicht verwundern. In den Ausbildungsordnungen für Lehrerinnen und Lehrer spielt der Datenschutz nur eine nachgeordnete Rolle, das gilt selbst für das Fach Informatik. Nicht besser sieht es in den Lehrplänen aus, in denen – wenn überhaupt – nur für bestimmte Schulen und einzelne Fächer die Behandlung des Datenschutzes vorgeschrieben wird. Dabei bleibt meist offen, welche Aspekte des Datenschutzes eigentlich behandelt werden sollen.

Maßnahmen zur Förderung der Datenschutzkompetenz – Ist- und Sollanalyse

Man muss allerdings anerkennen, dass es mittlerweile ernsthafte Bemühungen gibt, diese Situation zu verbessern. Auf Anregung der Datenschutzbeauftragten des Bundes und der Länder hat die Kultusministerkonferenz im März 2012 eine Erklärung zur »Medienbildung in Schulen«

verabschiedet, die Lehrkräften Anregungen für die Behandlung des Datenschutzes im schulischen Unterricht geben will. Hier und dort gibt es auch schon einschlägige Positionspapiere und sogar »Richtlinien zur Verbraucherbildung an allgemeinbildenden Schulen«, in denen der Datenschutz als Kernkompetenz der Verbraucher hervorgehoben und deshalb auch im Unterricht vermittelt werden soll.[7] Daneben existieren Pilotprojekte, Modellversuche und Regierungsprogramme, in denen bestimmte Schulen in den Genuss besonderer Fördermaßnahmen zur Medienkompetenz kommen. Das schließt die Ausstattung mit spezieller Hard- und Software, die Ausbildung von sogenannten Medienscouts und die Fortbildung von Lehrkräften ein.

Ein Beispiel dafür ist das rheinland-pfälzische Regierungsprogramm »Medienkompetenz macht Schule« (*www.medienkompetenz.rlp.de*). Mit diesem 2007 gestarteten Programm soll die Medienkompetenz von Schülerinnen und Schülern, Lehrkräften und Eltern auch in Datenschutzfragen vorangebracht werden. Seit Beginn des Programms wurden mehr als 20 000 Lehrkräfte fortgebildet und rund 1 300 Lehrkräfte zu Jugendmedienschutzberatern ausgebildet. In mehr als 300 Elternabenden wurden rund 13 000 Teilnehmende von fachkundigen Referentinnen und Referenten über verschiedene Jugendmedienschutzthemen informiert. Einen *Peer-to-Peer*-Ansatz verfolgt das Programm mit der Ausbildung von Medienscouts. Diese durchlaufen eine anderthalbtägige Ausbildung und stehen dann ihren Mitschülerinnen und Mitschülern als Ansprechpersonen in Fragen der Mediennutzung zur Seite. Mittlerweile sind rund 900 Schülerinnen und Schüler an über 50 Schulen als Medienscouts tätig.

Es fällt allerdings auf, dass Medienkompetenz in diesen und ähnlichen Programmen oft auf Fragen des Jugendmedienschutzes reduziert wird. Datenschutzfragen bleiben dabei auf der Strecke. Das kommt auch in Stellungnahmen von politisch Verantwortlichen zum Ausdruck, etwa in der 19-seitigen Antwort der Bundesregierung auf die Kleine Anfrage von Abgeordneten der SPD-Bundestagsfraktion zur »Verbesserung von Medienkompetenz und Medienbildung im *Online*-Bereich«[8], in der immer wieder von Jugendmedienschutz, aber nur beiläufig von Datenschutz die Rede ist.

Damit ist einer der wesentlichen Mängel der gegenwärtigen Fachdiskussion über Medienbildung und Medienkompetenz angesprochen. Obwohl wir in einer Informationsgesellschaft leben, in der so viele persönliche Daten erhoben, gespeichert und verarbeitet werden wie nie zuvor, wird dem Datenschutz im theoretischen Konzept von Medienbildung und Medienkompetenz und erst recht in dessen praktischer Umsetzung nur eine nachgeordnete Rolle eingeräumt.

Es genügt nicht, in den einschlägigen amtlichen Bekanntmachungen für die Schulen darauf hinzuweisen, dass Jugendliche lernen müssen, verantwortlich mit ihren persönlichen Daten umzugehen. Und es reicht auch nicht aus, im Unterricht auf das Problem von Kostenfallen oder von *Cyber-Mobbing* einzugehen. Digitale Aufklärung muss weit darüber hinausgehen, auf die Fähigkeit zur Datenvermeidung und zum Selbstdatenschutz abzielen und – wie gesagt – die freiheitssichernde Kraft des Datenschutzes thematisieren. Davon ist man aber in der Medienbildung und bei der Förderung der Medienkompetenz – trotz vieler guter Ansätze – noch ein ganzes Stück entfernt, sowohl im schulischen wie im außerschulischen Bereich.

Bildungspolitische Forderungen

Aus diesem Befund leiten sich einige grundsätzliche bildungspolitische Forderungen ab:

- Dem Datenschutz muss vor allem im schulischen Unterricht ein größeres Gewicht beigemessen werden. Dies muss in einer schulpolitischen Grundsatzentscheidung des zuständigen Ministeriums zum Ausdruck gebracht werden.
- Die vorhandenen Erfahrungen und Konzepte für eine unterrichtliche Vermittlung des Datenschutzes müssen von Fachleuten überprüft, ergänzt und zu einem geschlossenen Unterrichtskonzept zusammengefasst werden. Die Grundzüge eines solchen Konzeptes sollten in einer ministeriellen Richtlinie oder in einer vergleichbaren Regelung festgelegt werden.
- Die Fort- und Weiterbildung von Lehrerinnen und Lehrern muss sich stärker als bisher auch auf den Datenschutz erstrecken. Vor allem aber ist die entsprechende Ausbildung der Lehrkräfte zu forcieren. Deshalb sollte der Datenschutz auch in den Bildungskanon der Hochschulen aufgenommen werden.
- Den Eltern sind wirkungsvolle Hilfestellungen in den ihre Kinder betreffenden Datenschutzfragen zu geben.
- Dem Vorschlag der Europäischen Kommission[9] entsprechend sollte die digitale Aufklärung im Allgemeinen und in den Schulen im Besonderen normativ verankert werden.

4 Beitrag der Datenschutzbeauftragten

Die Datenschutzbeauftragten des Bundes und der Länder sehen es als ihre Aufgabe an, dazu beizutragen, die Defizite bei der Vermittlung von Datenschutzkompetenzen abzubauen. Das beginnt bei der Erstellung von Unterrichtsmaterialien, schließt die Fortbildung von Lehrkräften ein und endet bei der Durchführung von Unterrichtseinheiten zum Datenschutz.

An guten Unterrichtsmaterialien besteht mittlerweile kaum noch ein Mangel. Einen guten Überblick bietet die Homepage des rheinland-pfälzischen Datenschutzbeauftragten.[10] Ein großer Teil der dort angebotenen Unterrichtsmaterialien ist mit Hilfe der Datenschutzbeauftragten von Bund und Ländern entstanden. Hinzu kommen in vielen Bundesländern spezielle Angebote zur Lehrerfortbildung, die auch die Fortbildung schulischer Datenschutzbeauftragter und der Schulleitung mit einschließt.

Mittlerweile gibt es auch kostenlose Workshops, die von einzelnen Datenschutzbeauftragten den Schulen zu aktuellen Datenschutzfragen angeboten werden. In Rheinland-Pfalz ist die Nachfrage hierzu groß. Seit September 2010 gingen beim dortigen Datenschutzbeauftragten von über 130 Schulen Anfragen für entsprechende – in der Regel vier Schulstunden umfassende – Unterrichtseinheiten ein, die von besonders ausgebildeten Mitarbeitern auf der Grundlage eines speziellen pädagogischen Konzeptes und mit Hilfe ausgewählter Unterrichtsmaterialien organisiert und durchgeführt werden. Aktuell sind bereits über 230 Workshops mit mehr als 6 000 Schülerinnen und Schülern durchgeführt worden.

Ein ähnliches Projekt wird übrigens auch vom Berufsverband der Datenschutzbeauftragten Deutschlands durchgeführt, der seit 2010 mit ehrenamtlich tätigen Mitgliedern unterwegs ist, um Schülerinnen und Schülern ab der sechsten Klasse klare und einfache Verhaltensregeln für einen sensiblen Umgang mit ihren persönlichen Daten im Netz näher zu bringen (siehe auch den Beitrag von Spaeing/Spaeing in diesem Band, S. 249 ff.).

Die große Nachfrage offenbart die Defizite, die in den Schulen bestehen, und der Ablauf der Workshops die Defizite, die bei den Schülerinnen und Schülern festzustellen sind. Auf Dauer werden diese Defizite nur dann nachhaltig zu beseitigen sein, wenn die Schulen die entsprechende Aufklärung nach Maßgabe konkreter Lehrpläne und mit datenschutzrechtlich vorgebildeten Lehrkräften selbst übernehmen. Die Unterstützung der Datenschutzbeauftragten bleibt ihnen gewiss.

Das gilt in gleicher Weise für eine Reihe weiterer Einrichtungen, die in diesem Kontext mit hoher Kompetenz Hilfestellung leisten. Erwähnt sei vor allem die Initiative »Klicksafe« (*www.klicksafe.de*). Klicksafe setzt seit 2004 in

Deutschland den Auftrag der Europäischen Kommission um, Internetnutzern die kompetente und kritische Nutzung von Internet und neuen Medien zu vermitteln. Dies geschieht durch Schulungen, Bereitstellung von Informations- und Unterrichtsmaterial und durch breit angelegte öffentliche Kampagnen, wie die Beteiligung am *Safer Internet Day*, einem europaweiten Aktionstag zum sicheren Umgang mit dem Internet.

5 Datenschutzbildung als Daueraufgabe

Die Probleme sind erkannt und werden auch bereits angegangen, zögerlich zwar und eher punktuell. Aber die Erfahrungen, die auf diese Weise gesammelt werden, sind notwendig für die entsprechende Ausbildung der Lehrerinnen und Lehrer, die Überarbeitung der Lehrpläne, die Gestaltung des Unterrichts und die Einbindung der Eltern. Im Übrigen können die bisherigen Anstrengungen – in den Schulen und im außerschulischen Umfeld – offenbar erste Erfolge vorweisen: Nach der JIM (Jugend, Information und Multimedia)-Studie 2010 hat die Zahl jener Jugendlichen zugenommen, die in sozialen Netzwerken besser auf ihre Privatsphäre achten.[11] Diese und andere Studien zeigen aber auch, dass noch sehr viel zu tun ist. Daran wird sich angesichts der rasanten digitalen Entwicklung auf absehbare Zeit nichts ändern. Datenschutz als Bildungsaufgabe bleibt eine Daueraufgabe.

Anmerkungen

1 Zum Datenschutz durch Technik siehe auch den Beitrag von Schaar in diesem Band, S. 363 ff. sowie die Orientierungshilfen der Datenschutzbeauftragten des Bundes und der Länder »Datenschutzfreundliche Technologien« und »Datenschutzfreundliche Technologien in der Telekommunikation« – im Internet unter http://www.datenschutz.rlp.de, Rubrik »Service – Materialien«. Zum Datenschutz durch Recht siehe auch die Beiträge von Papier, S. 67 ff. und Roßnagel, S. 331 ff. in diesem Band.

2 Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8.10.2009 mit dem Titel »Aktueller Handlungsbedarf beim Datenschutz – Förderung der Datenschutzkultur«.

3 Fraktionen der SPD, CDU und FDP im Landtag Rheinland-Pfalz, Datenschutz ist auch eine Erziehungs- und Bildungsaufgabe. Entschließungsantrag vom 17.2.2011 (LT-Drs. 15/5417; Beschlussfassung vom 23.2.2011 – s. Plenar-Protokoll 15/109).

4 Heinrich Geiselberger (Hrsg.), WikiLeaks und die Folgen, Berlin 2011.

5 So bereits das Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983 (BVerfGE 65, 1 ff.); siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.

6 Andreas Breiter/Stefan Welling/Björn Eric Stolpmann, Medienkompetenz in der Schule. Integration von Medien in den weiterführenden Schulen in Nordrhein-Westfalen (Schriftenreihe Medienforschung der Landesanstalt für Medien NRW Bd. 64), Berlin 2010, im Internet unter http://www.lfm-nrw.de/de/forschung/abgeschlossene-projekte.html.

7 »Richtlinie Verbraucherbildung an allgemeinbildenden Schulen in Rheinland-Pfalz«, hg. vom Ministerium für Bildung, Wissenschaft, Jugend und Kultur, Mainz 2010, im Internet unter: http://verbraucherbildung.bildung-rp.de/fileadmin/user_upload/verbraucherbildung.bildung-rp.de/Materialien/Richtlinie_VB.pdf.

8 Siehe BT-Drs. 17/4161 vom 10.12.2010.

9 Empfehlung der Europäischen Kommission (2009/625/EG) vom 20.8.2009, im Internet unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:227:0009:0012:DE:PDF.

10 Landesbeauftragter für den Datenschutz und die Informationsfreiheit, RLP, Informationen zum Thema Datenschutz und Schule, im Internet unter http://www.datenschutz.rlp.de/de/jugend.php?submenu=schule.

11 Medienpädagogischer Forschungsverbund Südwest (Hrsg.), Jugend, Information, (Multi-)Media. Basisstudie zum Medienumgang 12- bis 19-Jähriger in Deutschland, Presseerklärung und Studie im Internet unter http://www.mpfs.de.

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.

Marion Albers

Das Präventionsdilemma

Prävention, also das »Zuvor-Kommen«, ist eine Leitidee der modernen Gesellschaft. Sie zielt darauf, absehbaren oder denkbaren Schäden möglichst frühzeitig mit Vorbeugungs- und Vorsorgemaßnahmen zu begegnen. Ein klassisches Feld für präventives Vorgehen, bei dem die Möglichkeit von Schäden ausreicht und das bereits im Vorfeld von Gefahrenschwellen ansetzt, bietet zum Beispiel der Umwelt- und Gesundheitsschutz. Zunehmend präventiven Charakter gewinnt auch das Handeln der Polizei (siehe auch den Beitrag von Petri in diesem Band, S. 115 ff.). So gibt es immer häufiger

- anlass- und verdachtslose Kontrollen,
- flächendeckende Massenüberwachungen,
- langfristige Videoüberwachungen öffentlicher Räume,
- vorsorgliche Sammlungen von Daten.

Ausgreifend verstanden reicht die Kriminalitätsprävention weit in die Gesellschaft hinein und erfasst etwa auch die Erziehung, die Sozialarbeit oder die städtebauliche Vermeidung sozialer Brennpunkte.[1]

Nicht nur staatliche Stellen, sondern auch Private wählen immer ausgefeiltere Präventionsstrategien. Beispiele hierfür sind

- umfangreiche private Videoüberwachungen,
- umfassende Datenbanken professioneller → Auskunfteien,
- Risikobeurteilungen mittels computerunterstützter → *Scoring*-Verfahren.

Wie weit präventive private Videoüberwachungen gehen, verdeutlicht der inzwischen wegen zahlreicher Proteste wieder eingestellte Dienst *Internet Eyes*. Dieser Dienst ermöglichte es den Inhabern eines Geschäfts, das gesamte Geschehen in ihren Läden live im Internet zu zeigen. Beliebige Personen konnten so das Geschehen im Geschäft über das Internet beobachten, dem Geschäftsinhaber vermutete Diebstähle oder Auffälligkeiten per Mausklick anzeigen und gegebenenfalls eine Belohnung erhalten. Für die Kundinnen und Kunden des Geschäfts bedeutete diese Form der Diebstahlsprävention eine vollständige Überwachung ihres Verhaltens im Geschäft durch weltweite Beobachtung.

Präventive Risikobeurteilungen mittels → *Scoring*-Verfahren gibt es unter anderem bei Kreditentscheidungen. Dabei hängt die Kreditwürdigkeit einer

Person von statistisch errechneten gruppenbezogenen Datenprofilen und damit statt von ihrer persönlichen Lage etwa von der Gegend ab, in der sie wohnt (siehe auch den Beitrag von Lüke in diesem Band, S. 154 ff.).

Eine erfolgreiche Prävention hat auf der einen Seite den Vorteil, dass Schäden gar nicht erst entstehen oder sogar überhaupt nicht mehr zu entstehen drohen, so dass man sie weder im Nachhinein beseitigen noch aufwändige Schadensabwehrmaßnahmen treffen muss. Auf der anderen Seite können Präventionsstrategien mit unerwünschten Folgen verbunden sein, vor allem mit Freiheitsverlusten.

Das Präventionsdilemma bezeichnet den politisch und rechtlich zu entscheidenden Konflikt zwischen den Vorteilen und den Nachteilen frühzeitiger, bereits weit im Vorfeld von Gefahrenlagen einsetzender Präventionsmaßnahmen. Datenschutz kann dazu beitragen, die unterschiedlichen Interessen der in einem bestimmten Konfliktfeld beteiligten Personen oder Institutionen auszugleichen.

1 Prävention in der Risiko- und Informationsgesellschaft

Moderne Gesellschaft als Risiko- und Informationsgesellschaft

Dass Prävention zu einer Leitidee der modernen Gesellschaft geworden ist, hat viel mit gesellschaftlichen Veränderungen zu tun. Lange Zeit konnte man die Gesellschaft als bürgerlich-liberale Gesellschaft oder als Industriegesellschaft beschreiben. Heute charakterisiert man sie dagegen als Risikogesellschaft und als Informationsgesellschaft.[2] Das hat mehrere Gründe: Die Beschreibung als »Risikogesellschaft« erklärt sich zunächst mit den umwälzenden Entwicklungen von Wissenschaft und Technik. Diese Entwicklungen haben neue Technologien mit gesteigertem Katastrophenpotenzial hervorgebracht, etwa Kernreaktoren oder Bio- und Gentechnologien. Darüber hinaus hat sich gezeigt, dass mit wachsendem Wissen zugleich das Nichtwissen zunimmt: Einerseits wird in der Gesellschaft immer mehr Wissen erzeugt oder zusammengetragen. Andererseits werden gerade dadurch immer neue Gefahren, Ungewissheiten und nachhaltige Erkenntnislücken deutlich.

Heute ist beispielsweise bekannt, dass Umweltschäden sich nicht unbedingt – wie früher angenommen – über gleichmäßige Kausalverläufe von erkennbaren Ursachen hin zu absehbaren Wirkungen entwickeln. Oft entstehen sie plötzlich über ein nicht vollständig durchschaubares Zusammenwirken zahlreicher Faktoren, so dass sie nur schwer vorherzusehen sind.[3]

Nicht zuletzt ist die Beschreibung Risikogesellschaft eine Konsequenz der Auflösung traditioneller Sozialstrukturen und der Gefährdungen infolge der Säkularisierung, Differenzierung und Pluralisierung der modernen Gesellschaft.[4] Negative Ereignisse und Schäden werden heute kaum noch unabänderlichen Naturgewalten oder dem Schicksal zugeschrieben. Stattdessen werden sie Entscheidungen von Personen oder Institutionen zugerechnet. Beruhen Schäden aber nicht länger auf dem unbeeinflussbaren Schicksal, sondern auf beeinflussbaren Zusammenhängen, werden sie nicht mehr einfach hingenommen. Im Gegenteil wird von den beteiligten Personen oder Institutionen erwartet, dass sie ihre Entscheidungen so gestalten, dass angemessene Vorhersagen und Vorsorgemaßnahmen getroffen und Schäden vermieden werden.[5] Die Risikogesellschaft und die Idee der Prävention hängen entsprechend eng miteinander zusammen.

Ähnlich enge Verbindungen bestehen zur »Informationsgesellschaft«. Dieser Begriff stellt die zentrale Rolle heraus, die Informationen und Wissen infolge des gesellschaftlichen Wandels und vor dem Hintergrund immer leistungsfähigerer Kommunikations- und Datenverarbeitungstechniken zukommt. Computer und Chipkarten, Rechnernetzwerke und Internet führen dazu, dass Daten in wachsendem Umfang erhoben und erzeugt, praktisch unbegrenzt gespeichert, automatisiert verknüpft, vielfältig ausgewertet und immer leichter übermittelt werden können. Auch hier gilt jedoch, dass Wissen keineswegs proportional zu- und Ungewissheit proportional abnimmt. Verbesserte Möglichkeiten der Erhebung, Verknüpfung und Auswertung von Daten erweitern das Präventionswissen und erleichtern Präventionsmaßnahmen. Neues Wissen erzeugt allerdings immer auch neue Ungewissheiten und führt uns die strukturellen Grenzen der Erkenntnismöglichkeiten ebenso vor Augen wie die unausweichliche Selektivität allen Wissens. Die Informationsgesellschaft bietet mehr Wissen als je zuvor. Zugleich zeigt sie neue Risiken und neue Erkenntnislücken auf, die wiederum nach noch mehr Wissen und noch mehr Vorsorge verlangen.

Prävention wird somit in der Risiko- und Informationsgesellschaft in verstärktem Umfang nötig und möglich. Zugleich wird der Wissens- und Präventionsbedarf immer neu angefeuert. Entsprechend können sich auch die Nachteile ausufernder Präventionsstrategien steigern. Prävention wird daher selbst zu einem regulierungsbedürftigen gesellschaftlichen Risiko.[6]

Konzept, Kennzeichen und Folgen der Prävention

Ziel der Prävention ist es, absehbare oder denkbare Schäden und Gefahrenlagen so früh wie möglich bereits an deren Quellen zu verhindern. Da

es zahlreiche Gefahrenquellen gibt und ihnen möglichst effektiv begegnet werden soll, ist das Instrumentarium der Prävention breit gefächert. Während eine Schadensbehebung im Wesentlichen Beseitigungs-, Wiedergutmachungs- und Sanktionsmaßnahmen umfasst, sind die Mittel der Prävention beispielsweise

- staatliche Ge- oder Verbote,
- Überwachungs- und Kontrollmaßnahmen,
- Bildungs- und Aufklärungskampagnen,
- Warnungen und Empfehlungen,
- Vorteilsangebote im Falle eines erwünschten Verhaltens,
- finanzielle Sanktionen im Falle unerwünschten Verhaltens,
- Sicherstellung von Informationen und Wissen, insbesondere Expertenwissen.

Zumindest als Prinzip kennt die Risikoprävention keine immanenten gegenständlichen, personellen, räumlichen oder zeitlichen Grenzen. Sie lässt sich in zahlreichen Bereichen realisieren – etwa in den Feldern des Umweltschutzes, der Gesundheitsvorsorge, der Kriminalitätsverhütung, der unternehmerischen Geschäftstätigkeiten oder der privaten Verträge. Dabei lässt sie sich immer noch erweitern, immer noch vorverlagern und immer noch verbessern. Sie ist insbesondere auf eine immer umfassendere Informations- und Wissenserzeugung angelegt. Nicht nur den in Betracht kommenden Gefahrenquellen, auch den denkbaren Präventionsmaßnahmen sind kaum Grenzen gezogen. Setzt die Prävention ein, bevor ein Schaden unmittelbar droht, werden Präventionsmaßnahmen getroffen, obwohl ungewiss ist, ob diese Maßnahmen zur Schadensverhinderung überhaupt nötig sind. Möglicherweise ist sogar ungewiss – wie bei manchen Maßnahmen der Terrorismusbekämpfung, bei bestimmten Klimaschutzvorkehrungen oder bei einer Kreditablehnung auf der Basis rein statistischer Risikoaussagen –, ob die präventiven Maßnahmen überhaupt zum Schutz des gefährdeten Gutes beitragen. Es kann daher schwerfallen, den Sinn und die Effizienz von Präventionsmaßnahmen zu beurteilen.

Prävention hat erwünschte und unerwünschte Folgen

Auf den ersten Blick klingt Prävention ausschließlich positiv: Eine frühzeitige Vermeidung scheint besser zu sein als eine nachträgliche Beseitigung von Schäden. Bei näherer Betrachtung ergibt sich jedoch ein differenziertes Bild.

Erstens kann die Antwort auf die Frage, was als Schaden einzustufen ist, durchaus unterschiedlich ausfallen. Sie hängt nämlich von der Beschreibung der Ziele oder Schutzgüter und von den jeweiligen Interessen ab. So wird etwa eine private Krankenversicherung mit Rücksicht auf ihre wirtschaftlichen Interessen und ihre Gewinnorientierung bemüht sein, Personen, deren genetische Anlagen eine künftige Krankheit befürchten lassen, gar nicht oder nur unter Sonderkonditionen zu versichern. Aus ihrer Perspektive sind präventive Vorkehrungen, die dafür sorgen, dass sie von genetischen Risiken erfährt und ihre Vertragspolitik darauf einstellen kann, von Vorteil. Dagegen werden Personen mit diesen genetischen Risikofaktoren einen diskriminierungsfreien Krankenversicherungsschutz von vornherein nicht als Schaden einordnen. Aus ihrer Sicht erscheinen derart präventive Vorkehrungen als nicht gerechtfertigt.

Zweitens haben die zu Präventionszwecken eingesetzten Maßnahmen viele Wirkungen – nicht nur den beabsichtigten Nutzen, sondern auch Nachteile. Über ein Präventionsziel mag uneingeschränkter Konsens bestehen, beispielsweise über die Verhinderung von Gewalttaten. Eine generelle nächtliche Ausgangssperre zu dem Zweck, zumindest die oft im Schutz der Dunkelheit begangenen Gewalttaten zu vermeiden, würde diese einerseits unter Umständen tatsächlich verringern, andererseits jedoch zu einer massiven Beeinträchtigung individueller Entfaltungsmöglichkeiten führen. Ebenso würde eine umfassende Datensammlung über jeden Bürger und jede Bürgerin (Identifikationsdaten, genetische Merkmale, persönliche Eigenschaften, Bewegungsmuster, Kommunikationsverhalten usw.), auf die Staatsanwaltschaft und Polizei zugreifen könnten, die Straftatenaufklärung und -verfolgung zwar erleichtern, dies aber um den Preis eines massiven Freiheitseingriffs.

Das zeigt drittens, dass Prävention auch deshalb nicht einseitig beurteilt werden darf, weil sie sich immer auf mehrere Prognosen stützt. So etwa auf die Prognosen, dass

- ohne Präventionsmaßnahmen zukünftig ein Schaden eintritt,
- bestimmte Umstände Ursache dieses Schadens sind,
- der Schaden mit den gewählten Präventionsmaßnahmen verhindert werden wird.

Ob die Prognosen jeweils tatsächlich zutreffen, ist naturgemäß ungewiss. So würde im letzten Beispiel für den Fall einer etwaigen künftigen Strafverfolgung eine Vielzahl von Daten über zahlreiche Personen gesammelt, obwohl die meisten Menschen ihr Leben lang keine Straftat begehen.

Prävention ist also keineswegs uneingeschränkt vorteilhaft. Sie hat zugleich unerwünschte Folgen für die Gesellschaft oder für einzelne Bür-

ger und Bürgerinnen. Mit ihren Merkmalen und ihren teilweise unerwünschten Folgen stellt sie eine Herausforderung für die weitere Gewährleistung individueller und gesellschaftlicher Freiheiten dar.

2 Spannungsverhältnis zwischen Prävention und Freiheit

Rechtsstaat und Präventionsgesellschaft

Im Modell des liberalen Rechtsstaats wird Freiheit im Wesentlichen als Freiheit vom Staat begriffen. Dieses Modell hat historische Voraussetzungen und ihm liegen bestimmte Annahmen zugrunde: Die Gesellschaft vermag sich grundsätzlich selbst zu ordnen. Der Staat braucht individuelle Entscheidungs- und Verhaltensfreiheiten nur einzuschränken, sobald und sofern nach relativ gesicherten Erkenntnissen ein Anlass zum Einschreiten zu Gunsten des Allgemeinwohls oder der berechtigten Interessen anderer besteht.

Daraus ergeben sich klare rechtsstaatliche →Einschreitschwellen im Hinblick auf Zeitpunkt, Wissensgrundlagen und Adressaten:

- Staatliche Maßnahmen erfolgen in zeitlicher Hinsicht so früh wie nötig und so spät wie möglich.
- In sachlicher Hinsicht stützen sie sich auf ein hinreichendes Wissen sowohl über Sachlagen als auch über entstandene oder künftig entstehende Schäden.
- In personeller Hinsicht richten sie sich prinzipiell nur gegen die Personen, die für Gefahren oder Schäden verantwortlich sind.

Über diese staatlichen Einschreitgründe hinaus müssen die staatlichen Einschränkungsmaßnahmen gerechtfertigt sein. Das Übermaßverbot (s. auch Grundsatz der →Verhältnismäßigkeit) verlangt, dass die gewählten Maßnahmen im Hinblick auf das Schutzziel geeignet, als mildestes Mittel erforderlich und angemessen sind.[7] Im Abwägungsergebnis muss ihr Nutzen die Freiheitsbeeinträchtigungen überwiegen.

Die in der modernen Gesellschaft zentrale Präventionsidee basiert demgegenüber auf grundlegend anderen Annahmen. Freiheit wird mehrdimensional begriffen, insbesondere nicht nur als Freiheit vom Staat, sondern auch als Freiheit durch den Staat. Sie erfordert daher mehr als die bloße Abwesenheit staatlichen Zwangs, weil sie voraussetzungsvoll ist und die Gesellschaft diese Voraussetzungen eben nicht aus sich heraus mit ihrer Selbstregulierungskraft herstellen kann. Zumindest teilweise kann und muss der Staat dies leisten.

Im Vergleich zum Modell des liberalen Nachtwächterstaates[8] erhält der moderne Staat eine deutlich erweiterte Rolle, die sich auf die Gewährleistung von Sicherheit, Schutz oder Bildung, Kultur und Wohlfahrt erstreckt. Machtverhältnisse und Ungleichheiten zwischen Privaten soll er ausgleichen und private Interessenkonflikte angemessen regulieren. Mit den wachsenden Staatsaufgaben steigen die staatlichen Verantwortlichkeiten und die gesellschaftlichen Erwartungen an den Staat. Hinzu kommt der in der Risiko- und Informationsgesellschaft gewandelte Umgang mit Wissen, Ungewissheit und Nichtwissen. All dies führt zur Vervielfältigung der Anlässe staatlichen Einschreitens und zur Auflösung der bisherigen rechtsstaatlichen →Einschreitschwellen und Handlungsgrenzen. Zugleich steigt die gesellschaftliche Aufmerksamkeit für die Freiheitsbedrohungen, die es im Verhältnis Privater untereinander gibt.

Grundsätze der Präventionsgesellschaft

In der Präventionsgesellschaft gelten folgende Grundsätze im Hinblick auf Zeitpunkt, Wissensgrundlagen und Adressaten:

- Vorbeugungs- und Vorsorgemaßnahmen erfolgen in zeitlicher Hinsicht nicht so spät, sondern so früh wie möglich.
- In sachlicher Hinsicht hängen Vorbeugungs- und Vorsorgemaßnahmen nicht davon ab, dass gesicherte Tatsachen vorliegen und die zu erwartenden Schäden hinreichend wahrscheinlich sind.
- In personeller Hinsicht werden die Bürger und Bürgerinnen weit reichenden Überwachungen, Inpflichtnahmen, Einflussnahmen und Risikobeurteilungen ausgesetzt, ohne dass sie dafür einen Anlass gegeben haben.

Freiheitsbeeinträchtigungen können sich dadurch quantitativ vervielfachen und qualitativ intensivieren. Das gilt insbesondere, weil die Wurzeln von Risiken tief in Persönlichkeits- und Gesellschaftsstrukturen hineinreichen. Präventionsmaßnahmen zielen auch auf persönliche Einstellungen, Lebensweisen oder gesellschaftliche Muster und versuchen sie gegebenenfalls zu verändern.[9]

3 Präventionsgesellschaft und Präventionsdilemma

Präventionsstrategien stellen die klassischen Vorstellungen liberal-rechtsstaatlicher Freiheit in Frage. Wie erläutert, kennt Prävention als theoretisches Prinzip keine immanenten Grenzen. Einige kritische Stimmen

beklagen deswegen, die Präventionsidee sei notwendig mit dem Dilemma verbunden, dass sich Anlässe, Reichweite oder Tiefe präventiver Maßnahmen nicht begrenzen ließen. Die Präventionsidee dränge infolgedessen dazu, Präventionsmaßnahmen immer weiter vorzuverlagern und immer weiter auszudehnen. Sie führe zu immer größeren Freiheitsverlusten.

Im Ausgangspunkt darf man Prävention jedoch nicht als bloßen Verlust der Freiheit einstufen. Denn das liberal-rechtsstaatliche Modell hat Voraussetzungen – die Selbstregulierungskraft der Gesellschaft, die konservativ begrenzte Rolle des Staates oder die gesichertes Wissen unterstellende Erfassung und Beschreibung der Realität –, auf die man heute nicht mehr aufbauen kann. Unter den Bedingungen der modernen Gesellschaft muss man anerkennen, dass Prävention immer einerseits Vorteile, andererseits Nachteile hat. Von ihren Folgen her kann sie nicht nur freiheitsbeeinträchtigend wirken, sondern durchaus freiheitsfördernd oder vergleichsweise freiheitsschonend sein.

Im Weiteren muss man zwischen Präventionsprinzip und Präventionsverwirklichung unterscheiden. Als theoretisches Prinzip mag Prävention keine Grenzen haben. Aber sie wird nicht als theoretisches Prinzip, sondern in Form bestimmter Praktiken in verschiedenen Anwendungsfeldern realisiert. Ziele, Maßnahmen und Folgen lassen sich aufschlüsseln. Da Prävention so vielfältig ist, gibt es auch immer viele Ansatzpunkte einer ausgestaltenden und begrenzenden Regulierung.[10]

Das »Dilemma« der Prävention besteht deshalb nicht darin, dass man überhaupt keine Grenzen für die Anlässe, Reichweite oder Tiefe präventiver Maßnahmen mehr formulieren könnte. Das Präventionsdilemma besteht vielmehr darin, dass die zulässigen Strategien und die Grenzen der Prävention nicht mehr aus dem liberal-rechtsstaatlichen Modell ableitbar und im Wege der deswegen nötigen gesellschaftlichen oder politischen Entscheidungen nur schwer festzulegen sind. Denn man hat es mit einem sehr heterogenen Feld unterschiedlicher Interessen, mit unterschiedlichen Bewertungen und vor allem auch mit Prognoseproblemen sowie strukturellen Wissensdefiziten zu tun. Entscheidungen über Präventionsstrategien und -maßnahmen sind vielschichtig, Ergebnis komplexer Abwägungen und immer neu überprüfungsbedürftig. Dabei ergeben sich oft heftige und nachhaltige Meinungsstreitigkeiten.

Kontroverse gesellschaftliche Debatten sind allerdings notwendig, damit eine ausgewogene und hinreichend akzeptierte Regulierung der Prävention, ihrer näheren Ziele und ihrer Grenzen erreicht wird. Das Präventionsdilemma verweist insofern auf die Bedeutung politischer Macht- und Aushandlungsprozesse zwischen Staat, relevanten Institutionen, privaten

Interessengruppen und zivilgesellschaftlichen Organisationen.[11] In diesen Prozessen werden der Prävention, die theoretisch immer weiter ausgedehnt werden könnte, Grenzen gezogen.

4 Prävention und Datenschutz

Grenzen für immer weiter getriebene Präventionsstrategien sind unter anderem durch datenschutzrechtliche Regelungen möglich. Der Datenschutz bietet ein gutes Beispiel dafür, dass Prävention differenziert beurteilt werden muss und rechtlich gestaltet werden kann.

Datenschutzidee und Präventionsidee

Datenschutz dient nicht dem Schutz von Daten, sondern dem Freiheitsschutz sowohl der einzelnen Bürgerinnen und Bürger als auch der Gesellschaft insgesamt. Verfassungsrechtlich wird er breit verbürgt: durch das Grundrecht auf informationelle Selbstbestimmung[12], durch die Gewährleistungen der Unverletzlichkeit der Wohnung[13] und der Telekommunikation[14] oder durch Freiheitsrechte wie die Berufsfreiheit[15] oder die Versammlungsfreiheit. Hinzu kommt der Schutz durch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.[16] Die Grundrechte wirken nicht nur gegenüber staatlichem Verhalten. Sie beeinflussen zudem die Beziehungen Privater untereinander, indem sie den Staat verpflichten, diese Beziehungen grundrechtskonform – also auch datenschutzgerecht – zu regeln.

Im Näheren umfasst der Datenschutz ein Bündel von Schutzzielen und -interessen (siehe dazu auch den Beitrag von Rost in diesem Band, S. 353 ff.). Auf übergreifender Ebene dient er dem Schutz der einzelnen Person gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten, wie sie technisch heute ohne Weiteres möglich wären. Stichworte sind das allumfassende »Persönlichkeitsprofil« oder der »gläserne Bürger«. In der zunehmend technisierten und vernetzten Informationsgesellschaft zielt Datenschutz auch auf eine angemessene Gestaltung der IT-Systeme und technischer Infrastrukturen.

Zudem schützt der Datenschutz punktuell vor der Verarbeitung konkreter personenbezogener Daten. Das mögen Angaben über Geschehnisse in der Wohnung, über die Inhalte persönlicher Kommunikationen, über Krankheiten oder über eine Angewiesenheit auf staatliche Sozialleistungen sein. Dabei geht es nicht allein darum, dass solche Daten relativ vertraulich

bleiben. Ihre Erhebung, Speicherung, Nutzung oder Weitergabe soll nur zu legitimen Zwecken erfolgen. Insofern ist Datenschutz »kalkuliertes Nichtwissen«.[17] Eine wichtige und oft übersehene Funktion des Datenschutzes ist außerdem die Richtigkeit von Daten und Informationen.

Weiter gehört es zu den zentralen Zielen, Transparenz und die Wissenschancen der Bürger und Bürgerinnen um das sie selbst betreffende Wissen staatlicher Stellen oder Privater zu gewährleisten. Daten- und Informationsverarbeitungsvorgänge sollen nicht an den Betroffenen vorbei oder hinter ihrem Rücken verlaufen. Vielmehr haben die Betroffenen das Recht, davon zu erfahren. Und schließlich sollen sie auf Verarbeitungsvorgänge und auf das sie betreffende Wissen Anderer Einfluss nehmen können, etwa mit Berichtigungs-, Widerspruchs- oder Löschungsansprüchen.

Rechtlich ist der Datenschutz bislang vor allem für Daten und Informationen ausgearbeitet worden, deren Aussageinhalte auf bestimmte Personen bezogen werden können (personenbezogene Daten). Die Bürger und Bürgerinnen sind jedoch auch dann betroffen, wenn allein aufgrund gruppenbezogener statistischer Informationen eine negative Entscheidung über sie oder über ihr Anliegen gefällt wird. Präventionsstrategien können in genau dieser Form gestaltet sein. Ein Beispiel ist die Kreditvergabe aufgrund übergreifend errechneter *Score*-Werte (→ *Scoring*). Datenschutz kann auf solche Konstellationen erstreckt werden. Insoweit ist er Schutz vor ungerechtfertigten Entscheidungen und Diskriminierungsschutz.

Damit zeigt sich, dass Datenschutz einerseits selbst Präventionscharakter hat, indem er die Bürger und Bürgerinnen vor Einschüchterungseffekten, Stigmatisierungen oder Diskriminierungen bewahren, Verunsicherungen aufgrund mangelnder Transparenz von Datenverarbeitungen verhindern sowie den Risiken komplexer IT-Systeme begegnen will. Mit seinen Zielen führt er andererseits zugleich zu Vorgaben und Grenzen für staatliche oder private Datenverarbeitungen, die anderweitigen Präventionszwecken dienen. Datenschutzregeln können zum Beispiel Grenzen für polizeiliche Überwachungen zwecks Straftatenverhütung oder für private Datensammlungen zwecks Kreditsicherung setzen.

5 Datenschutzrechtliche Ansätze zum Umgang mit dem Präventionsdilemma

Auf das im Präventionsprinzip angelegte Problem unbegrenzter Datensammlungen und weit greifender Informationsvorsorge nach dem Motto »Alles kann ja irgendwann und irgendwo mal wichtig sein« reagiert der

Datenschutz mit grundlegenden Regelungen zur Zulässigkeit der Verarbeitung personenbezogener Daten (siehe auch den Beitrag von Hartge in diesem Band, S. 280 ff.). Unter anderem werden Verarbeitungsvorgänge an bestimmte Zwecke geknüpft und müssen für diese Zwecke erforderlich sein (zum Zweckbindungsgrundsatz siehe auch den Beitrag von Heckmann in diesem Band, S. 267 ff.). Bereits auf der Vorstufe gilt das Prinzip, dass die Aufgabenorganisation möglichst datensparsam gestaltet werden soll.

Mit solchen Vorgaben stellt der Datenschutz die Zwecke staatlicher oder privater Datenverarbeitungen als solche nicht unvermittelt in Frage. Prävention und Präventionsmaßnahmen werden im Grundsatz nicht verboten. Die datenschutzrechtlichen Vorgaben lenken aber die Aufmerksamkeit darauf, dass die Aufgaben so genau wie möglich beschrieben werden und Datenverarbeitungen dafür wirklich nötig sein müssen. Werden Präventionsaufgaben zu vage beschrieben, genügen sie den Anforderungen nicht. Indem sie präzise benannt werden müssen, werden sie zugleich in bestimmtem Umfang eingegrenzt. Datenschutz zwingt insofern zu Reflektionen und verlangt nach einer rationalen und von Beginn an ausgleichend-grenzziehenden Gestaltung von Prävention.

Mit Blick auf konkrete Schutzinteressen macht der Datenschutz darüber hinaus deutlich, dass selbst präzisierte Präventionsaufgaben und Präventionsmaßnahmen nicht um jeden Preis zulässig sind. Insoweit setzt er nähere Grenzen, unter anderem in Form sachlicher, zeitlicher oder personeller Einschreit- und Verarbeitungsschwellen. Das Bundesverfassungsgericht hat beispielsweise polizeiliche Vorfeldermittlungen davon abhängig gemacht, dass tatsächliche Anhaltspunkte für die Prognose vorliegen, dass »Zielpersonen« Straftaten zu begehen drohen. Darüber hinaus hat das Gericht den Kreis der Personen eingeschränkt, die einem präventiven Zugriff der Polizei unterliegen dürfen.[18]

Mit Blick auf eine Regelung in Großbritannien hat der Europäische Gerichtshof für Menschenrechte entschieden, dass eine generelle und undifferenzierte staatliche Befugnis, Fingerabdrücke, Zellproben und → DNA-Profile zwar verdächtigter, aber nicht verurteilter Personen auf Vorrat zu speichern, keinen fairen Interessenausgleich herstellt. Die generelle Speicherung der Fingerabdrücke sei in einer demokratischen Gesellschaft nicht notwendig.[19]

Die → Vorratsdatenspeicherung von Telekommunikationsdaten hat das Bundesverfassungsgericht als eine »vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten zur späteren anlassbezogenen Übermittlung« an Polizei und Nachrichtendienste bezeichnet und in dieser Form zwar nicht für grundsätzlich unzulässig gehalten, aber an enge Vor-

aussetzungen geknüpft (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.). Diese Beispiele zeigen, in welch vielfältiger Weise Präventionsstrategien datenschutzrechtlich eingrenzbar sind.

Datenschutzrechtliche Regelungen stellen des Weiteren die Transparenz von Datenverarbeitungen und Informationsrechte betroffener Personen sicher. Beispielsweise versucht der Gesetzgeber, durch solche Vorkehrungen die Interessenkonflikte auszugleichen, die zwischen Privaten beim Einsatz von → *Scoring*-Verfahren im Zusammenhang mit Kreditverträgen bestehen. Die neuen gesetzlichen Regelungen zu diesen Verfahren stellen nicht nur bestimmte Anforderungen an deren Durchführung. Sie erlegen der Vertragspartei, die sie einsetzt, außerdem Transparenz-, Aufklärungs- und Begründungspflichten auf.[20]

Vielfältige Lösungsmöglichkeiten des Präventionsdilemmas

Das Datenschutzrecht bietet insgesamt vielfältige Möglichkeiten zum Umgang mit dem Präventionsdilemma. Über die Angemessenheit der jeweils gefundenen Lösungen mag man streiten. Aber eben dieses stetige und immer wieder nötige Ringen um gute Entscheidungen macht den Kern des Präventionsdilemmas aus. Deswegen liefert es keinen Anlass zur Kapitulation, sondern viele Gründe, sich gegebenenfalls für bessere Lösungen einzusetzen.

Anmerkungen

1 Vgl. auch zur »vorverlagerten Kriminalisierung«: Wendy Fitzgibbon, Risikoträger oder verletzliche Individuen: über die präemptive Kriminalisierung von Menschen mit psychischen Problemen, in: Bettina Paul/Henning Schmidt-Semisch (Hrsg.), Risiko Gesundheit, Wiesbaden 2010, S. 227 ff. Unter präemptiver Kriminalisierung versteht Fitzgibbon einen Trend, bei dem die Zuschreibung der Kriminalität nicht mehr auf das konkrete Handeln eines Individuums, sondern auf die Zugehörigkeit zu einer Gruppe zurückgeführt wird, bei der eine hohe statistische Wahrscheinlichkeit einer Straftatenbegehung angenommen wird.

2 Siehe etwa Niklas Luhmann, Die Gesellschaft der Gesellschaft, Frankfurt/M. 1997, S. 1088 ff.

3 Beispiel: der See, der wegen einer minimalen Zusatzbelastung mit schädlichen Stoffen plötzlich »umkippt«.

4 Dazu etwa die Beiträge in Gotthard Bechmann (Hrsg.), Risiko und Gesellschaft, Opladen 1993.

5 Sogenanntes entscheidungsorientiertes Risikoverständnis, herausgestellt etwa bei Niklas Luhmann, Soziologie des Risikos, Berlin/New York 1991, S. 30 ff.

6 Rainer Wolf, Die Risiken des Risikorechts, in: Alfons Bora (Hrsg.), Rechtliches Risikomanagement, Berlin 1994, S. 65 (80 ff.).
7 Die Angemessenheit setzt eine Abwägung zwischen den positiven Folgen für die Rechtsgüter, die der Staat durch den Eingriff schützen möchte, und den negativen Folgen für diejenigen Rechtsgüter voraus, die durch den Eingriff beeinträchtigt werden. Im Abwägungsergebnis müssen die positiven Folgen die Freiheitsbeeinträchtigungen überwiegen.
8 Als Nachtwächterstaat bezeichnet man einen Staat, der nach der liberalen Staatsauffassung in möglichst wenigen Fällen tätig werden soll.
9 Näher dazu Dieter Grimm, Verfassungsrechtliche Anmerkungen zum Thema Prävention, in: ders., Die Zukunft der Verfassung, Frankfurt/M. 1991, S. 197 (198 ff.). Für das Recht der inneren Sicherheit Stefan Huster/Karsten Rudolph, Vom Rechtsstaat zum Präventionsstaat, in: dies. (Hrsg.), Vom Rechtsstaat zum Präventionsstaat, Frankfurt/M. 2008, S. 9 (17 ff.).
10 Bei adäquater Aufschlüsselung von Vorsorgestrategien gibt auch das Übermaßverbot Grenzen vor. Näher dazu Marion Albers, Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, Berlin 2001, S. 241 ff. Ausführlich zum Risikoregulierungsrecht Marion Albers, Risikoregulierung im Bio-, Gesundheits- und Medizinrecht, in: dies. (Hrsg.), Risikoregulierung im Bio-, Gesundheits- und Medizinrecht, Baden-Baden 2011, S. 9 (13 ff.).
11 Mit Blick auf Entscheidungsbedarf und strukturelle Wissensdefizite sind die Folgen der Prävention dahin beschrieben worden, dass der Willkürpegel des Rechts steige, so Niklas Luhmann, Ökologische Kommunikation, Opladen 1986, S. 144/145. Eine solche Beschreibung ist jedoch überspitzt. Richtig ist, dass aufgrund politischer Macht- und Aushandlungsprozesse Entscheidungen über die rechtliche Ausgestaltung und die rechtlichen Grenzen von Prävention getroffen werden müssen.
12 BVerfGE 65, 1 (S. 43/44); Az. 1 BvR 209, 269, 362, 420, 440, 484/83.
13 BVerfGE 109, 279; Az. 1 BvR 2378/98, 1084/99.
14 Etwa BVerfGE 100, 313 (S. 358 ff.); Az. 1 BvR 2226/94, 2420, 2437/95.
15 Dazu mit Differenzierungen BVerfGE 113, 29 (S. 48 ff.); Az. 1 BvR 1027/02.
16 Siehe BVerfGE 120, 274 (S. 302 ff.); Az. 1 BvR 370, 595/07; sowie den Beitrag von Papier in diesem Band, S. 67 ff.
17 So Spiros Simitis, Datenschutz – Notwendigkeit und Voraussetzungen einer gesetzlichen Regelung, Deutsche Verkehrssteuerrundschau (DVR)1973, S. 138 (154).
18 BVerfGE 113, 348 (364 ff.); Az. 1 BvR 668/04.
19 EGMR (Große Kammer), Urteil vom 4.12.2008 – 30562/04 u. 30566/04 –, in: Neue Juristische Online Zeitschrift 2010, S. 696.
20 Dazu insgesamt §§ 6a, 28b, 34 BDSG und zum Gesetzentwurf BT-Drs. 16/10529.

Thomas Petri

Sicherheitsbehördliche Datenverarbeitung

1 Die Trennung zwischen Polizei und Verfassungsschutz

In der Bundesrepublik Deutschland waren Polizeibehörden und Nachrichtendienste lange Zeit strikt getrennt. Diese Unterscheidung hat sich in der Zeit nach dem Zweiten Weltkrieg entwickelt. Im Rahmen der Verhandlungen über die Rückübertragung von Hoheitsrechten auf die deutschen Behörden gestatteten die alliierten Militärgouverneure der drei westlichen Siegermächte USA, Großbritannien und Frankreich im Jahr 1949 der deutschen Bundesregierung zwar, neben Bundespolizeibehörden auch eine Stelle »zur Sammlung und Verbreitung von Auskünften über umstürzlerische gegen die Bundesregierung gerichtete Tätigkeiten einzurichten«[1]. Diese Stelle dürfe aber keine polizeilichen Befugnisse erhalten. Diese im sogenannten »Polizeibrief« gemachte Auflage verfestigte sich zu dem sogenannten »Trennungsprinzip«[2]. Nach diesem Grundsatz erfüllen Polizei und Nachrichtendienste zwei unterschiedliche Funktionen, die voneinander zu trennen sind.

Aufgaben der Polizei

Die wichtigsten Aufgaben der Polizei bestehen darin,
- Gefahren abzuwehren,
- Störungen der öffentlichen Sicherheit zu beseitigen sowie
- die Staatsanwaltschaft bei der Strafverfolgung zu unterstützen.

Dazu gibt ihr der Gesetzgeber eine Vielzahl von unterschiedlichen Befugnissen, die es der Polizei erlauben, in die Grundrechte von Bürgerinnen und Bürgern einzugreifen. Im Grundgesetz (GG) ist vorgesehen, dass die Polizeiarbeit im Regelfall Aufgabe der Bundesländer ist.[3] Deshalb unterhält jedes Bundesland eine eigene Polizei, die nach dem Polizeigesetz des jeweiligen Bundeslandes zu handeln hat.

Es gibt jedoch auch Polizeibehörden des Bundes, vor allem das Bundeskriminalamt (BKA) und die Bundespolizei. Das BKA nimmt in erster Linie die Aufgabe einer »Zentralstelle für das polizeiliche Auskunfts- und Nachrich-

tenwesen« und »für die Kriminalpolizei« wahr.[4] Mit anderen Worten hat das BKA den notwendigen Informationsaustausch zwischen den Polizeibehörden der Länder zu koordinieren. Darüber hinaus unterstützt das BKA den Generalbundesanwalt bei der Verfolgung bestimmter schwerwiegender Straftaten. Im Jahr 2008 wurde eine Vorschrift[5] erlassen, die dem BKA die Aufgabe überträgt, Gefahren des internationalen Terrorismus in bestimmten Fällen abzuwehren. Diese Vorschrift ist verfassungsrechtlich umstritten, weil mit ihr das Trennungsprinzip durchbrochen wird.[6]

Die Bundespolizei hieß früher Bundesgrenzschutz. Auch noch heute stellt der polizeiliche Grenzschutz eine wesentliche Aufgabe der Bundespolizei dar. Darüber hinaus soll sie Bahnanlagen und Einrichtungen des Luftverkehrs sowie von Bundesorganen schützen.[7] Sie hat dazu alle Befugnisse, die Landespolizeibehörden üblicherweise auch haben.

Aufgaben der Nachrichtendienste

Zu den Nachrichtendiensten zählen:
- Militärischer Abschirmdienst (MAD),
- Bundesnachrichtendienst (BND),
- Bundesamt für Verfassungsschutz (BfV),
- Verfassungsschutzämter der Länder.

Im Unterschied zu den Polizeibehörden sammeln Nachrichtendienste Informationen über Vorgänge, die den Bestand des Staates gefährden könnten. Gemäß dem Polizeibrief hatten (und haben) Nachrichtendienste keine polizeilichen Befugnisse. Dies bedeutet, sie dürfen personenbezogene Daten zwar erheben, aber keine Zwangsmaßnahmen wie beispielsweise Verhaftungen oder Durchsuchungen von Personen vornehmen.

2 Offene Datenbeschaffung und »verdeckte Ermittlungsmethoden«

Datenerhebung durch die Nachrichtendienste

Es ist ein typisches Merkmal der Nachrichtendienste, dass sie Informationen heimlich sammeln. Charakteristisch für nachrichtendienstliche Methoden sind beispielsweise die Observation von verdächtigen Personen[8], verdeckte technische Überwachungsmittel[9] und insbesondere der Einsatz sogenannter V-Leute[10]. V-Leute sind für die Geheimdienste von großer Bedeutung,

weil sie in aller Regel bereits der zu überwachenden »Szene« angehören. Sie erhalten in der Regel sehr detaillierte Vorgaben durch den Geheimdienst (»V-Mann-Führung«).

Besonders der Einsatz von V-Leuten stößt auf Bedenken, weil sich der Rechtsstaat den Vertrauensbruch einzelner Bürgerinnen und Bürger zu Nutze macht, um so an Informationen über Dritte zu gelangen.[11] Aus Sicht des Datenschutzrechts ist der Einsatz von V-Personen zwar nicht generell menschenrechtswidrig. In einem freiheitlichen Rechtsstaat muss er sich jedoch im Rahmen klarer gesetzlicher Grenzen bewegen und von ausreichenden Sicherungen gegen Missbrauch begleitet sein. Insbesondere ist ein eindeutiges und vorhersehbares Verfahren erforderlich, um die fraglichen Verfahren zu genehmigen, durchzuführen und zu überwachen.[12] Diese Grundsätze werden aber in der Praxis nicht immer eingehalten.

Dazu ein Beispiel: Das Bundesverfassungsgericht hat ein von der Bundesregierung angestrengtes Parteiverbotsverfahren gegen die Nationaldemokratische Partei Deutschlands (NPD) im Jahr 2003 vor allem deswegen eingestellt[13], weil diese Partei in extensiver Weise von V-Leuten durchsetzt war. Das Gericht sah darin die Gefahr, dass Mitarbeiter der Geheimdienste die Zielsetzungen und die Tätigkeit der NPD maßgeblich mitbestimmten.

Ein anderer Teil der Datenerhebung bei den Geheimdiensten erfolgt offen und ist demgegenüber weniger spektakulär: Er besteht in dem Sammeln und Auswerten »allgemein zugänglicher Quellen«. Dabei wertet der Geheimdienst relevante Zeitschriften- und Zeitungsartikel sowie Verlautbarungen von Organisationen aus, die er als verfassungsfeindlich einstuft. Wer die Berichte der Verfassungsschutzämter des Bundes und der Länder aufmerksam liest, wird feststellen, dass die dort zusammengestellten Informationen zumeist aus solchen allgemein zugänglichen Quellen stammen dürften.

Datenerhebung durch die Polizei

Gegenüber dem grundsätzlich heimlichen Sammeln von Informationen durch Geheimdienste unterschied sich das Grundkonzept der Polizeien nach 1949 darin, dass die Polizei den Bürgerinnen und Bürgern mit »offenem Visier« gegenübertrat. Prinzipiell gilt dieses Konzept heute ebenfalls, inzwischen gibt es jedoch viele Ausnahmen. Nach und nach sind nämlich die Polizeien des Bundes und der Länder ebenfalls mit zahlreichen verdeckten Ermittlungsmethoden ausgestattet worden. Derartige heimliche Ermittlungsinstrumente waren früher den Geheimdiensten als den »Früh-

warnsystemen« unseres Rechtsstaates vorbehalten, sie werden deshalb auch heute noch oft als »nachrichtendienstliche Methoden« oder euphemistisch als »besondere Mittel der Datenerhebung« bezeichnet. Einige Beispiele dazu: Auch die Polizei setzt (allerdings seltener als die Geheimdienste) heute in bestimmten Kriminalitätsbereichen V-Leute und verdeckte Ermittler[14] ein. Zur Strafverfolgung darf sie unter den gesetzlichen Voraussetzungen der Strafprozessordnung Telekommunikationsüberwachungen (TKÜ) durchführen, das heißt heimlich Telefongespräche abhören oder auch von Telekommunikationsdiensten die Herausgabe von Informationen über Telekommunikationsverbindungen verlangen.

Verfassungsrechtlich nur unter engen Voraussetzungen zulässig ist die akustische Wohnraumüberwachung, die man auch als → Großen Lauschangriff bezeichnet. Dabei hören die Strafverfolgungsbehörden mit Hilfe von technischen Mitteln heimlich Gespräche ab, die in geschlossenen Räumen (Wohnungen, Geschäftsräume usw.) geführt werden.

Online-Durchsuchung und andere verdeckte Maßnahmen der Polizei

Bekannt geworden, aber nach der Strafprozessordnung nicht zugelassen, ist die »*Online*-Durchsuchung«: Dabei infiltrieren Sicherheitsbehörden informationstechnische Systeme mit Hilfe von Schadprogrammen, um an die auf den Systemen gespeicherten Daten zu gelangen. Da heute viele Nutzende mithilfe ihrer IT-Systeme auch telefonieren und E-Mails austauschen, kann durch eine solche Infiltration von IT-Systemen auch die (Tele-)Kommunikation überwacht werden. Dies nennt man »Quellen-TKÜ«. Diese Art der Überwachung hat das Bundesverfassungsgericht in seinem Urteil zur »*Online*-Durchsuchung«[15] nicht eingeschränkt. Ausdrücklich unzulässig ist jedoch das Kopieren sämtlicher auf dem Rechner gespeicherter Daten wie es bei der *Online*-Durchsuchung mit Hilfe eines → Trojaners erfolgt. Trotz dieser Vorgaben wurde im September 2011 bekannt, dass die Polizei solche Trojaner ohne eine hinreichend konkrete gesetzliche Grundlage in der Strafprozessordnung eingesetzt hat.[16] Dies hat die Debatte um die *Online*-Durchsuchung neu entfacht. Im Bereich der Strafverfolgung erfolgen verdeckte Ermittlungen der Polizei unter Anleitung der Staatsanwaltschaften. Sie sollen die Rechtmäßigkeit des Ermittlungsverfahrens gewährleisten.

Für die Zwecke der Gefahrenabwehr werden die Polizeien in eigener Verantwortlichkeit tätig; auch hier werden die beschriebenen heimlichen Ermittlungsmaßnahmen im Bundeskriminalamtsgesetz und in einigen Länderpolizeigesetzen der Polizei gestattet.[17] Solche heimlichen Ermitt-

lungsmethoden sind häufig effektiv. Allerdings ist der Preis hoch, den der Rechtsstaat hierfür bezahlt. Wenn beispielsweise ein Gespräch in einer Wohnung oder im Rahmen eines Telefonats abgehört wird, erhalten die Ermittler oft überwiegend banale, aber auch intime Informationen, die mit einer begangenen Straftat oder mit einer bevorstehenden Gefahr nichts zu tun haben. Bei der *Online*-Durchsuchung erhalten die Sicherheitsbehörden typischerweise auf einen Schlag Zugriff auf große Datenbestände, die einen sehr weitgehenden Aufschluss über die Persönlichkeit der betroffenen Person geben.

Verdeckte Ermittlungsmethoden stellen einen besonders tiefen Eingriff in die Privatsphäre der überwachten Menschen dar.[18] Betroffen sind zahlreiche Grundrechte, die dem Schutz der Persönlichkeit der Menschen dienen, beispielsweise

- die Garantie der Unverletzlichkeit der Wohnung aus Artikel 13 GG,
- das Fernmeldegeheimnis aus Artikel 10 GG,
- das allgemeine Persönlichkeitsrecht aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG.

In besonders gelagerten Fällen können die Ermittlungen sogar das höchste Rechtsgut unserer Verfassung, nämlich die Menschenwürde aus Artikel 1 Absatz 1 GG verletzen. Regelmäßig droht ein solcher Verstoß, wenn höchstvertrauliche Gespräche überwacht werden, beispielsweise Beicht- oder Therapiegespräche, in denen Menschen mit seelischen Nöten kämpfen oder um ihre Identität ringen. Das Bundesverfassungsgericht spricht insoweit von einem »absolut geschützten Kernbereich privater Lebensgestaltung«[19], der auch von Ermittlungsbehörden in jedem Fall zu respektieren ist. Sowohl der Gesetzgeber als auch die Behörden sind verfassungsrechtlich verpflichtet, Schutzvorkehrungen zu treffen, um keine Daten zu erheben, die den Kernbereich privater Lebensgestaltung betreffen. Erfolgt gleichwohl eine Erhebung von solchen Daten, müssen sie sofort gelöscht und dürfen nicht verwendet werden. Im Übrigen muss der Rechtsstaat dafür sorgen, dass verdeckte Ermittlungen nur in einem angemessenen Umfang gegen die Bürgerinnen und Bürger eingesetzt werden. Der Gesetzgeber muss dazu in der Regel strenge Voraussetzungen an den Einsatz verdeckter Ermittlungsmethoden aufstellen.

Wie die Entscheidungen des Bundesverfassungsgerichts zeigen, haben die Gesetzgeber des Bundes und der Länder diese verfassungsrechtliche Pflicht nicht immer erfüllt, sondern bisweilen die Befugnisse der Sicherheitsbehörden zu einseitig zu Gunsten von Sicherheitsinteressen ausgestaltet.

3 Ermittlungsmethoden mit großer Streubreite

Eine relativ neue Entwicklung bei den polizeilichen Ermittlungen wird durch die moderne Informationstechnologie ermöglicht. Die herkömmlichen Ermittlungsmethoden betreffen in der Regel einen überschaubaren Kreis von Personen, die zumeist auch in einem engen Verhältnis zu einer Straftat oder einer drohenden Gefahr stehen. Neuere Ermittlungsmethoden führen wegen ihrer enormen Streubreite jedoch oftmals dazu, dass häufiger Unbeteiligte verdächtigt werden.

Zu diesen neuen Ermittlungsmethoden, auf die nachfolgend eingegangen wird, zählen beispielsweise

- Rasterfahndungen,
- automatisierter Kfz-Kennzeichenabgleich und
- präventive Videoüberwachungen öffentlicher Räume.

Rasterfahndung

Bei der Rasterfahndung fertigt die handelnde Sicherheitsbehörde im Rahmen ihrer Ermittlung ein Eigenschaften-Profil der Personen an, die sie sucht. Anschließend beschafft sie bei Stellen, die entsprechende Daten gespeichert haben, alle verfügbaren einschlägigen Datensätze. Zum Abgleich beschaffen sich die Fahndungsbehörden vor allem Daten von Energieversorgungsunternehmen, Ausländerbehörden und Hochschulen. Diese Datensätze werden mit dem erstellten Raster (Profil) verglichen. Die Trefferfälle werden als Ansatz für weitere Ermittlungen verwendet. Diese Fahndungsmethode wurde in den 1970er Jahren im Rahmen der RAF-Fahndungen erstmals im großen Stil eingesetzt und erfuhr nach den Terroranschlägen vom 11. September 2001 eine Art Wiedergeburt.[20]

Das Bundesverfassungsgericht hat jedoch entschieden, dass eine präventive polizeiliche Rasterfahndung mit dem Grundrecht auf informationelle Selbstbestimmung nur vereinbar ist, wenn eine konkrete Gefahr für hochrangige Rechtsgüter wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person gegeben ist.[21] Im Vorfeld der Gefahrenabwehr scheidet eine solche Rasterfahndung aus. Es müssen nach Auffassung des Gerichts tatsächliche Anhaltspunkte vorliegen, die eine konkrete Gefahr belegen. Es genügt nicht, auf eine allgemeine Bedrohungslage zu verweisen.

Automatisierter Kfz-Kennzeichenabgleich

Ganz ähnlich wie die Rasterfahndung beruht die Kfz-Kennzeichen-Erfassung auf einem massenhaften Abgleich von persönlichen Daten mit polizeilichen Datenbeständen: Dabei erfasst eine an einer Straße aufgestellte Kamera die Kraftfahrzeugkennzeichen aller vorbeifahrenden Kraftfahrzeuge. Diese Kennzeichen werden dann digitalisiert und mit Fahndungsdatenbanken abgeglichen. Das Bundesverfassungsgericht hat die Regelungen mehrerer Bundesländer, die einen solchen Abgleich vorsahen, für nichtig erklärt. Die automatisierte Erfassung von Kfz-Kennzeichen darf nach Ansicht des Gerichts nicht ohne Anlass, das heißt ohne konkrete Gefahr, erfolgen oder flächendeckend durchgeführt werden.[22]

Präventive Videoüberwachung öffentlicher Orte

Etwas anders gelagert ist die Videoüberwachung öffentlicher Orte. Dort werden alle Personen, die den überwachten Raum betreten, erfasst und zumeist auch aufgezeichnet. Teilweise erfolgt diese Form der Überwachung, ohne dass die Betroffenen sie bemerken. Bei Castor-Transporten in Gorleben setzte die Polizei beispielsweise Drohnen[23] ein, um die Demonstrierenden aus der Luft zu überwachen.[24]

Das Bundesverfassungsgericht hat im Jahr 2009 eine Vorschrift des bayrischen Polizeigesetzes für verfassungswidrig erklärt, die es der Polizei erlaubte, präventiv Übersichtsaufnahmen im Vorfeld von Versammlungen zu machen.[25] Auch bei der Videoüberwachung öffentlicher Räume muss also zumindest eine Gefahr vorliegen, bevor die Polizei das Verhalten der Versammlungsteilnehmer überwachen darf. Eine Überwachung ohne jeden Anlass ist nicht gerechtfertigt.

Solche Ermittlungsmethoden mit großer Streubreite betreffen viele Menschen, die keinen Anlass für einen Straftatverdacht gegeben haben. Trotzdem laufen sie insbesondere bei den dargestellten Methoden Gefahr, Objekt von Ermittlungen zu werden.

4 Datenbanken bei der Polizei

Allein die Erfassung von Personen in den Datenbanken der Sicherheitsbehörden stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar, der im Hinblick auf die Eingriffsintensität häufig unterschätzt wird. In Bezug auf die polizeiliche Datenverarbeitung ist vor allem das Kriminal-

aktennachweissystem »KAN« zu nennen. Der Kriminalaktennachweis ist ein polizeiliches elektronisches Informationssystem. Sein Hauptzweck ist die Erteilung einer aktuellen Kurzauskunft über die in den Kriminalakten enthaltenen Unterlagen zu

- Straftaten,
- schwerwiegenden Ordnungswidrigkeiten sowie über
- Unterlagen und Hinweise, die der Gefahrenabwehr oder vorbeugenden Kriminalitätsbekämpfung dienen.

Zugangs- beziehungsweise abfrageberechtigt sind in der Regel alle Polizeivollzugsbeamten und -beamtinnen sowie Beschäftigte der Polizei, wenn diesen bestimmte Aufgaben übertragen wurden.

Sehr häufig kommt es dabei vor, dass Personen als Tatverdächtige oder Beschuldigte zunächst rechtmäßig gespeichert werden. Im Laufe des Ermittlungsverfahrens oder auch im anschließenden Gerichtsverfahren erhärtet sich dieser Tatverdacht jedoch nicht immer. Der Rechtsprechung zufolge dürfen die Polizeibehörden die Daten der betroffenen Person dann – und nur dann – weiterspeichern, wenn ein (Rest-)Tatverdacht von ausreichender Substanz verbleibt und nicht auszuschließen ist, dass die Speicherung der Daten des Beschuldigten künftig bei der vorbeugenden Straftatenbekämpfung von Nutzen sein könnte.[26]

Den Erfahrungen der Datenschutzbehörden zufolge werden diese Grundsätze der Rechtsprechung immer wieder verletzt.[27] Diese Verstöße beruhen nicht zwingend auf einem bösen Willen der handelnden Polizeibeamten, sondern sind systembedingt, weil die Polizei oft nicht erfährt, aus welchen Gründen ein Verfahren eingestellt oder ein Tatverdächtiger freigesprochen wird. Was bleibt, sind allerdings die Freiheitsbeschränkungen und -gefährdungen, die sich aus derartigen Datenspeicherungen für die Betroffenen ergeben. Neben dem Umstand, dass die betroffene Person bei der Polizei nach wie vor als verdächtig gilt, kann sie auch berufliche Nachteile erfahren (zum Beispiel anlässlich von Zuverlässigkeitsüberprüfungen).[28]

Abweichend von den allgemeinen datenschutzrechtlichen Grundsätzen ist die Polizei regelmäßig gesetzlich nicht dazu verpflichtet, die betroffenen Personen unabhängig von einer Anfrage über die Datenspeicherung zu informieren. Sofern eine Person also Verdächtige in einem strafrechtlichen Ermittlungsverfahren gewesen ist, ist zu empfehlen, nach Einstellung dieses Verfahrens beziehungsweise nach einem Freispruch vor Gericht einen datenschutzrechtlichen Auskunftsanspruch bei der Polizei geltend zu machen und gegebenenfalls die Löschung der Daten einzufordern.

In der Eingriffsintensität gesteigert sind Struktur- und Fallanalysedateien, die insbesondere bei der Bekämpfung organisierter Kriminalität eingesetzt werden. Diese Systeme sind teilweise »lernfähig« und in der Lage, bislang nicht erkannte Querverbindungen zwischen verschiedenen Ermittlungsverfahren herzustellen.

Dazu ein fiktives Beispiel: Wenn in einem Ermittlungsverfahren ein roter Pkw mit dem amtlichen Kennzeichen AB 123 erfasst wird, und genau dieser Pkw bereits in einem anderen Verfahren gespeichert wurde, dann meldet das Verarbeitungssystem diesen Umstand. Auf diese Weise kann die Polizei aus ihren eigenen Datenbeständen mithilfe der Informationstechnologie neue Ermittlungsansätze schaffen. Zugleich entsteht das Risiko, dass unbescholtene Bürger und Bürgerinnen aufgrund von Zufälligkeiten in das Fahndungsvisier geraten.

Bedenklich ist die aktuelle Entwicklung zu Dateien, die behördenübergreifende Datenzugriffe erlauben. Solange es im Rahmen eines sicherheitsbehördlichen Bereichs bleibt, stößt dies nicht grundsätzlich auf rechtsstaatliche Bedenken, wenn dabei das Prinzip der →Verhältnismäßigkeit beachtet wird. Seit langem besteht das gemeinsame polizeiliche Informationsverbundsystem (INPOL). Dieses Verbundsystem wird beim BKA geführt. Sowohl die Kriminalpolizeien des Bundes und der Länder als auch der Zoll sowie das Zollkriminalamt können Daten eingeben und bei Bedarf abrufen. Zu Recht sehr umstritten sind allerdings gemeinsame Dateien von Behörden, die unterschiedliche Aufgaben zu erfüllen haben, beispielsweise Geheimdienste und Polizeibehörden. Aus rechtsstaatlicher Sicht besteht hier unter anderem die Besorgnis, dass bei solchen Dateien das eingangs vorgestellte Prinzip der Trennung von Geheimdiensten und Polizeien umgangen wird. Beispielsweise ist gegen die sogenannte »Antiterrordatei« deshalb Verfassungsbeschwerde eingelegt worden.

5 Veränderung der Sicherheitsarchitektur durch neue Trends sicherheitsbehördlicher Datenverarbeitung

Die Bekämpfung der organisierten Kriminalität und des internationalen Terrorismus haben in den letzten Jahren dazu geführt, dass sich die oben beschriebene Verteilung der Aufgaben und Befugnisse zwischen Polizei und Nachrichtendiensten verändert hat. Überwiegend kritisch wird insoweit von einem Umbau der Sicherheitsarchitektur gesprochen.

Gemeint ist damit, dass die Gesetzgeber Sicherheitsaufgaben zentralisieren, den Sicherheitsbehörden einander überschneidende Aufgaben zuwei-

sen, sie zu einer Intensivierung des Informationsaustausches anhalten und allgemein polizeiliche Befugnisse in das Vorfeld der klassischen Gefahrenabwehr verlagern. So haben die Verfassungsschutzbehörden einiger Länder jetzt auch die traditionell polizeiliche Aufgabe zur Beobachtung der organisierten Kriminalität.

Ein Wesensmerkmal dieser Sicherheitsgesetze ist eine immer weiter ins Vorfeld verlagerte Eingriffsbefugnis.[29] Der Staat soll möglichst früh einschreiten dürfen, um befürchtete Gefahren von unserem Gemeinwesen abzuwenden (siehe auch den Beitrag von Albers in diesem Band, S. 102 ff.). Das führt dann zu Beobachtung, Kontrolle und Überwachung von Personen, die zwar noch nichts Gesetzwidriges getan haben, denen die Sicherheitsbehörden aber wegen bestimmter Persönlichkeitsmerkmale einen Verstoß zutrauen.

Darüber hinaus ist seit den Terroranschlägen vom 11. September 2001 die informationelle Zusammenarbeit auf nationaler, europäischer und internationaler Ebene intensiviert worden. In Deutschland wurden unter anderem folgende Einrichtungen neu geschaffen:

- das »Gemeinsame Terrorismusabwehrzentrum« (→ GTAZ),
- das »Gemeinsame Internetzentrum« (→ GIZ),
- die Antiterrordatei (ATD)[30].

Auf europäischer Ebene gibt es unter anderem folgende Datenbanken, Initiativen und Einrichtungen:

- die *Counter Terrorist Group* (CTG)[31] und die übergreifende Auswertung des Internet *Check the Web* im Rahmen von Europol
- das Schengener Informationssystem (SIS)[32]
- die Fingerabdruckdatenbank Eurodac[33]
- das Visa-Informationssystem (VIS)[34]
- das *Advance Passenger Information System* (APSIS)[35]
- das *Customs Information System* (CIS)[36]
- die *Customs file identification database* (FIDE).

Weitere Datenaustauschsysteme mit europäischen beziehungsweise internationalen Bezügen sind im sogenannten Vertrag von Prüm,[37] in Flugpassagierabkommen mit den USA, Australien und Kanada und in Bezug auf die europäische Polizeibehörde Europol geregelt. In Deutschland wurde dafür zumindest im Bereich der Terrorismusbekämpfung die sicherheitsbehördliche Datenverarbeitung zentralisiert.[38]

Je mehr Aufgabenüberschneidungen geschaffen werden, je mehr Aufgaben auf die Ebene der europäischen Zusammenarbeit verlagert werden,

je mehr Befugnisse auch für Maßnahmen im Vorfeld konkreter Gefahren vorgesehen werden, desto mehr Effektivität erhofft man sich bei der Bekämpfung schwerwiegender Kriminalitätsformen. Unabhängig davon, ob diese Annahme stimmt: Als Kehrseite wird es für die Bürgerinnen und Bürger immer schwerer, ihre Grundrechte wahrzunehmen, wobei es keine Rolle spielt, ob sie rechtstreu sind oder nicht. Wer einmal versucht hat, sein Recht auf Auskunft oder Datenlöschung gegenüber einer europäischen Sicherheitsbehörde durchzusetzen, wird dies bestätigen können. Eine besondere Herausforderung insbesondere bei der Schaffung von Befugnissen europäischer Sicherheitsbehörden liegt deshalb in der Gewährleistung eines effektiven Grundrechtsschutzes.

Die beschriebenen Trends mögen vor dem Hintergrund einer informationell stark vernetzten organisierten Kriminalität und von Terrornetzwerken wie *Al Quaida* gut begründbar sein. Ebenso wichtig für den freiheitlichen Rechtsstaat ist jedoch die Beachtung der Grundrechte und der rechtsstaatlichen Prinzipien. Sie sollen gewährleisten, dass sich unsere Gesellschaft in ihren Grundstrukturen nicht so sehr verändert, dass ihr Freiheitscharakter verloren geht. Nicht nur die zitierten Entscheidungen des Bundesverfassungsgerichts verdeutlichen, dass der freiheitliche Rechtsstaat beim Umbau der Sicherheitsarchitektur insoweit wachsam bleiben muss.

Anmerkungen

1 Zitiert nach »Letter from the military governors to the parliamentary council defining the powers of the federal governments in the police field« – sogenannter »Polizeibrief« der drei Allierten Militärgouverneure an den Parlamentarischen Rat vom 14.4.1949 (Regelung Ziffer 2): »The Federal Government will also be permitted to establish an agency to collect and disseminate information concerning subversive activities directed against the Federal Government. This agency shall have no police authority.« Die deutsche Fassung ist im Internet abrufbar unter http://www.verfassungen.de/de/de49/grundgesetz-schreiben49-3.htm.

2 Das »Trennungsprinzip« geht unter anderem darauf zurück, dass die »geheime Staatspolizei« (kurz: Gestapo) während der NS-Diktatur die Befugnisse einer Polizeibehörde und eines Nachrichtendienstes innehatte. Diese »doppelte« Befugnis nutze die Gestapo unter anderem zur systematischen Überwachung und Verfolgung politischer Gegner. Das Trennungsgebot sollte der erneuten Entstehung eines übermächtigen Überwachungsstaates entgegenwirken.

3 Das ergibt sich aus den Artikeln 70 und 83 GG.

4 Diese Funktion ergibt sich aus Artikel 87 Absatz 1 GG.

5 Gemäß § 4a des Gesetzes über das Bundeskriminalamt (BKA) und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG). Die *Aufgaben* des BKA sind im Grundgesetz (GG) ausdrücklich benannt. So sieht Artikel 73 Absatz 1 Nr. 10 GG die Einrichtung eines Bundeskriminalpolizeiamtes und die Abwehr von Gefahren des internationalen Terrorismus durch das BKA als Gesetzgebungskompetenz des Bundes vor. Nicht ausdrücklich vorgesehen ist aber die Befugnis zur internationalen Verbrechensbekämpfung *durch* das BKA. Gegen zahlreiche neue Vorschriften des BKAG, die mit der Aufgabe nach § 4a BKAG in Zusammenhang stehen, sind im Sommer 2010 mehrere Verfassungsbeschwerden eingereicht worden (Az. 1 BvR 966/09 u. a.).

6 Die Vorgaben des Polizeibriefs entfalten heute keine unmittelbaren verfassungsrechtlichen Bindungswirkungen mehr. Das Trennungsgebot wird heute nach Auffassung des Bundesverfassungsgerichts aus dem Rechtsstaatsprinzip sowie aus grundgesetzlichen Kompetenzvorschriften (Art. 73 Nr. 10 und Art. 87 Abs. 1 S. 2 GG) abgeleitet.

7 Die Aufgaben der Bundespolizei ergeben sich vor allem aus den §§ 2–6 Bundespolizeigesetz; § 7 regelt die Aufgaben der Bundespolizei im Verteidigungs- oder Notstandsfall.

8 Als Observation gilt die regelmäßig heimliche, auf gewisse Dauer angelegte Beobachtung einzelner Personen.

9 Dazu zählen beispielsweise das Abhören von Telefongesprächen, das Abhören von Gesprächen in Wohnungen und verdeckte Videoaufzeichnungen.

10 Das Kürzel »V« steht hier für »Vertrauen«. Vertrauensleute sind Privatpersonen, die bereit sind, mit staatlichen Behörden über einen längeren Zeitraum vertrauensvoll zusammenzuarbeiten. Das Motiv für diese vertrauensvolle Kooperation kann uneigennützig sein, häufig erkaufen sich Sicherheitsbehörden jedoch auch die Zusammenarbeit mit Geld oder mit anderen Vergünstigungen.

11 Vgl. dazu bereits Klaus Lüderssen (Hrsg.), V-Leute. Die Falle im Rechtsstaat, Frankfurt/M. 1985.

12 Das hat auch der Europäische Gerichtshof für Menschenrechte (EGMR) festgestellt, vgl. EGMR, Entscheidung vom 5.2.2008, in: Neue Juristische Wochenschrift (NJW) 2009, S. 3565 ff.; Az. 74420/01; im Internet unter http://www.hrr-strafrecht.de/hrr/egmr/01/74420-01.php.

13 BVerfGE 107, 339; Az. 2 BvB 1, 2, 3/01.

14 Verdeckte Ermittler sind Polizeibeamte, die unter einer »Legende« in die zu beobachtende Szene eingeschleust werden, um dort unerkannt als Polizeibeamte zu ermitteln.

15 BVerfGE 120, 274; Az. 1 BvR 370/07; 1 BvR 595/07.

16 Vgl. http://www.ccc.de/de/updates/2011/analysiert-aktueller-staatstrojaner. Die Rechtssprechung hält die Quellen-TKÜ gleichwohl teilweise für rechtmäßig.

17 Als Beispiel hier die Bestimmungen im Bundeskriminalamtsgesetz (BKAG): zur TKÜ siehe § 20l BKAG; zur Erhebung von Telekommunikations-Verkehrsdaten siehe § 20m BKAG; zur *Online*-Durchsuchung siehe § 20k BKAG; zur akustischen Wohnraumüberwachung siehe § 20h BKAG.

18 Darauf hat auch das Bundesverfassungsgericht wiederholt hingewiesen: zur Online-Durchsuchung und zur Quellen-TKÜ siehe Urteil vom 27.2.2008, 1 BvR 370/07 (und andere); zur akustischen Wohnraumüberwachung siehe Urteil vom 3.3.2004 – 2378/98; zur vorbeugenden TKÜ siehe Urteil vom 27.7.2005 – 1 BvR 668/04.
19 BVerfGE 109, 279; Az. 1 BvR 2378/98; 1 BvR 1084/99.
20 Anders als bei der Ermittlung von RAF-Terroristen erbrachten die Rasterfahndungen zur Terrorabwehr in den Jahren 2001/2002 keinen zählbaren Erfolg.
21 BVerfGE 115, 320; Az. 1 BvR 518/02.
22 BVerfGE 120, 378; Az. 1 BvR 2074/05 und 1 BvR 1254/07.
23 Vom Boden funkgesteuertes Fluggerät ohne Besatzung, das zur Überwachung, Erkundung und Aufklärung verwendet werden kann.
24 Vgl. etwa Oliver Das Gupta, Sehenden Auges in die Panne, SZ-Online v. 17.11.2010, im Internet unter http://www.sueddeutsche.de/politik/drohneneinsatzbeim-castortransport-sehendenauges-indie-panne-1.1025003.
25 BVerfGE 122, 342; Az. 1 BvR 2492/08.
26 BVerfG in: NJW 2002, S. 3231; BVerfGK 8, 165; Az. 1 BvR 2293/03.
27 Vgl. beispielsweise Bayerischer Landesbeauftragter für Datenschutz, 18. Tätigkeitsbericht, Abschnitt 5.3.1; ders., 21. Tätigkeitsbericht, Abschnitt 7.1; ders., 22. Tätigkeitsbericht, Abschnitt 4.1; alle im Internet unter www.datenschutz-bayern.de.
28 Vgl. Bayerischer Landesbeauftragter für Datenschutz, 24. Tätigkeitsbericht (2010), Abschnitt 3.11.
29 Vgl. Benno Zabel, Terrorgefahr und Gesetzgebung, in: Juristische Rundschau (JR) 2009, S. 453 ff.; Fredrik Roggan, Das neue BKA-Gesetz – Zur weiteren Zentralisierung der deutschen Sicherheitsarchitektur, in: NJW 2009, S. 257 ff.; Hans Elmar Remberg, Die Bekämpfung des islamistischen Terrors, in: Kriminalistik 2008, S. 82 ff.; Martin H. W. Möllers/Robert Chr. van Ooyen, Bundeskriminalamt, Bundespolizei und »neue« Sicherheit, in: Das Parlament (Beilage) 48/2008, S. 26 ff.
30 Anm. d. Red.: Die ATD ist eine seit 1.3.2007 bestehende gemeinsame Datenbank deutscher Sicherheitsbehörden (Polizei und Nachrichtendienste sowie Staatsschutz und Zollkriminalamt). In ihr sind des islamistischen Terrorismus verdächtige Personen sowie damit in Verbindung stehende Kommunikationseinrichtungen und Bankverbindungen gespeichert. Mit der ATD wurden zuvor getrennte, bei verschiedenen Behörden angesiedelte Sicherheitsdateien zusammengeführt. Ziel der ATD ist es, weit im Vorfeld potenzielle Attentäter zu erkennen und den Informationsaustausch der Sicherheitsbehörden zu erleichtern. Die Datei wird vom Bundeskriminalamt verwaltet, derzeit (Stand: Juni 2011) verzeichnet sie 18280 Personeneinträge (lt. BT-Drs. 17/6223). Legale Grundlage der ATD ist das »Gesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz)« vom 22.12.2006.
31 Anm. d. Red.: Die CTG ist ein loser Zusammenschluss der Polizeibehörden und Nachrichtendienste aus den EU-Mitgliedsstaaten. Sie beruht auf einer informellen Vereinbarung dieser Behörden (*Memorandum of understanding*). Die CTG wurde kurz nach den Anschlägen des 11. September 2001 auf Initiative des »Club of

Berne« begründet. Ihre Mitglieder treffen sich regelmäßig, um Kooperationsmöglichkeiten in Bezug auf islamistischen Terrorismus zu besprechen.

32 Anm. d. Red.: Eine Datenbank von Polizei- und Grenzschutzbehörden aus derzeit 16 europäischen Staaten, die als gemeinsames Fahndungssystem genutzt wird. SIS wurde 1985 auf der Grundlage des Schengener Übereinkommens (vom 14. Juni 1985) begründet. Die zentrale Verwaltung von SIS ist in Straßburg angesiedelt. SIS enthält derzeit circa 11 Millionen Einträge, das heißt Informationen über Personen (gesucht, vermisst, verdächtig etc.) und Sachen (Kraftfahrzeuge, Banknoten, gestohlene Dokumente, Schusswaffen). Das System erlaubt die Fahndung und die verdeckte Überwachung. Derzeit wird an einer Weiterentwicklung der Datenbanken gearbeitet (SIS-II), mit der ein Abgleich von Fingerabdruckdaten und DNA-Profilen möglich werden soll.

33 Anm. d. Red.: Eine europäische Datenbank zur Speicherung von Fingerabdrücken. Sie wurde durch EG-Verordnung Nr. 2725/2000 am 11. Dezember 2000 geschaffen und soll die Anwendung des Dublin-II-Übereinkommens (Feststellung der Asylzuständigkeit für Migranten bei ihrer Einreise in die EU) gewährleisten. Dazu werden von allen Asylsuchenden sowie Personen mit illegalem Aufenthaltsstatus Fingerabdrücke erfasst. Die Datenerfassung geschieht unter der Regie der Mitgliedsstaaten, die Verwaltung der Daten erfolgt im *Automated Fingerprint Identification System* (AFIS), für das die EU-Kommission verantwortlich zeichnet.

34 Anm. d. Red.: Ein System der Mitglieder des Schengen-Übereinkommens (s. Anm. 35 zu SIS) zum europaweiten Austausch von Kurzzeit-Visa-Informationen. Das VIS wurde am 11.10.2011 in Betrieb genommen, die zentrale Datenbank befindet sich Straßburg (Frankreich) und enthält zugleich das AFIS (s. Anm. 32 zu Eurodac). Im VIS werden Informationen zu allen Visa-Angelegenheiten (Anträge, Ausstellungen, Ablehnungen, Annullierungen, Widerrufe und Verlängerungen) im Schengen-Raum gespeichert. Das VIS soll eine schnelle Identitätsfeststellung an den europäischen Grenzen ermöglichen und Mehrfachanträge vermeiden.

35 Informationen aus dem maschinenlesbaren Bereich von Pässen bei Flügen in die EU.

36 Die Datenbanken CIS und FIDE sind der Neapel-II-Konvention zur Kooperation der Zollbehörden zuzuordnen.

37 Anm. d. Red.: Der »Vertrag über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration« (Prümer Vertrag) ist ein zwischenstaatliches Abkommen, das am 27.5.2005 im rheinland-pfälzischen Prüm abgeschlossen wurde. Die zehn Unterzeichnerstaaten vereinbarten darin Regeln für den grenzüberschreitenden Datenaustausch (DNA- und Fingerabdruck-Spurendateien, Kfz-Halterdaten) sowie die polizeiliche Zusammenarbeit. Das Abkommen wurde mittlerweile – auf Initiative der europäischen Innen- und Justizminister – weitgehend in den europäischen Rechtsrahmen überführt, wodurch alle EU-Mitgliedsstaaten an dem Datenaustausch teilnehmen.

38 Anm. d. Red.: Kritisch dazu: 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Mehr Augenmaß bei der Novellierung des BKA-Gesetzes. Entschließung vom 3./4.4. 2008, im Internet unter http://www.datenschutz-bayern.de (-> Konferenzen).

Jörg Ziercke

Kriminalität im 21. Jahrhundert

In rechtlich verlässlichen Strukturen frei und sicher leben zu können, ist eines der wichtigsten menschlichen Grundbedürfnisse. Nicht zuletzt angesichts der deutschen Geschichte besteht in der Bundesrepublik Deutschland eine besonders hohe Sensibilität bezüglich der Einschränkung von bürgerlichen Freiheitsrechten. Das bedeutet für die Polizei, die staatliche Macht so unmittelbar und spürbar für die Bürgerinnen und Bürger wie keine andere Institution repräsentiert, dass sie ihr Handeln fortlaufend hinsichtlich der Einhaltung aller rechtsstaatlichen Grundsätze überprüfen muss (siehe auch den Beitrag von Petri in diesem Band, S. 115 ff.). Andererseits muss die Polizei das Versprechen des Staates, die Sicherheit seiner Bürgerinnen und Bürger zu gewährleisten, erfüllen.

1 Polizeiliche Ermittlungen im Informationszeitalter

Die neuen technischen Möglichkeiten, die Straftätern heute zur Verfügung stehen, beeinflussen die Ermittlungspraxis erheblich. So verliert beispielsweise die Sicherstellung schriftlicher Unterlagen bei Hausdurchsuchungen durch Polizei und Staatsanwaltschaft immer mehr an Bedeutung. Es geht heute vor allem darum, Beweise in digitaler Form – also beispielsweise auf Computern, Navigationsgeräten, Mobiltelefonen, Digitalkameras oder MP3-Playern – zu sichern. Außerdem werden Informationen mit Beweiswert häufig im Internet abgelegt.

Täter nutzen moderne Kommunikationsmittel, um ihre Identität zu verschleiern

Um ihre Kommunikationswege zu verschleiern, besuchen die Täter zum Verfassen von E-Mails Internet-Cafés oder nutzen offene →WLAN-Zugänge unbeteiligter Dritter. → *Voice-over-IP* und verschlüsselte Telefonate über internationale Anbieter werden zum Beispiel viel häufiger genutzt als herkömmliche Festnetzanschlüsse, so dass die Möglichkeiten der Telekommunikationsüberwachung erheblich eingeschränkt werden. Nutzen die Täter E-Mail-Accounts, deren Daten auf ausländischen Ser-

vern abgelegt sind, müssen die Strafverfolgungsbehörden den langwierigen Weg der internationalen Rechtshilfe beschreiten, während der Täter für den Sprung über die Grenze nur einen Mausklick benötigt. Hier stößt das Strafrecht an seine funktionalen und territorialen Grenzen.

Bekämpfung des internationalen Terrorismus

Die größte Herausforderung für die deutschen Sicherheitsbehörden stellt nach wie vor die Bekämpfung des islamistischen Terrorismus dar. Die Akteure des gewalttätigen internationalen *Dschihad*[1] bedrohen unmittelbar auch deutsche Interessen. Wie real diese Gefahr ist, hat das Attentat auf US-Soldaten im März 2011 am Frankfurter Flughafen gezeigt.

Heute bedienen sich Terroristen aller technischen Errungenschaften der modernen Informations- und Kommunikationsgesellschaft. Über das Internet werden Bombenbauanleitungen verbreitet und Anschlagspläne geschmiedet, junge Menschen radikalisiert oder als Suizidattentäter angeworben. Es ist Fern-Universität des Terrorismus und virtuelles Trainingscamp zugleich. Außerdem öffnen sich terroristische Gruppierungen auf diese Weise gegenüber ihrem sympathisierenden Umfeld: Kampfeswillige müssen nicht mehr nach Afghanistan kommen, um sich ausbilden zu lassen – die Ausbildung kommt zu ihnen.

Cybercrime

Eine ebenfalls sehr ernst zu nehmende Gefahr geht vom sogenannten *Cybercrime* im engeren Sinne aus. Davon umfasst werden Phänomene, bei denen Elemente der elektronischen Datenverarbeitung wesentlich für die Tatausführung sind. Dabei geht es unter anderem um Computerbetrug (beispielsweise → *Phishing* im Bereich *Online*banking), Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten, Datenfälschung, Täuschung im Rechtsverkehr bei der Datenverarbeitung und das Ausspähen beziehungs-

weise Abfangen von Daten. Die Zahl der hierunter in der Polizeilichen Kriminalstatistik (PKS)[2] erfassten Straftaten stieg von 2009 zu 2010 in Deutschland um circa 19 Prozent auf 59 839 Fälle.

Im aktuellen Berichtsjahr 2011 lag das Fallaufkommen mit 59 494 Fällen auf dem gleich hohen Niveau wie im Vorjahr. Wie in den Vorjahren stellen die Fälle des Computerbetrugs die mit Abstand größte Fallgruppe mit einem Anteil von 45 Prozent dar. Der im Jahr 2011 registrierte Schaden aller *Cybercrime*-Delikte belief sich auf über 71 Millionen Euro und stieg damit im Vergleich zum Vorjahr um circa 14 Prozent.

2 Ungleichzeitigkeiten von Technik und Recht

Die Aufgaben der Polizei sowie die Rahmenbedingungen, innerhalb derer sie heute agiert, unterliegen einer erheblichen Dynamik. Damit verlieren auch die Instrumente, die der Polizei vor Jahren zur Bekämpfung der damals aktuellen Kriminalitätsphänomene an die Hand gegeben wurden, nach und nach an Wirkung. Es ist daher eine Ungleichzeitigkeit von Technik und Recht entstanden, die es zu überwinden gilt: Wir müssen den technologischen Vorsprung der Täter aufholen. Um auf die dynamische Veränderung der *Modi Operandi* reagieren zu können, braucht die Polizei im Hinblick auf die Bandbreite der ihr zur Verfügung stehenden Eingriffsmaßnahmen Wahlmöglichkeiten. Zusätzlich muss sie auf zweckgeeignete Maßnahmen zurückgreifen können, die mit Blick auf die jeweils aktuelle Gefahrenlage auch angemessen und zielgerichtet sind.

3 Spannungsverhältnis zwischen Freiheit und Sicherheit

Das Bundesverfassungsgericht hat sich in zahlreichen Entscheidungen mit dem Spannungsverhältnis zwischen Freiheit und Sicherheit auseinandergesetzt und bereits in seiner Entscheidung vom 16. Oktober 1977 zur Entführung von Hanns-Martin Schleyer[3] festgestellt, dass das Grundgesetz eine Schutzpflicht nicht nur gegenüber dem Einzelnen begründet, sondern auch gegenüber der Gesamtheit aller Bürger und Bürgerinnen. In dem Urteil heißt es: »Die Schutzpflicht ist umfassend. Sie gebietet dem Staat, sich schützend und fördernd vor dieses Leben zu stellen; das heißt vor allem, es auch vor rechtswidrigen Eingriffen von Seiten anderer zu bewahren. An diesem Gebot haben sich alle staatlichen Organe, je nach ihren besonderen Aufgaben, auszurichten. Da das menschliche Leben

einen Höchstwert darstellt, muss diese Schutzverpflichtung besonders ernst genommen werden.«[4]

Eine wirksame Wahrnehmung dieser Schutzpflicht setzt voraus, dass die zuständigen staatlichen Organe in der Lage sind, auf die jeweiligen Umstände des Einzelfalles angemessen zu reagieren. So heißt es in dem Urteil weiter: »Die Eigenart des Schutzes gegen lebensbedrohliche terroristische Erpressungen ist dadurch gekennzeichnet, dass die gebotenen Maßnahmen der Vielfalt singulärer Lagen angepasst sein müssen.«[5] Danach müssen gesetzliche Regelungen für die Sicherheitsbehörden auch handhabbar sein.

Insgesamt gilt: Die Herrschaft des Rechts ist eine notwendige Bedingung für nachhaltige Freiheit. In einem Rechtsstaat sind Freiheit und Sicherheit untrennbar miteinander verbunden und bedingen sich wechselseitig. Nur wer sich sicher fühlt, kann seine Freiheit ausleben. Freiheit und Sicherheit müssen immer wieder ausbalanciert werden, wobei fest steht, dass die Aufgabe, Menschen vor Gefahren zu schützen, im Einzelfall auch Eingriffe in Freiheitsrechte – und damit auch in das Recht auf Privatsphäre – erforderlich macht.

So genießen sowohl Sicherheit als auch das Recht auf informationelle Selbstbestimmung verfassungsrechtlichen Rang und haben dementsprechend eine hohe Bedeutung. Der Staat ist aufgefordert, eine größtmögliche Vereinbarkeit dieser beiden Rechtsgüter herbeizuführen und dabei mit Augenmaß vorzugehen. Wo Datenschutz und das Erfordernis der Bekämpfung schwerster Kriminalität und der Abwehr terroristischer Gefahren kollidieren, ist eine sorgfältige Abwägung erforderlich.

Über- und Untermaß staatlichen Handelns

Ein Übermaß staatlicher Befugnisse und Eingriffe würde grundrechtliche Freiheiten auf bloße Lippenbekenntnisse reduzieren. Eine allumfassende Überwachung des Einzelnen brächte, sofern sie überhaupt praktisch möglich wäre, unsere Freiheitsordnung und damit unseren demokratischen Rechtsstaat zum Erliegen.

Demgegenüber könnte ein Untermaß staatlicher Befugnisse einen Zustand des Faustrechts und der Selbstjustiz herausfordern und würde das geordnete Zusammenleben der Menschen in Freiheit gefährden. Auch das Recht auf informationelle Selbstbestimmung wäre damit ad absurdum geführt. Bürgerinnen und Bürger müssen sich im Rechtsstaat auf effektiven Schutz durch den Staat ebenso verlassen können, wie auf den Schutz vor dem Staat.

Die Gewährleistung von Freiheit, hier also des Rechts auf informationelle Selbstbestimmung, ist immer eine Risikoabwägung durch den demokratisch legitimierten Gesetzgeber. Wir brauchen einen offenen Dialog über diese Risiken und die Instrumente, über die der Staat verfügen muss, um seine Bürgerinnen und Bürger wirksam und zugleich angemessen vor Kriminalität zu schützen.

4 Wichtige Instrumente effektiver Gefahrenabwehr

Online-Durchsuchung

Bei der *Online*-Durchsuchung wird der Rechner eines Tatverdächtigen ohne sein Wissen und ohne, dass die Ermittler am Standort des Rechners anwesend sind, auf verfahrensrelevante Daten mit spezieller Software durchsucht. Sie ist nur unter eng umrissenen Voraussetzungen mit dem Grundgesetz vereinbar. Das Bundesverfassungsgericht hat in seinem Urteil vom 27. Februar 2008[6] festgestellt, dass die *Online*-Durchsuchung kein Standardverfahren sein kann, sondern als ultima ratio – also letztes Mittel – ausschließlich der Abwehr von Gefahren des internationalen Terrorismus dient (zur *Online*-Durchsuchung siehe den Beitrag von Petri in diesem Band, S. 115 ff.). Es geht also um den Schutz hochrangiger Rechtsgüter wie Leib, Leben und Freiheit der Person oder solcher Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berühren. Keinesfalls soll im Wege der *Online*-Durchsuchung flächendeckend und willkürlich auf die Rechner unbescholtener Personen zugegriffen und deren verfassungsrechtlich verankertes Grundrecht aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG und damit deren Recht auf Privatsphäre verletzt werden.

Die *Online*-Durchsuchung versetzt die Polizeibehörden in die Lage, zur Gefahrenabwehr im Einzelfall unter engen Voraussetzungen adäquat auf das veränderte Kommunikations-, Interaktions- und Datenspeicherungsverhalten von Terrorismusverdächtigen – und nur von solchen – zu reagieren.

Mindestspeicherfristen

Bei der Strafverfolgung und Gefahrenabwehr spielt heute auch der Zugriff auf Daten über die Nutzung elektronischer Telekommunikationsmittel eine bedeutende Rolle. Diese Verkehrsdaten stehen den Poli-

zei- und Strafverfolgungsbehörden jedoch aufgrund einer Entscheidung des Bundesverfassungsgerichts vom 2. März 2010[7] weit überwiegend nicht mehr zur Verfügung. Dabei wurden die bisherigen Regelungen zur sogenannten →Vorratsdatenspeicherung für nichtig erklärt und festgestellt, dass für eine verfassungskonforme Ausgestaltung von gesetzlich festgelegten Mindestspeicherfristen für Verkehrsdaten Regelungen zur Datensicherheit, zur Begrenzung der Datenverwendung, zur Transparenz und zum Rechtsschutz erforderlich seien.

Zugleich machte das Bundesverfassungsgericht deutlich, dass eine Rekonstruktion von Telekommunikationsverbindungen für eine effektive Strafverfolgung und Gefahrenabwehr von besonderer Bedeutung sei und dass daher eine Regelung zur Speicherung von Verkehrsdaten nicht grundsätzlich verfassungswidrig sei. Darüber hinaus stellte das Bundesverfassungsgericht fest, dass die Vorratsdatenspeicherung unter bestimmten Voraussetzungen mit Artikel 10 GG (Brief-, Post- und Fernmeldegeheimnis) vereinbar sei.

Die Auskunft zu polizeilich bereits bekannten →IP-Adressen – oft der schnellste und sicherste, bei manchen Delikten der einzige Weg, Straftäter im Internet zu identifizieren – stellt laut Bundesverfassungsgericht keinen Eingriff in Artikel 10 GG dar, sondern lediglich eine Art Anschlussinhaberfeststellung. Ein Eingriff in Artikel 10 GG sei erst dann gegeben, wenn die Polizei rückwirkend Telekommunikationsverkehrsdaten eines Anschlusses erhebe. Sofern ein Verkehrsdatum der Polizei bereits vorläge und dieses noch einem Anschluss zugeordnet werden solle, läge lediglich ein Eingriff in das allgemeine Persönlichkeitsrecht vor. Danach bemisst sich die Eingriffsgrundlage[8]: Liegt ein Anfangsverdacht oder eine konkrete Gefahr vor, sind Auskunftsersuchen also auf Basis der geltenden Rechtslage generell zulässig, wie bei der Auskunft zu einer Telefonnummer oder einem Kfz-Kennzeichen. Der Internet-Anbieter kann die Auskunft zum Nutzenden einer IP-Adresse aber nur erteilen, indem er intern auf Verkehrsdaten zurückgreift, um das Datum exakt zuzuordnen. Da diese nun in der Regel nicht mehr gespeichert werden, ist eine Auskunft nur noch selten möglich.

Das sogenannte *Quick-Freeze*-Verfahren stellt keine adäquate Lösung dar. Es sieht vor, anstatt der Speicherung aller Verkehrsdaten nur auf Antrag Daten »einzufrieren«, die den Sicherheitsbehörden anlassbezogen übermittelt werden sollen. Speichern Telekommunikationsanbieter aber keine Verkehrsdaten, können auch keine Daten »eingefroren« werden. Insbesondere bei zeitintensiven und umfangreichen Ermittlungen wird dies offensichtlich. Das hat das Bundesverfassungsgericht übrigens in der erwähnten Entscheidung ebenfalls festgestellt.

Wie macht sich die seit März 2010 bestehende Sicherheits- und Schutzlücke konkret bemerkbar? Dazu drei Beispiele:

- Ohne Speicherung von Verkehrsdaten ist das Internet weitgehend ein strafverfolgungsfreier Raum, da ohne die Verifizierung der →IP-Adresse ein ganz zentraler Ermittlungsansatz fehlt.
- Werden im Internet, beispielsweise in einem Chat, Tatankündigungen von Amokläufen oder Sprengstoffanschlägen, Suizidäußerungen, terroristische Videoverlautbarungen, Angebote von Kinderpornografie veröffentlicht oder offene Diskussionen über Kindesmissbrauch geführt, kann die Polizei lediglich über den Internet-Anbieter des Chats die IP-Adresse der Nutzenden in Erfahrung bringen, da User anonymisiert, nur gekennzeichnet durch ihren frei wählbaren *Nickname*[9] oder unter einer gestohlenen Identität erscheinen. Polizeiliche Gefahrenabwehr geht hier mangels Datengrundlage ins Leere.
- Auch die zunehmende Gefahr, die von sogenannten →Botnet-Attacken ausgeht, kann auf der derzeitigen rechtlichen Grundlage nicht gebannt werden. So wurden in einem Verfahren der Behörden in Luxemburg über 200 000 deutsche IP-Adressen bekannt, die mit einem internationalen kriminellen Botnet verbunden sind. Es besteht aus mit Schadsoftware infizierten Rechnern, deren Inhaber nichts davon ahnen, dass ihr Rechner auf einen sogenannten *Command and Control-Server*[10] zugreift und zur fortgesetzten Begehung von Straftaten eingesetzt wird. Die überwiegende Anzahl der Geschädigten konnte mangels vorhandener Verkehrsdaten, die aus der Vergangenheit stammten, nicht ermittelt und gewarnt werden. Von ihren Computern geht somit weiter eine Gefahr aus.

5 Das Internet darf kein strafverfolgungsfreier Raum sein

Die Menschen in der Bundesrepublik Deutschland haben einen Anspruch auf wirksame Gefahrenabwehr und Strafverfolgung. Der Schutzauftrag der Polizei würde zu einer leeren Floskel verkommen, wenn der Staat die Augen vor den neuartigen Erscheinungsformen der Kriminalität verschließen würde. In diesem Sinne sind sicherheitspolitische Instrumentarien also immer vor dem Hintergrund gesamtgesellschaftlicher und technologischer Rahmenbedingungen zu reflektieren. Nur wer mit der Zeit geht und voll handlungsfähig ist, kann wirksam schützen. So darf das Internet nicht zu einem verfolgungsfreien Raum werden.

Möglichst umfangreiche Datenmengen zu sammeln und zu speichern, hilft nicht weiter. Im Gegenteil: Das BKA ist ebenso wie alle deutschen

Polizeien daran interessiert, das Datenvolumen, mit dem gearbeitet wird, nach Möglichkeit zu reduzieren.

Anders als in der öffentlichen Diskussion gelegentlich behauptet wird, speichert das BKA auch keine (Nutzer-)Profile. Verfügbar müssen nur jene Daten sein, die für die Erfüllung der polizeilichen Aufgaben unbedingt erforderlich sind.

Auch im digitalen Zeitalter muss die Polizei dem Anspruch gerecht werden, Kriminalität in der realen Welt ebenso wie im virtuellen Raum konsequent und mit der nötigen Sensibilität im Umgang mit den ihr vom Gesetzgeber anvertrauten Eingriffsinstrumentarien zu bekämpfen.

Anmerkungen

1 »*Dschihad*« oder »*Jihad*« bedeutet wörtlich die »Anstrengung auf dem Wege Gottes«. Oft wird der Begriff als »Heiliger Krieg« übersetzt. In diesem Zusammenhang steht er auch für islamistischen Terrorismus.
2 Abrufbar unter: http://www.bka.de/nn_229440/DE/Publikationen/PolizeilicheKriminalstatistik/pks__node.html?__nnn=true.
3 BVerfGE 46, 160; Az. 1 BvQ 5/77.
4 Ebd. (S. 165).
5 Ebd. (S. 165).
6 BVerfGE 120, 274; Az. 1 BvR 370, 595/07.
7 BVerfGE 125, 260; Az. 1 BvR 263/08, 1 BvR 586/08.
8 Die gesetzliche Bestimmung, wonach der Eingriff erfolgen darf.
9 Spitzname, der zum Beispiel in Foren oder Kommunikationsdiensten genutzt wird.
10 Unter einem *Command and Control-Server* (auch Botnetz-Operator, Bot-Master und Bot-Herder) versteht man einen Rechner, der den Bots (Computerprogramme, die weitgehend selbstständig sich wiederholende Aufgaben abarbeiten) auf infizierten Rechnern eines Botnetzwerks Befehle und Anweisungen senden und sie überwachen kann. Der *Command and Control-Server* kann also beispielsweise 5000 infizierten Rechnern den Befehl geben, immer wieder eine bestimmte Website aufzurufen, um den entsprechenden Webserver zum Erliegen zu bringen. Weitere Informationen im Internet unter http://blj.zbw.ch/wiki/index.php5/Command_%26_Control_Server.

Bettina Sokol

Grundrechte sichern!

Unsere Grundrechte geben uns Freiheiten. Freiheits- und Gleichheitsrechte sind das Fundament einer Demokratie und deshalb keine »kleine Münze«, sondern ein hohes Gut. Mit der Verankerung der Grundrechte im Grundgesetz sollten 1949 Lehren aus der Zeit des menschenverachtenden Nationalsozialismus gezogen werden. Aber fast von Anfang an standen die Grundrechte auch in der Gefahr, eingeschränkt zu werden. Als historische Stichworte, ohne Anspruch auf Vollständigkeit, mögen hier genügen: die Auseinandersetzungen um die sogenannte Notstandsgesetzgebung in den 1960er Jahren des letzten Jahrhunderts, die aus Anlass des RAF-Terrorismus in der zweiten Hälfte der 1970er Jahre stattgefundenen Gesetzesverschärfungen, die weiteren »Gesetzgebungswellen« Mitte der 1980er, Anfang der 1990er sowie Mitte der 1990er Jahre. Sie alle erweiterten unter der Fahne der »Bekämpfung von Terrorismus und organisierter Kriminalität« staatliche Befugnisse auf Kosten der Grundrechte.

Gleichwohl ist die mit dem →Großen Lauschangriff seit Ende der 1990er Jahre eingeleitete Entwicklung beispiellos. Es folgten im Anschluss an die Anschläge vom 11. September 2001 die unter der Bezeichnung »Otto-Kataloge«[1] streitig diskutierten sogenannten Sicherheitspakete, die eine Fülle zusätzlicher staatlicher Überwachungs- und Kontrollmöglichkeiten schufen. Seitdem ebbt im Bund und in den Ländern diese Flut nicht ab. Nicht gegeben hat es allerdings bisher eine seriösen wissenschaftlichen Ansprüchen genügende Untersuchung, ob die vielen neu geschaffenen Befugnisse – außer zu der mit ihnen verbundenen Erosion der Grundrechte – tatsächlich auch zu dem behaupteten Gewinn an Sicherheit geführt haben.

Maßgeblich zum Abbau der Grundrechte beigetragen haben allerdings zwei Umstände:

- Erstens die rasanten Fortschritte der technischen Möglichkeiten von Überwachung und Kontrolle sowie
- zweitens ein in der Öffentlichkeit zu wenig beachteter tendenzieller Wandel im Staatsverständnis vom Rechtsstaat zum Präventionsstaat (siehe auch den Beitrag von Albers in diesem Band, S. 102 ff.).

1 Datenspuren im digitalen Zeitalter

Die heutigen technischen Möglichkeiten der elektronischen Datenverarbeitung sind enorm. Die Menschen hinterlassen nicht nur im Internet durch gleichsam jeden Tastendruck und jeden Mausklick Spuren, die nicht verwehen, sondern auch im realen Leben, etwa beim Einsatz jeder der vielen personalisierten Plastikkärtchen, beim Benutzen des Telefons, beim Aufenthalt im Erfassungsbereich einer der unzähligen Videoüberwachungskameras oder bei der Verwendung biometrischer Verfahren. Mittels biometrischer Verfahren werden Menschen ge- oder vermessen, um sie anhand bestimmter, in ihrer individuellen Ausprägung als einzigartig geltender körperlicher Merkmale eindeutig zuordnen zu können. Ein klassisches Beispiel dafür sind unsere Fingerabdrücke, die mittlerweile ebenso wie digitalisierte Passbilder in die Reisepässe aufgenommen werden. Biometrische Verfahren werden jedoch immer vielfältiger und ausgereifter. Es gibt inzwischen höchst unterschiedliche Identifizierungs- und Authentisierungsverfahren, die die Merkmale von Gesichtern, Ohren oder Händen betreffen, aber auch Verfahren, die auf der Erkennung von Venenbildern oder von Gangarten basieren.

Diese digitalen Spuren werden häufig hinterlassen, ohne dass die betroffenen Personen sich dessen tatsächlich bewusst sind. Die Datenerfassung durch private oder öffentliche Stellen ist möglich, ohne dass die Betroffenen hiervon etwas bemerken. Die Informationstechnologie ist derart weit fortgeschritten, dass diese Spuren alle gesammelt, ausgewertet und neu miteinander verknüpft werden könnten. Aus Kombinationen und mit Hilfe weiterer Datenverarbeitungsprogramme lassen sich sogar neue Informationen gewinnen. Die schiere Menge der vorhandenen Daten sowie das Tempo und die vielfältigen Arten ihrer Verarbeitung stellen ebenso eine neue Qualität der Informationsgewinnung dar wie die Vernetzbarkeit und die drahtlose Übermittlungsmöglichkeit.

RFID-Technologie

Eine nicht unwichtige Rolle bei dieser Entwicklung dürfte künftig wohl die Radiofunktechnik einnehmen, denn die Miniaturisierung der Prozessoren lädt geradezu dazu ein, die zumeist noch eher schlicht ausgestatteten Funkchips (→RFID-*Tags*) erheblich leistungsfähiger zu gestalten. Mit RFID-*Tags* werden bislang überwiegend Gegenstände mit einer weltweit einzigartigen Kennung versehen. Das ermöglicht ihre eindeutige Identifizierung. Vorhergesagt wird uns – und die Zukunft hat schon begonnen –

die eigenständige Kommunikation von Gegenständen und die Allgegenwart von Computeranwendungen (→ *Ubiquitous Computing*), also eine Welt der totalen Datenverarbeitung. Solche technischen Möglichkeiten wecken natürlich Begehrlichkeiten bei öffentlichen wie privaten Stellen. Wenn alles das, was technisch möglich ist, auch erlaubt wäre, bliebe vom Grundrecht auf informationelle Selbstbestimmung so gut wie nichts mehr übrig. Zur Illusion würde das verfassungsrechtliche Gebot werden, dass jede Person wissen können soll, wer, was, wann und bei welcher Gelegenheit über sie weiß, wie es im Volkszählungsurteil des Bundesverfassungsgerichts heißt (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.).

2 Rechtsstaat statt Präventionsstaat

Einen Rechtsstaat kennzeichnen unter anderem folgende Elemente: Der Rechtsstaat respektiert die individuellen Freiheiten der Menschen. Wird in einem Rechtsstaat in individuelle Grundrechte eingegriffen, geschieht dies auf der Basis eines die →Verhältnismäßigkeit wahrenden Gesetzes und grundsätzlich nur dann, wenn die davon im Einzelfall betroffene Person zuvor einen Anlass dafür gegeben hat. Die innere Logik des Rechtsstaates besteht in der Begrenzung staatlicher Macht. Demgegenüber betrachtet der Präventionsstaat, also der Staat der vorbeugenden Gefahrenabwehr, alle Menschen grundsätzlich als Risikofaktoren (siehe auch den Beitrag von Albers in diesem Band, S. 102 ff.). Nach seiner Strategie bedarf es möglichst vieler vorsorglicher Kontrollen und flächendeckender Überwachungsmaßnahmen. Für individuelle Grundrechtseingriffe wird folglich kein Anlass mehr benötigt. Vollständige Sicherheit ist zwar nicht erreichbar, aber die innere Logik des Präventionsstaates ist geprägt vom Streben nach mehr und mehr Sicherheit. Damit geht zwangsläufig die Tendenz zur Maßlosigkeit bei Freiheitsbeschränkungen einher.

3 Gesetzgebung auf dem Prüfstand des Bundesverfassungsgerichts

Einige der vielen gesetzgeberischen Aktivitäten aus Bund und Ländern wurden zur Überprüfung ihrer Verfassungsmäßigkeit vor das Bundesverfassungsgericht gebracht. Kaum eines der jüngeren Gesetze oder eine der angegriffenen Maßnahmen hielt jedoch der verfassungsrechtlichen Überprüfung in vollem Umfang Stand. Hier eine Auswahl:

Rasterfahndung

Schon die Anordnung der Rasterfahndung nach den Terroranschlägen vom 11. September 2001 entsprach nicht den verfassungsrechtlichen Anforderungen[2] (siehe auch den Beitrag von Petri in diesem Band, S. 115 ff.). Da die Rasterfahndung verdachtslose Grundrechtseingriffe mit einer großen Streubreite bewirkt und für die Betroffenen ein erhöhtes Risiko begründet, Ziel weiterer behördlicher Ermittlungen zu werden, müssen für die Zulässigkeit dieser Maßnahme die bedrohten Rechtsgüter hochrangig und einer konkreten Gefahr ausgesetzt sein. Eine allgemeine Bedrohungslage genügt dafür nicht.

Lauschangriff

Aus der Garantie der Menschenwürde hat das Gericht in seiner Entscheidung über den → Großen Lauschangriff für die Wohnung den Schutz eines unantastbaren Kernbereichs privater Lebensgestaltung abgeleitet, der einem staatlichen Zugriff absolut entzogen bleiben muss.[3] Abgestuft ist ein solcher Kernbereich privater Lebensgestaltung ebenfalls für den Bereich des Telekommunikationsgeheimnisses anerkannt.

Präventive Telefonüberwachung

Nicht verfassungsgemäß waren auch die Befugnisse zur präventiven Telekommunikationsüberwachung im niedersächsischen Polizeigesetz.[4] Zu unbestimmt und unverhältnismäßig waren die gesetzlichen Regelungen. Zudem fehlte es an Normen, die Eingriffe in den absolut geschützten, unantastbaren Kernbereich privater Lebensgestaltung ausschlossen.

Online-Durchsuchung

Mit eben diesen verfassungswidrigen Mängeln war auch das nordrhein-westfälische Verfassungsschutzgesetz behaftet, das die sogenannte *Online*-Durchsuchung erlauben wollte, also den heimlichen Zugriff auf informationstechnische Systeme (siehe auch den Beitrag von Petri in diesem Band, S. 115 ff.). Die heimliche Infiltration beispielsweise von Computern, um ihre Nutzung überwachen und die Speichermedien auslesen zu können, bedarf nach den verfassungsrechtlichen Anforderungen mindestens tatsächlicher Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut sowie grundsätzlich der richterlichen Anordnung.[5] Das Bundesverfassungsgericht hat in dieser Entscheidung aus dem allgemeinen Persönlichkeitsrecht zudem eine weitere Ausprägung abgeleitet, nämlich das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme – sozusagen eine »kleine Schwester« des Grundrechts auf informationelle Selbstbestimmung (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.).

Videoüberwachung

Nicht im Zusammenhang mit der Bekämpfung von Terrorismus oder organisierter Kriminalität, sondern wegen einer städtischen Maßnahme im öffentlichen Raum hatte sich das Bundesverfassungsgericht mit der Videoüberwachung öffentlicher Plätze zu befassen (siehe auch den Beitrag von Petri in diesem Band, S. 115 ff.). Die Videoüberwachung wird vom Gericht ausdrücklich als ein Grundrechtseingriff von erheblichem Gewicht qualifiziert.[6] Von Bedeutung ist dabei, dass flächendeckend Personen erfasst werden, die selbst keinen Anlass für Überwachungsmaßnahmen gegeben haben. Aus verfassungsrechtlichen Gründen erforderlich ist danach zumindest eine normenklare, dem → Verhältnismäßigkeitsgrundsatz entsprechende gesetzliche Grundlage für die Videoüberwachung.

Automatisierte Kennzeichenerfassung

Nicht ganz identisch, aber ähnlich wird in der Entscheidung zur automatisierten Erfassung von Kraftfahrzeugkennzeichen argumentiert.[7] Verfassungsrechtlich noch hinnehmbar kann die Erfassung sein, wenn sie sich nicht zur anlasslosen, flächendeckenden Totalkontrolle auswächst, sie keine »Einschüchterungseffekte« bewirkt und weitere Vorgaben wie beispielsweise die Zweckbindung der gewonnenen Daten, die hinreichende Bestimmtheit der Normen[8] und ihre Verhältnismäßigkeit eingehalten werden.

Vorratsdatenspeicherung

Nach wie vor politisch umstritten ist die →Vorratsdatenspeicherung. Schon im Volkszählungsurteil hatte das Bundesverfassungsgericht ausdrücklich festgestellt, dass das Sammeln nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmten Zwecken mit dem Gebot der notwendigen gesetzlichen Festlegung des Verwendungszweckes nicht vereinbar ist (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.). An dieser, im Laufe der Jahre vielfach bestätigten Rechtsprechung hält das Gericht auch in seinem Urteil zur Vorratsdatenspeicherung[9] ausdrücklich fest. Es verwirft die konkrete gesetzliche Ausgestaltung dieser Maßnahme als verfassungswidrig, sieht aber zugleich derartige Vorhaben als nicht schlechthin unvereinbar mit dem Grundgesetz an. Die Maßstäbe, die nach der Entscheidung insbesondere im Hinblick auf die Verhältnismäßigkeit im Detail für eine verfassungskonforme Regelung formuliert werden, sind allerdings außerordentlich strikt. Beispielsweise käme eine unmittelbare Verwendung der Daten danach nur für überragend wichtige Aufgaben des Rechtsgüterschutzes in Betracht. Es ist zudem nicht auszuschließen, dass die Vorratsdatenspeicherung – so wie mittlerweile nachweislich die Videoüberwachung – von ihren Befürwortern in ihrem Nutzen überschätzt wird. Wenn die Medienberichte zutreffen, nach denen in der Zeit, in der die Vorratsdatenspeicherung in Deutschland praktiziert wurde, die Aufklärungsrate von Straftaten im Internet prozentual zurückgegangen ist, sollte dies zumindest nachdenklich stimmen.

4 Grundlinien der verfassungsgerichtlichen Rechtsprechung

Aus den oben genannten Beispielen, aber auch aus der sonstigen langen Tradition der Rechtsprechung des Bundesverfassungsgerichts lassen sich Grundlinien zur Bewertung von Grundrechtseingriffen erkennen. Das Gericht bezieht für die Beurteilung der Intensität oder des Gewichts eines Grundrechtseingriffs möglichst sämtliche Lebensumstände mit ein. Verdeutlichen lässt sich dies anhand eines Zitats aus der Pressemitteilung des Gerichts zur Vorratsdatenspeicherung[10], das wie folgt lautet:

»Allerdings handelt es sich bei einer solchen Speicherung um einen besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt. Auch wenn sich die Speicherung nicht auf die Kommunikationsinhalte erstreckt, lassen sich aus diesen Daten bis in die Intimsphäre

hineinreichende inhaltliche Rückschlüsse ziehen. Adressaten, Daten, Uhrzeit und Ort von Telefongesprächen erlauben, wenn sie über einen längeren Zeitraum beobachtet werden, in ihrer Kombination detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönlichen Vorlieben, Neigungen und Schwächen. Je nach Nutzung der Telekommunikation kann eine solche Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers ermöglichen. Auch steigt das Risiko von Bürgern, weiteren Ermittlungen ausgesetzt zu werden, ohne selbst hierzu Anlass gegeben zu haben. Darüber hinaus verschärfen die Missbrauchsmöglichkeiten, die mit einer solchen Datensammlung verbunden sind, deren belastende Wirkung. Zumal die Speicherung und Datenverwendung nicht bemerkt werden, ist die anlasslose Speicherung von Telekommunikationsverkehrsdaten geeignet, ein diffus bedrohliches Gefühl des Beobachtetseins hervorzurufen, das eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen kann.«

Von Bedeutung sind somit unter anderem die sogenannte Streubreite – also die Größe des von einem Grundrechtseingriff betroffenen Personenkreises, der Inhalt – also die Persönlichkeitsrelevanz der gewonnen Informationen sowie die Art ihrer weiteren Verwendung und Verwertung, insbesondere im Hinblick auf mögliche nachteilige Folgen für die Betroffenen. Wichtig ist ferner, ob die betroffene Person einen Anlass für die staatliche Maßnahme gegeben hat. Anlasslose Grundrechtseingriffe sind grundsätzlich von höherem Gewicht als anlassbezogene. Gleiches gilt für heimliche Eingriffe, die die Gesellschaft insgesamt zudem noch intensiver als offene Eingriffe betreffen. In vielen Entscheidungen der letzten Jahre verweist das Bundesverfassungsgericht auch auf die Gefahr von Einschüchterungseffekten. Dies könnte Verhaltensanpassungen, den Verlust von Unbefangenheit in der Kommunikation und letztlich den Verzicht auf die Ausübung von Grundrechten nach sich ziehen – mit den bekannten negativen Folgen für ein demokratisches Gemeinwesen.

5 Achtsamkeit ist gefragt

Die Rechtsprechung des Bundesverfassungsgerichts und die daraus erkennbaren Grundlinien zeigen, dass die einzelnen Elemente, die eine Gesetzgebung in einem Präventionsstaat kennzeichnen, sich durchaus schon häufiger in Gesetzen fanden, die dem Gericht zur verfassungsrechtlichen Prüfung vorlagen. Zum Glück für uns und unsere Demokratie wacht das Gericht über die Grundrechte und begegnet sowohl anlasslosen Kontroll-

maßnahmen als auch der vorsorglichen flächendeckenden Überwachung mit einer demokratischen und rechtsstaatlichen Grundsätzen entsprechenden kritischen Rechtsprechung.

Unsere Gesellschaft muss achtsam sein und sich vor der Eigendynamik hüten, die sich entwickelt, wenn auf immer neue Terrordrohungen mit immer neuen und immer tiefer greifenden Freiheitseinschränkungen geantwortet würde. Als Folge einer solchen Eigendynamik würde die Demokratie dahinschwinden. Besser als es die frühere Richterin am Bundesverfassungsgericht, Christine Hohmann-Dennhardt, in einem Aufsatz formuliert hat, kann es nicht auf den Punkt gebracht werden: »Gleiche Augenhöhe mit dem Terrorismus darf nicht bedeuten, sich wie dieser über Grundrechte und Rechtsstaatlichkeit hinwegzusetzen.« [11]

Anmerkungen

1 Anm. d. Red.: Der Begriff verweist auf den Vornamen des damaligen Bundesministers des Innern, Otto Schily.
2 BVerfGE 115, 320; Az. 1 BvR 518/02.
3 BVerfGE 109, 279; Az. 1 BvR 2378/98, 1 BvR 1084/99.
4 BVerfGE 113, 348; Az. 1 BvR 668/04.
5 BVerfGE 120, 274; Az. 1 BvR 370/07, 1 BvR 595/07.
6 BVerfGK 10, 330; Az. 1 BvR 2368/06.
7 BVerfGE 120, 378, Az. 1 BvR 2074/05, 1 BvR 1254/07.
8 Der Grundsatz der Bestimmtheit besagt, dass Gesetze inhaltlich hinreichend bestimmt sein müssen. Die Bürgerinnen und Bürger sollen anhand des Gesetzestextes erkennen können, welche staatlichen Maßnahmen erlaubt sind. Der Bestimmtheitsgrundsatz ergibt sich aus dem Rechtsstaatsprinzip.
9 BVerfGE 125, 260; Az. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08.
10 Bundesverfassungsgericht, »Konkrete Ausgestaltung der Vorratsdatenspeicherung nicht verfassungsgemäß«. Pressemitteilung Nr. 11/2010 vom 2.3.2010, im Internet unter http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.html.
11 Christine Hohmann-Dennhardt, Informationeller Selbstschutz als Bestandteil des Persönlichkeitsrechts, in: Recht der Datenverarbeitung (RDV) 2008, S. 1 ff.

Sven Polenz

Informationstechnik und Datenschutz in der Finanzverwaltung

Als das italienische Finanzministerium 2008 auf einer Internetseite die drei Jahre alten Steuererklärungen von circa 38 Millionen Personen veröffentlichte, recherchierten mindestens ebenso viele Menschen auf der angegebenen Internetseite nach den Einkommensverhältnissen ihrer Bekannten, von Politikern und Politikerinnen oder sonstigen in der Öffentlichkeit stehenden Persönlichkeiten. Alle Internetnutzenden hatten die Gelegenheit, auf sensible Informationen frei zuzugreifen, wobei das Auffinden der gesuchten Steuererklärung zu einer bestimmten Person durch die Bereitstellung einer alphabetisch geordneten Liste erleichtert wurde, die Angaben zu den Familiennamen, Geburtsdaten und Anschriften enthielt. Der damalige Finanzminister Vincenzo Vesci begründete die Veröffentlichung der Daten mit dem Ziel, mehr »Demokratie und Transparenz« zu schaffen.[1] Zahlreiche Bürgerinnen und Bürger waren über die Preisgabe ihrer Steuerdaten jedoch verärgert und fühlten sich in ihrer Privatsphäre verletzt, was schließlich zu einer öffentlichen Debatte über Entschädigungsregelungen (520 Euro pro Person) führte.

1 Das Steuergeheimnis

Das Steuergeheimnis schützt alle Informationen über die Verhältnisse der Steuerpflichtigen. Alle Angaben, die Steuerpflichtige gegenüber einer Behörde machen, müssen vertraulich behandelt werden. Das Schutzversprechen ist ein Ausgleich für die weitgehenden Offenbarungspflichten der Bürgerinnen und Bürger im Steuerprozess und soll deren Steuerehrlichkeit verbessern. Aber nicht alle Informationen, die vom Steuergeheimnis geschützt werden, fallen unter das Recht auf informationelle Selbstbestimmung. Nur wenn es sich um Daten handelt, die einen Bezug zu einer natürlichen Person haben, greifen datenschutzrechtliche Vorschriften. Oftmals entsteht dieser Personenbezug erst durch die Zusammenführung einer Vielzahl der für eine Besteuerung relevanten Informationen.

2 Ankauf von steuerlich relevanten Daten durch den Staat

Im Jahre 2008 wurde öffentlich bekannt, dass die Finanzbehörden unter Beteiligung des Bundesnachrichtendienstes in den Besitz einer DVD mit Steuerdaten gekommen waren, die eine Privatperson gestohlen hatte. Diese soll von den staatlichen Behörden für die circa 400 Kontounterlagen einer Bank in Liechtenstein vier Millionen Euro erhalten haben, woraufhin gegen 700 Personen wegen des Verdachts der Steuerhinterziehung beim Amtsgericht Bochum 900 Durchsuchungsbeschlüsse erwirkt wurden. Die Finanzbehörden rechneten aufgrund der eingeleiteten Verfahren mit Steuermehreinnahmen von 3,4 Milliarden Euro.[2] In der Folgezeit boten weitere Personen Daten zahlreicher Steuerpflichtiger zum Kauf an.[3] Speziell im Hinblick auf die zum Kauf angebotenen Kontodaten lag auf der Hand, dass diese unter Verletzung des Bankgeheimnisses in den Besitz des Informanten gelangt waren. Dieser kann daher nach dem in Liechtenstein geltenden Datenschutz- und Strafrecht zur Verantwortung gezogen werden. Vergleichbares gilt für den Fall, in dem ein Informant Datenträger in Deutschland unter Verstoß gegen Datenschutzvorschriften an sich nimmt. Selbst wenn der Diebstahl des Datenträgers nicht zweifelsfrei bewiesen werden kann, muss dieser noch mit einem Bußgeld wegen Verstoßes gegen deutsches Datenschutzrecht rechnen, welches bis zu dreihunderttausend Euro betragen kann.

Gerichtliche Verfahren

In Gerichtsverfahren stellt sich oft die Frage, ob Informationen, die unter Verstoß gegen datenschutzrechtliche Vorschriften erlangt wurden, genutzt werden dürfen, um Steuersündige zu überführen. Der Staat sollte Beweise grundsätzlich nur im Rahmen eines ordnungsgemäßen Ermittlungsverfahrens erheben. Handeln die Ermittlungsbeamten außerhalb ihrer Befugnisse, so kann ein sogenanntes Beweisverwertungsverbot entstehen. Eine unter Folter abgenötigte Aussage wäre beispielsweise in einem Gerichtsprozess nicht verwertbar. Eine Verurteilung dürfte nicht auf der im Rahmen der Folter getätigten Aussage basieren.

Beweisverwertungsverbote entstehen aber nicht, wenn die staatlichen Stellen einen Informanten nicht beauftragt haben: Handelt der Informant aus freien Stücken, das heißt stiehlt er einen Datenträger ohne vorherige Beeinflussung durch staatliche Behörden, so dürfen die im Anschluss gekauften Daten in einem Verfahren verwertet werden. Grundsätzlich stehen zwar auch die Daten der Steuersünder unter dem Schirm des

Datenschutzes. Allerdings besteht an der Aufdeckung von Steuerhinterziehungen ein hohes Gemeinwohlinteresse, welches diesen Schutz begrenzt. Es ist schließlich zu berücksichtigen, dass die Daten in die Hände von staatlichen Behörden gelangen, welche auf eine gleichmäßige Besteuerung der Bürgerinnen und Bürger hinwirken wollen. Dieses Handeln steht im Interesse der Bevölkerung, wonach vollständige steuerehrliche Angaben im Rahmen der Steuererklärung zu machen sowie Steuern ordnungsgemäß zu zahlen sind. Vor diesem Hintergrund kann das Verschweigen steuerrelevanter Angaben sowie die Erlangung rechtswidriger Steuervorteile durch Einzelne nicht akzeptiert werden.

3 Die bundeseinheitliche Identifikationsnummer

Die erste behördliche Post, die heute ein Neugeborenes erhält, kommt regelmäßig vom Bundeszentralamt für Steuern. Sie enthält folgenden Hinweis: »Sehr geehrte Dame, sehr geehrter Herr, das Bundeszentralamt für Steuern hat Ihnen die Identifikationsnummer (…) zugeteilt. Sie wird für steuerliche Zwecke verwendet und ist lebenslang gültig. Sie werden daher gebeten, dieses Schreiben aufzubewahren, auch wenn Sie derzeit steuerlich nicht geführt werden sollten.« Die Identifikationsnummer besteht aus elf Ziffern und ändert sich bis zum Lebensende nicht. Sie soll dazu dienen, die Steuerpflichtigen unter erleichterten Bedingungen zu identifizieren und dadurch auch dem Steuerbetrug entgegen zu wirken. Das Bundeszentralamt für Steuern errichtete zudem eine riesige Datenbank mit weiteren Angaben zu allen Bürgerinnen und Bürgern, die neben der Identifikationsnummer gespeichert werden. Hierzu zählen

- Familienname, frühere Namen, Vornamen, Doktorgrad,
- Tag und Ort der Geburt,
- Geschlecht,
- gegenwärtige oder letzte bekannte Anschrift,
- zuständige Finanzbehörden sowie
- Todestag.

Aufgrund von Geburten, Sterbefällen, Umzügen oder Namensänderungen müssen die Daten ständig aktualisiert werden, wobei für die über 80 Millionen Bundesbürgerinnen und Bürger täglich etwa 40 000 Änderungen zu berücksichtigen sind.[4] Zum Abgleich dienen die Daten aus den Melderegistern.

Wer darf die Identifikationsnummer verarbeiten?

Nicht nur die Finanzbehörden dürfen die Identifikationsnummer verarbeiten. Durch Rechtsvorschriften kann der Kreis der Berechtigten erweitert werden. Der Gesetzgeber hat bereits zahlreiche neue Bestimmungen geschaffen und behördlichen Stellen sowie auch Unternehmen Verpflichtungen zur Verarbeitung der Identifikationsnummer auferlegt. Zu den bisher Berechtigten gehören:

- Träger der gesetzlichen Rentenversicherungen,
- Arbeitgeber,
- Bundesagentur für Arbeit,
- Versicherungsunternehmen,
- Kreditinstitute,
- Lebensversicherungsunternehmen,
- Kreditinstitute mit Sitz in einem anderen Staat des europäischen Wirtschaftraums.

Wie der letzte Punkt zeigt, ist der Umgang mit dieser Nummer also nicht auf das Gebiet der Bundesrepublik Deutschland beschränkt. Eröffnet wird vielmehr ein weltweiter Zugang für bestimmte Unternehmen und Institutionen. Die Übersicht zeigt, dass der Kreis der Berechtigten sehr weit gewählt wurde. Weitere Gesetzesänderungen sind geplant, sodass für die Zukunft mit einer umfassenden Verarbeitung der Steueridentifikationsnummer zu rechnen ist.

Gefahr eines Personenkennzeichens

Frühzeitig haben die Datenschutzaufsichtsbehörden darauf hingewiesen, dass sich aus der Identifikationsnummer ein Personenkennzeichen entwickeln kann, über welches andere Datenbestände verknüpft und umfassende Persönlichkeitsprofile erstellt werden können.[5] Eine Alternative zur Einführung der bundeseinheitlichen Identifikationsnummer hätte darin bestanden, die Identifikationsdaten nicht zentral in einer großen Datenbank, sondern dezentral zu verwalten und eine pseudonyme Nutzung zu ermöglichen. Durch → Pseudonymisierung können die Identifikationsdaten durch andere Daten ersetzt werden, um die Identifikation zu erschweren. Dieser Gedanke wurde vom Gesetzgeber nicht aufgegriffen.

Das Recht auf informationelle Selbstbestimmung verbietet eine Datensammlung zu sämtlichen Bereichen der Lebensführung einer Person und damit eine Katalogisierung ihrer gesamten Persönlichkeit. Ein Verstoß

gegen dieses Recht läge dann vor, wenn die zur Verarbeitung der Identifikationsnummer berechtigten Stellen die gespeicherten Daten zusammenführen und die Nummer dabei als allgemeines Personenkennzeichen verwenden würden. Unzulässig ist bereits eine einzige Abfrage weiterer Daten über Personen außerhalb der bestehenden Berechtigung bei einer anderen Stelle unter Angabe der Identifikationsnummer.

4 Ermittlung von Kontodaten

Das Bundeszentralamt für Steuern führt für die Finanzbehörden sowie für bestimmte andere Behörden Kontodatenabrufe für steuerliche und nichtsteuerliche Zwecke durch. Dies kann nur die in der jeweiligen Datei des Kreditinstituts gespeicherten sogenannten Kontostammdaten umfassen, nicht jedoch Angaben zu Kontoständen oder -bewegungen. Vor jedem automatisierten Kontodatenabruf müssen jedoch die Betroffenen direkt zu allen steuer- oder leistungserheblichen Tatsachen befragt werden. Erst wenn die Aufforderung zur Auskunft nicht zum Ziel führt oder keinen Erfolg verspricht, darf der Datenabruf erfolgen.

Abfragen zu Kontoauszügen

Die bloße Ermittlung der Kontostammdaten würde nicht immer ausreichen, um einen steuerlichen Sachverhalt aufzuklären. Die Finanzbehörden können daher andere Personen als die jeweils Steuerpflichtigen auffordern, Konto- oder Depotauszüge vorzulegen. Auch in diesem Fall darf dies erst dann erfolgen, wenn die Direktbefragung gegenüber den betroffenen Steuerpflichtigen nicht zum Ziel führt oder keinen Erfolg verspricht. Als andere Personen kommen vor allem die Kreditinstitute in Betracht. Eine Berufung auf das Bankgeheimnis ist insoweit ausgeschlossen. Die Finanzbehörden dürfen in diesen Fällen anhand der Kontobewegungen prüfen, ob die Steuerpflichtigen korrekte Angaben gemacht haben. Einem solchen Vorgehen sind wiederum Grenzen gesetzt, da sonst zu jeder Person entsprechende Auskünfte eingeholt werden könnten: Die Aufforderung zur Herausgabe von Konto- oder Depotauszügen muss zur Aufklärung eines steuerlichen Sachverhaltes geeignet sein und es muss ein konkreter Anlass für die vertiefte Prüfung bestehen. Ermittlungen »ins Blaue hinein« sind daher rechtswidrig.

5 Wegfall der Lohnsteuerkarte

Das Bundeszentralamt für Steuern speichert zu allen Steuerpflichtigen elektronische Daten (Lohnsteuerabzugsmerkmale), die für die Arbeitgeberseite abrufbar ist. Durch diese Datensammlung wird die Lohnsteuerkarte entbehrlich. Der automatisierte Datenabruf umfasst unter anderem

- Angaben zur Religionszugehörigkeit,
- Angaben zu den Identifikationsnummern des Ehegatten und der Kinder sowie
- Angaben zur Religionszugehörigkeit des Ehegatten und zum Familienstand.

Aus datenschutzrechtlicher Sicht problematisch ist, dass die Arbeitgeberseite Einsicht in persönliche Daten erhält, die dem Steuergeheimnis unterliegen. Die Einsicht in die Daten sollte jedoch den Beschäftigten in den Finanzbehörden vorbehalten bleiben, die zur Verschwiegenheit verpflichtet sind.[6] Ferner ist zu bedenken, dass zu einem späteren Zeitpunkt noch weitere Abrufberechtigte festgelegt werden könnten, wie es oft bei Datenbanken der Fall ist. Damit würde der Personenkreis wachsen, der Zugriff auf Steuerdaten hat. Zwar waren auch auf der Lohnsteuerkarte bestimmte persönliche Daten für die Arbeitgeberseite und andere sichtbar abgedruckt. Bei elektronischen Verzeichnissen bestehen allerdings Bedenken, dass fremde Personen unbefugt die persönlichen Daten abrufen könnten.[7]

Sicherheit beim Abruf der Daten?

Um die Daten abzurufen, muss von Arbeitgeberseite die Anmeldung in einem Internetportal erfolgen. Dort muss sie eine sogenannten Wirtschaftsidentifikationsnummer sowie die Identifikationsnummer und das Geburtsdatum der Beschäftigten angeben. Die Wirtschaftsidentifikationsnummer bildet ein weiteres spezifisches Identifizierungsmerkmal und wird insbesondere Arbeitgebern und Arbeitgeberinnen zugeteilt. Nur diejenigen von ihnen sind zum Datenabruf befugt, die aufgrund des jeweiligen Arbeitsverhältnisses eine Berechtigung erhalten haben.

Fraglich bleibt die Sicherheit derartiger Datenabrufe, denn die Wirtschaftsidentifikationsnummer muss künftig zwingend bei den Kontaktdaten beziehungsweise im Impressum auf Internetseiten angegeben werden, so dass dieses Datum im Internet frei recherchierbar sein wird. Eine Person, welche die Identifikationsnummer des Beschäftigten sowie den Geburtstag kennt, könnte sich folglich im Internet anmelden und somit als Arbeitgeber auf-

treten. Der Gesetzgeber möchte dem durch einen programmgesteuerten Hinweis entgegenwirken, wonach ein unberechtigter Datenabruf strafrechtliche Folgen nach sich ziehen kann. Aus datenschutzrechtlicher Sicht wünschenswert wäre es jedoch, den Zugriff Unbefugter durch technische Maßnahmen zu verhindern.

6 Ermittlungen der Steuerfahndung

Die Steuerfahndung bilden Dienststellen innerhalb der Finanzverwaltung, die mit besonderen Ermittlungsbefugnissen ausgestattet sind. Sie haben unter anderem die Aufgabe, Steuerstraftaten und Steuerordnungswidrigkeiten aufzudecken. Die Steuerfahndung ist nicht verpflichtet, im Rahmen der Ermittlung zunächst die Steuerpflichtigen selbst zu befragen. Sie kann direkt an andere Stellen herantreten und Auskünfte über die Steuerpflichtigen einholen. Bestehen Anhaltspunkte dafür, dass eine Vielzahl von Steuerpflichtigen etwa bei den abgegebenen Steuererklärungen unwahre Angaben gemacht haben, dann sind sogenannte Sammelauskunftsersuchen gegenüber anderen Stellen erlaubt. Voraussetzung ist, dass die Steuerfahndung ihr Vorgehen auf einen konkreten Anlass stützen kann und keine Ermittlung »ins Blaue hinein« betreibt.

Beispielsweise ist die Steuerfahndungsbehörde befugt, von einer Zeitung die Übermittlung von Namen und Anschriften einzelner Chiffre-Anzeigen zu fordern, in welchen ausländische Immobilien mit hohem Wert angeboten werden, wenn konkrete Anhaltspunkte dafür vorliegen, dass die jeweiligen Personen keine vollständigen Steuererklärungen abgegeben haben. Solche Anhaltspunkte können beispielsweise bestehen, wenn es in naher Vergangenheit bezüglich werthaltiger Immobilien bereits belegbare Trefferfälle gegeben hat.

Die Suchmaschine *X-PIDER*

In die Kritik geraten war der Betrieb der Suchmaschine *X-PIDER*, mit deren Hilfe die Steuerfahndung vor allem Internetmarktplätze gezielt nach Unternehmen durchsuchte, die ihre Artikel als »Privatperson« verkauften, um ihre Gewinne nicht zu versteuern.[8] Zwar handelt es sich bei den erlangten Informationen um frei zugängliche Daten, wobei täglich circa 100 000 Webseiten automatisch durchsucht werden. Allerdings liegen keine Zahlen darüber vor, wie viele Steuerverfahren auf Basis der Ergebnisse eingeleitet wurden. Würde es sich nur um wenige Verfahren han-

deln, so läge zugleich ein Indiz dafür vor, dass entsprechende Ermittlungen nicht anlassbezogen erfolgen oder nicht auf gesicherten Erfahrungswerten beruhen und damit unzulässig sind.

7 Datenverarbeitung durch die Finanzbehörden im Überblick

- Das Steuergeheimnis schützt das private Geheimhaltungsinteresse der Steuerpflichtigen sowie das öffentliche Interesse an einer gleichmäßigen Besteuerung.
- Von Informanten rechtswidrig erlangte und im Anschluss an die staatlichen Behörden verkaufte Daten unterliegen nicht immer einem Beweisverwertungsverbot. Dabei ist auch das hohe Interesse der Bevölkerung an der Aufklärung von Steuerstraftaten zu beachten.
- Die bundeseinheitliche Identifikationsnummer darf nicht als Personenkennzeichen dienen. Eine Verknüpfung von Daten über diese Nummer darf nicht erfolgen.
- Finanzbehörden können unter bestimmten Bedingungen Kontostammdaten erhalten und auch Angaben zu Konten- und Depotbewegungen einfordern.
- Die Steuerfahndung ist befugt, Sammelauskünfte zu mehreren Steuerpflichtigen einzuholen, wenn konkrete Anhaltspunkte für falsche oder unvollständige Angaben bestehen und keine Ermittlung »ins Blaue hinein« erfolgt.
- Beim Datenabruf aus Datenbanken ist für eine sichere Anmeldung Sorge zu tragen.

Anmerkungen

1 Florian Rötzer, Italienisches Finanzministerium veröffentlichte Einkommensteuererklärungen aller Bürger, Heise Online vom 1.5.2008, im Internet unter http://heise.de/-204480.

2 Zeit online/DPA/Reuters, Millionen-Betrag für Informanten?, Zeit Online vom 17.2.2008, im Internet unter http://www.zeit.de/online/2008/08/zumwinkel-bnd-zahlungen.

3 Sven Afhüppe/Peter Reinhardt, Baden-Württemberg lehnt Kauf von Steuerdaten ab, Handelsblatt online vom 1.3.2010, im Internet unter http://www.handelsblatt.com/politik/deutschland/steuerstreit-baden-wuerttemberg-lehnt-kauf-von-steuerdaten-ab/3380490.html; »Ministerium prüft Kauf neuer Steuer-CD«, NDR online vom 23.7.2010; Frank Schuster, Kauf von Steuer-Daten geplatzt, in:

Frankfurter Rundschau vom 28.7.2010, im Internet unter http://www.fr-online.de/rhein-main/hessen-kauf-von-steuer-daten-geplatzt,1472796,4513790.html.

4 Bundesministerium der Finanzen, Bundeseinheitliche Identifikationsnummer für Steuerpflichtige, Informationsbroschüre Berlin 2009, S. 8.

5 Vgl. Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder »Zentrale Steuerdatei droht zum Datenmoloch zu werden« vom 25. bis 26.10.2007 in Saalfeld.

6 AP/AFP/DPA, Elektronische Lohnsteuerkarte – Zentrale Steuernummer stößt auf Kritik, SZ-Online vom 8.8.2007, im Internet unter http://www.sueddeutsche.de/politik/elektronische-lohnsteuerkarte-zentrale-steuernummer-stoesst-auf-kritik-1.894461.

7 Stefan Krempl/Jürgen Kuri, Bundesregierung beschließt zentrale Steuerdatei, Heise online vom 8.8.2007, im Internet unter http://heise.de/-161092.

8 DPA/TOL, Steuerfahndung online: Einnahmen in zweistelliger Millionenhöhe, Heise online vom 17.12.2003, im Internet unter http://heise.de/-90459.

Falk Lüke

Datenschutz aus Verbrauchersicht

Der Umgang mit personenbezogenen und personenbeziehbaren Daten hat sich in den vergangenen Jahren zu einem wichtigen Thema des Verbraucherschutzes entwickelt. Daten sind heute Teil des Verbraucheralltags und kaum mehr wegzudenken. Sie werden für viele Zwecke genutzt, teils mit und teils ohne Wissen und Zustimmung der Verbraucherinnen und Verbraucher. Oft wird die Diskussion relativ abstrakt über Bedrohungen und Gefahren geführt. Eine Technikfolgenabschätzung ist aus Verbrauchersicht besonders wichtig, da das Thema Datenschutz zu lange nicht ausreichend intensiv diskutiert wurde. Daten sind heute tief in kommerzielle Entscheidungsprozesse eingebunden. Dies sollen die folgenden Beispiele verdeutlichen:

- Wenn im Rahmen des Versandhandels nur Nachnahmeversand möglich ist, dann haben häufig Datenbestände damit zu tun.
- Ein Handyvertrag wird verweigert.
- Der Kredit ist teurer als erwartet oder wird ganz verweigert.
- Die Versicherung möchte jemanden nicht als Kunden.
- Die Werbung im Internet spricht gezielt auf persönliche Interessen an.
- Die Spendenorganisation fragt zu Weihnachten etwa die Großmutter, aber nicht den Enkel nach einem Spendenbeitrag für notleidende Kinder, den Naturschutz oder für andere gemeinnützige Zwecke.

1 Persönliche Daten als allgegenwärtiges Gut

Noch vor wenigen Jahrzehnten waren Daten behäbig. Sie lagen auf teuren Magnetbändern oder in Karteikästen. Heute sind sie wie jede digital vorliegende Information beliebig oft reproduzierbar, verlustfrei und binnen Millisekunden über den gesamten Globus zu verschicken. Speicherplatz kostet heute fast nichts mehr. Auf eine heute im Elektronikhandel übliche Festplatte passen beispielsweise mit einem Terabyte Kapazität etwa eine Billion Zeichen, was gut 300 Millionen eng beschriebenen DIN A4-Seiten entspricht. Eine solche Festplatte kostet derzeit etwa 80 Euro.

Möglichst viele Daten zu speichern und erst danach zu fragen, wozu, das scheint die Prämisse einiger Unternehmen geworden zu sein. Persön-

liche Daten sind in unserer Gesellschaft zu einem alltäglich verwendeten Gut geworden. Sie beschreiben Vorgänge, Umstände, Personen, Firmen, Organisationen indirekt oder direkt. Wenn wir im Kalender einen Termin eintragen oder ihn elektronisch bestätigen, wenn wir »Freunde« in einem →sozialen Netzwerk hinzufügen und wenn wir an der Kasse bargeldlos bezahlen – immer werden Informationen gespeichert und oft auch übermittelt. Das Urteil, das Unternehmen und andere Akteure fällen, wenn es um datenbasierte, geschäftliche Entscheidungen geht, fällt dabei oftmals sehr pauschal aus.

2 Grundprinzipien des Datenschutzes aus Verbrauchersicht

Datenschutz ist in Deutschland traditionell in zwei Teile gespalten: den öffentlichen und den nicht-öffentlichen Bereich. Im nicht-öffentlichen Bereich wird wiederum zwischen allgemeinen und speziellen Regelungen unterschieden:

- Die allgemeinen Regelungen des Bundesdatenschutzgesetzes (BSDG) sind auf jede Form der Datenerhebung, -nutzung und -weitergabe anwendbar.
- Spezialgesetzliche Regelungen für bestimmte Bereiche gehen diesen allgemeinen Regelungen vor.
  Die Regelungen im Bundesdatenschutzgesetz (BDSG) sind teilweise kompliziert und unübersichtlich. Doch neben dem BDSG gibt es insbesondere für den Bereich der Telekommunikation und der Telemediendienste in den entsprechenden Gesetzen[1] zusätzliche, für die Verbraucherseite relevante Normen.

Im Datenschutzrecht gilt die Regel: Alles ist verboten, was nicht erlaubt ist. Dies ist ein Regel-Ausnahme-Verhältnis, das oft als Verbot mit Erlaubnisvorbehalt bezeichnet wird (siehe auch den Beitrag von Hartge in diesem Band, S. 280 ff.).

Die Frage, wem wir wann und unter welchen Umständen unsere Daten zur Verfügung stellen und ihre Nutzung oder Weitergabe erlauben, beschäftigt den Verbraucherschutz seit Jahren intensiv. Mit der Digitalisierung haben sich jedoch die einschlägigen Chancen und Probleme vervielfältigt und beschleunigt.

Digitalisierte Kaufvorgänge

An zahlreichen Entscheidungen des Alltags sind heute Prozesse der elektronischen Datenverarbeitung (EDV) beteiligt, so etwa beim bargeldlosen Bezahlen. Zu diesem Zweck wird im Supermarkt vielfach das im Volksmund als »EC-Karte« bekannte Plastikkärtchen in ein Terminal eingeführt. Daraufhin muss eine persönliche Identifikationsnummer (PIN) eingetippt oder nur der Kassenbeleg unterschrieben werden.

Aus Sicht der Kundinnen und Kunden ist das Verfahren einfach. Sie müssen in irgendeiner Form nachweisen, dass es ihre Karte ist. Dann wird abgebucht. Was sie nicht ahnen: Damit wird eine Kette von datenbasierten Entscheidungsprozessen ausgelöst – die auch für sie in der Durchführung ihres Rechtsgeschäfts enorme Auswirkungen haben. Denn: Geben Sie ihre PIN ein, findet ein komplett anderes Verfahren statt, als wenn sie per Unterschrift bezahlen. Die Unterschrift ist Teil des für den Handel besonders günstigen Lastschriftverfahrens. Demgegenüber wird mit dem PIN-Verfahren eine etwas teurere Lösung gewählt, die für den Handel den Vorteil bietet, dass hier andere ein eventuelles Ausfallrisiko übernehmen. Für die Verbraucherseite hingegen ist das PIN-Verfahren das schlechtere: Wenn ihnen zu Unrecht auf diese Art Geld vom Konto abgebucht werden sollte, bietet das Lastschriftverfahren mehr Schutz. Es handelt sich hier also um eine klassische Entscheidungssituation, und genau in diesem Moment werden Daten zum Kriterium: die Karte wird bei der Kasse mit bestimmten Datenbeständen abgeglichen, während sie nur kurz im Terminal steckt.

Mitte 2010 führte diese alltägliche Situation zu einem Aufschrei in den Medien: Die Betreiber der Terminalnetze, die die eigentliche Zahlungsabwicklung übernehmen, standen damals im Verdacht, dass sie von Kundinnen und Kunden mit der Unterschrift nicht nur eine Einwilligung in die Nutzung ihrer Daten für die Abwicklung der Zahlung verlangen würden, sondern auch eine Einwilligung für die weitergehende Nutzung ihrer Daten (zum Beispiel zu Werbezwecken)[2].

Exzessive Nutzung von personenbezogenen Daten

Dies ist ein Alltagsphänomen: Unternehmen beschränken sich nicht auf das konkrete und für die Verbraucherseite verständliche Maß an Datenerhebung, -nutzung und -weitergabe. Es gibt immer wieder Fälle, in denen Firmen gerne mehr tun möchten. Aus Sicht des Verbraucherschutzes ist das oftmals unzulässig, vielfach aber vor allem ärgerlich: Wer kann schon am Freitagabend an der Supermarktkasse in Ruhe die ihm mit der Kassen-

bonrückseite vorgelegte Einwilligung durchlesen und wissentlich in die Datenübertragung einwilligen?

3 Freiwilligkeit der Einwilligung bei Verbraucherverträgen

Aus Verbraucherschutzsicht sind solche Einwilligungen, die in einer Form erteilt werden, die unter praktischen Gesichtspunkten nur als unwissentlich eingeschätzt werden können, oftmals als unwirksam zu beurteilen. Die Problematik der Willenserklärung, also der informierten und bewussten Einwilligung, ist eine Konstante in der Diskussion um den Datenschutz. Der Verbraucherschutz will niemandem die Möglichkeit verwehren, persönliche Daten preiszugeben. Aber es sollen all jene geschützt werden, die eben nicht wissen und unter den gegebenen Umständen nicht verstehen können, was mit ihren Daten passiert.

Neben dem oben genannten Beispiel sind es vor allem Klauseln in Verträgen, die eigentlich einen anderen Zweck erfüllen als den von Verbraucherseite erwarteten, beispielsweise der Abschluss eines Dienstleistungsvertrages oder eines Kaufvertrages. Hier mangelt es an Klarheit – ein Mangel, der nur dadurch zu beheben ist, dass entsprechend separat und deutlich in die Verwendung der Daten eingewilligt werden muss. Nicht nur, aber auch im digitalen Umfeld sind hier besondere Ärgernisse für die Verbraucherseite zu beobachten. Immer wieder kommt es dort zu untergeschobenen Einwilligungen, deren Wirksamkeit aufgrund der Umstände ihres Zustandekommens bezweifelt werden muss: Wer kann beispielsweise auf einem Mobiltelefon seitenlange Allgemeine Geschäftsbedingungen lesen?

4 Kundenbindung und Kundenmanagementsysteme

Viele Daten werden sozusagen nebenbei gesammelt, ohne dass sich die Verbraucherseite darüber im Klaren ist. Ein Beispiel sind Kunden- und Rabattkartensysteme, die der Kundenbindung dienen sollen. Hier gibt es jedoch auch datenschutzfreundliche, also datensparsame Varianten wie beispielsweise

- Stempelkarten im Café oder
- Rabatte bei Vorauszahlung im Schwimmbad und ähnlichen Institutionen.

Diese Systeme der Kundenbindung kommen ohne die Verarbeitung personenbezogener Daten aus. Es gibt aber auch andere Systeme – die »datenhungrigen« Varianten.

Beispielsweise speichern Bonuspunktsysteme oft nicht nur, dass Geld ausgegeben wurde, sondern auch, von welchen Personen, wann, wofür und welche Produkte oder Dienstleistungen sonst noch in Anspruch genommen wurden. Im Hintergrund werden diese Daten zusammengeführt und mit Algorithmen ausgewertet, um am Ende Wahrscheinlichkeiten zu berechnen: Welche Person wird wann was kaufen? Es geht um statistische Wahrscheinlichkeiten, um Mustererkennung.

Die Firmen verfolgen dabei vor allem zwei Interessen: Kundenbindung und Zahlungswahrscheinlichkeit, also bei letzterer die Frage, ob die Kundschaft eine »gute« oder »schlechte« Zahlungsmoral aufweist. Um dies zu beurteilen, gibt es umfangreiche Software, sogenannte → *Customer Relationship Management*-Systeme, die jeden Kaufvorgang abspeichern. Und es gibt externe Datenbanken, die zusätzliche Daten beisteuern können – oder gegen deren Datenbestand ein Abgleich stattfinden kann, um zum Beispiel die Plausibilität zu prüfen.

Diese Datenbanken können abstrakter oder konkreter Art sein. Konkret wären beispielsweise die Kundendaten eines politischen Wochenmagazins. Abstrakt ist hingegen der Abgleich mit einer Datenbank, die beispielsweise Vornamen enthält – denn Namen unterliegen gewissen Moden und die Wahrscheinlichkeit, dass Klaus-Jürgen über Vierzig, Ella entweder über Siebzig oder unter Achtzehn ist, ist statistisch betrachtet hoch. Es wird also immer ein Schluss gezogen: Für wen A zutrifft, für den könnte auch B zutreffen. Der *Online*-Buchhandel nutzt derartige Schlüsse zum Beispiel für Serviceleistungen. Wer sich für das eine Buch interessiert hat, könnte sich auch für ein anderes interessieren – weil andere Kaufwillige vorher danach gesucht oder dieses gekauft haben.

Derartige Muster sind es auch, die insbesondere im Internet dafür gesorgt haben, dass personenbezogene und personenbeziehbare Daten dort eine wesentliche Rolle spielen. Viele Angebote sind vordergründig kostenlos für die Nutzenden. Unwissentlich zahlen sie jedoch häufig mit Daten über sich selbst und über ihr Verhalten, ihre Freunde, ihre Welt. Das Interesse an diesen Daten beruht wiederum auf Wahrscheinlichkeiten. Wer sich für Autos, Frauen, Schlagermusik und Fußball interessiert, ist vermutlich ein Mann in einer bestimmten Altersgruppe. Diese Information reicht für manche Werbezwecke bereits aus – so könnte ihm etwa eine angepasste Werbung für Autoversicherungen offeriert werden.

Dies klingt zunächst harmlos. Doch spätestens wenn es um die Bezahlmethoden geht, um die Frage, ob ein Kredit gewährt wird – und wenn ja, zu welchen Konditionen – sind derartige → *Scoring*-Verfahren eine ernste Angelegenheit. Denn hier entscheiden Dateninterpretationen darüber,

ob und wann wir einen Vertrag abschließen dürfen und unter welchen Umständen. So werden regelmäßig Daten von Vergleichsgruppen herangezogen, die beispielsweise in einer vergleichbaren beruflichen Situation sind oder in einer ähnlichen Umgebung wohnen. Letzteres bezeichnet man auch als sogenanntes *Geo-Scoring*.

Wenn beispielsweise die Nachbarschaft für ihre schlechte Zahlungsmoral bekannt ist, bekommt man etwa zum Bezahlen eines Versandartikels häufig nur eine Nachnahme-Lieferung angeboten, auch wenn man selbst noch nie im Zahlungsverzug war. Der Gesetzgeber hat die Gefahren des *Geo-Scorings* erkannt. Eine Entscheidung, die aufgrund der Wohnadresse getroffen wird, ist zwar nach dem Datenschutzgesetz (§ 28b Nummer 3 BDSG) verboten. Allerdings ist dem Gesetzgeber bei der Fassung dieser Vorschrift im Jahr 2009 ein Fehler unterlaufen. Verboten ist ausschließlich das adressengenaue *Scoring*, während das Wohnumfeld-*Scoring*[3] selbst erlaubt bleibt.

5 Herkunft und Verwendung der Verbraucherdaten

Doch wo kommen all diese Daten ursprünglich her? Es gibt eine Menge Daten, die wir alle im Zuge unserer alltäglichen Beziehungen zu Organisationen, Unternehmen und Privatpersonen erzeugen oder hinterlassen. Im Regelfall ist davon auszugehen, dass diese Daten für einen bestimmten Zweck gespeichert und verwendet werden. Kritisch wird es immer dann, wenn für die Verbraucherseite nicht ersichtlich ist, dass Daten erhoben werden – wenn also nicht transparent ist, für welchen Zweck sie genutzt werden und wem diese Daten zugänglich gemacht werden. Nicht immer wird Verbraucherinnen und Verbrauchern beim Kauf eine Einwilligung im Rahmen verklausulierter Vertragswerke untergeschoben. Oft wird ihnen eine Leistung im Tausch gegen ihre Daten versprochen, über deren realen Wert jeder Einzelne entscheiden muss – was ihm jedoch schwer gemacht wird.

Wer beispielsweise an Gewinnspielen teilnimmt, gibt regelmäßig vielfältige Informationen über sich preis. Der Gegenwert ist oft gering. Was fehlt, ist Transparenz: Was passiert mit meinen Daten? Was sind meine Daten eigentlich wert?

Eine klare Kennzeichnung und die Möglichkeit, Dienstleistungen auch dann in Anspruch zu nehmen, wenn man nicht bereit ist, die eigenen Daten für den betreffenden Zweck zur Verfügung zu stellen, ist eine der Kernforderungen von Verbraucherschutzorganisationen.

Bei der Nutzung sozialer Netzwerke im Internet ist oft klar, dass Daten für Werbezwecke genutzt werden sollen. Aber wie viel die Daten wert sind, wird erst klar, wenn man gegen Zahlung eines entsprechenden Betrages alternativ auch auf diese Angabe von Daten verzichten könnte. In der öffentlichen Diskussion wird diese Forderung nach einer Trennung von Vertragsschluss und Datennutzung auch als Koppelungsverbot bezeichnet.

Im Jahr 2008 hatte der Verbraucherzentrale-Bundesverband einen Rechercheur beauftragt herauszufinden, wie leicht es ist, auf dem Schwarzmarkt Kundendaten zu erwerben. Ganze 850 Euro sollte ein Datenträger kosten, auf dem Daten von über sechs Millionen Bundesbürgern und -bürgerinnen enthalten waren, davon viele mit Bankverbindungsdaten und anderen sensiblen personenbezogenen Daten. Als Quellen für die Daten wurden Call-Center vermutet, deren Sicherheitskriterien nicht den Anforderungen genügten und bei denen Beschäftigte diese Daten kurzerhand mitnehmen konnten. In der darauf folgenden Debatte um einen verbesserten Datenschutz versprach die Bundesregierung zwar viel. Doch als der Gesetzgeber die Änderungen im BDSG dann schlussendlich verabschiedete, waren aus Verbraucherschutzsicht nur unzureichende Verbesserungen getroffen worden. Dazu gehörten beispielsweise:

- Es gab keine grundlegende Überarbeitung des Bundesdatenschutzgesetzes.
- Das → Listenprivileg wurde nicht abgeschafft, sondern nur modifiziert.
- Strafen und Bußgelder wurden nur begrenzt erhöht.

Insbesondere um das Listenprivileg wurde intensiv gestritten. Der Hintergrund hierfür war eine grundsätzliche Entscheidung: Gibt es überhaupt Umstände, unter denen es ohne Einwilligung und Wissen der Betroffenen in ihrem Sinne sein kann, dass Daten über sie erhoben oder genutzt werden?

Im Kern der Debatte geht es um die Frage: *Opt-in* oder *Opt-out*? *Opt-in* bezeichnet eine sogenannte Zustimmungslösung: Eine Nutzung und Weitergabe ist nur nach vorangegangener Zustimmung des Einzelnen möglich. *Opt-out* hingegen bezeichnet hingegen eine Widerspruchslösung: Der Einzelne muss widersprechen, sofern er mit dem Vorhaben nicht einverstanden ist (siehe dazu auch den Beitrag von Fiedler in diesem Band, S. 165 ff.). In der Praxis wirkt sich das zum Beispiel bei Gewinnspielen aus: Die Voreinstellung (das *Default-Setting*) wird maßgeblichen Einfluss haben. Kaum eine Person kann, möchte oder sollte sich den ganzen Tag damit beschäftigen, welche raffinierte Formulierung man in einem Vertrag streichen oder welche Häkchen man im Browser wegnehmen muss. Es wäre ja

auch undenkbar, dass jemand eine Waschmaschine vor der Haustür abliefert, obwohl wir sie nicht bestellt haben und wir auf Nachfrage zu hören bekommen, dass wir ja nicht widersprochen hätten.

Digitale Welt stellt Verbraucherschutz vor neue Herausforderungen

Insbesondere die digitale Welt hat den Verbraucher- und Datenschutz vor neue Herausforderungen gestellt. Mit der Digitalisierung haben sich einige Grundlagen deutlich verändert. So wird die grundsätzlich vorhandene →Anonymität, mit der wir uns im Alltag bewegen, im digitalen Umfeld immer wieder durchbrochen und zum Gegenstand der Diskussion gemacht.

In unserer klassisch analogen, »realen« Umwelt können wir in einen Laden gehen, eine CD erwerben und mit Bargeld bezahlen. Niemand wird uns nach unserem Personalausweis fragen, niemand unseren Einkauf personenbezogen speichern. Stellen wir uns die gleiche Szene im Internet vor: Wir müssen bei einem *Onlineshop* ein Konto eröffnen und Daten hinterlassen. Oft wird protokolliert, was wir kaufen und was man uns daraufhin noch anbieten könnte. Manche Stücke sind für uns auch nicht zu erwerben, denn unsere →IP-Adresse lässt sich oft regional zuordnen. Und wo kämen wir da hin, wenn etwa polnische Nutzer im französischen oder deutsche im englischen Internetshop einfach so Musik erwerben könnten? Manchmal wird in Musikdateien mittels »digitalem Wasserzeichen« (*Watermarking*) noch in die lauten Stellen des Liedes für Menschen unhörbar ein absichtlicher Fehler eingebaut: ein Vermerk über den Käufer oder die Käuferin dieses Stückes, der zugleich rückverfolgbar ist für den Fall, dass irgendwo im Internet Kopien auftauchen.

Zudem werden unsere Bezahldaten gespeichert, unter Umständen nicht nur auf der Seite, bei der wir Musik erworben haben, sondern zum Beispiel auch beim Kreditkartenunternehmen. Bislang sind Versuche, mit Funkchips die digitale in die klassische reale Umwelt zu transferieren, nicht sehr erfolgreich gewesen, da die Verbraucherseite solchen Techniken kritisch gegenübersteht und daher wenig Interesse daran gezeigt hat.

Aber nicht nur beim Kaufvorgang unterscheiden sich diese Welten. Vieles von dem, was in der realen Welt als flüchtig gilt, wird im digitalen Umfeld erfasst und analysiert. Chatprotokolle geben exakt die Unterhaltung wieder, die wir vor zwei Jahren führten – an das Gespräch im Café können wir uns nicht mehr genau erinnern. Wer weiß heute, vor welchem Schaufenster sie/er gestern stand, zu welchen Themen sie/er gestern einen Artikel in der Zeitung las? Die »Werbewirtschaftsdienstleister« wissen

häufig besser über das Surfverhalten im *World Wide Web* Bescheid als die Nutzenden selbst. Sie verfügen dazu über Techniken, die ursprünglich für ganz andere Zwecke gedacht waren – zum Beispiel dafür, dass Nutzende sich nicht immer neu bei E-Mail-Dienstleistern anmelden müssen.

6 Modernisierungsbedarf aus Verbraucherschutzsicht

Das deutsche Datenschutzrecht hat sich in weiten Teilen bewährt, aber an diese neuen Anforderungen ist es nur halbherzig angepasst worden. Dieser Schritt steht seit einigen Jahren aus, wird aber bald kommen müssen – auch aufgrund der absehbaren technischen Entwicklungen. Dabei sind aus Verbraucherschutzsicht einige Grundprinzipien unverzichtbar.

Einer der großen Knackpunkte ist die Frage, welches Datenschutzrecht Anwendung findet. Die Europäische Datenschutzrichtlinie gibt vor, dass Daten von EU-Bürgerinnen und -Bürgern auch im Nicht-EU-Ausland nicht unterhalb des Niveaus der Richtlinie erhoben, verarbeitet und weitergegeben werden dürfen. Dieses Grundprinzip ist sehr gut, doch praktisch läuft es ins Leere. Insbesondere die rechtliche Durchsetzung europäischer Datenschutzstandards gegenüber Firmen mit Sitz in den USA stellt den Verbraucherschutz vor ein unlösbares Problem. Zwar gibt es mit der → *Safe-Harbor*-Regelung ein Abkommen, das Mechanismen für die Durchsetzung vorsieht. Doch praktisch ist das für Verbraucherseite kaum durchsetzbar. Adäquat wäre eine dem Rom-I-Abkommen[4] vergleichbare Regelung: Sobald sich ein Unternehmen aktiv an Verbraucherinnen und Verbraucher in einem Staat wendet, findet dessen Recht Anwendung. Wenn etwa ein Kunde aus Deutschland bei einem amerikanischen *Onlineshop* Waren kauft, würde dann deutsches Recht angewandt werden.

Doch auch in der Frage der Durchsetzung von Datenschutz-Ansprüchen muss neu nachgedacht werden. Die Quantifizierung von Datenschutzschäden fällt regelmäßig schwer. Für einzelne Personen gibt es daher kaum Gründe, sich auf einen langen und teuren Rechtsstreit mit einem Unternehmen einzulassen. Hier gibt es mehrere Schritte, die neben einer weiteren Stärkung der Datenschutzaufsichtsbehörden erfolgversprechend sind. Ein erster Schritt wäre die Aufnahme des Datenschutzes in den Katalog der verbraucherschützenden Normen, die einen Unterlassungsanspruch durch vom Gesetzgeber benannte Organisationen an Stelle des Einzelnen ermöglichen. Ein zweiter Schritt wäre die Möglichkeit der Einführung weiterer kollektiver Klagerechte für die Verbraucherseite. Wenn jene zivilrechtliche Klageinstrumente erhält, um ihre individuell nur gerin-

gen, aber in der kollektiven Summe beachtlichen Schadensersatzansprüche durchzusetzen, wäre das für datenhaltende Unternehmen ein Anreiz, mit Verbraucherdaten zurückhaltend und sicher umzugehen.

Bei der Softwarenutzung muss hingegen über einen grundsätzlichen Prinzipienwandel nachgedacht werden. Die Einwilligung zur Verarbeitung personenbezogener Daten sollte nicht pauschal und abstrakt erteilt werden, sondern dann, wenn erstmalig Daten erhoben, genutzt oder weitergegeben werden. Neue Nutzende dürften nicht dazu gedrängt werden, ihre Daten unabsichtlich und unwissentlich preiszugeben. Software ist deshalb grundsätzlich nach dem *Privacy by Design*-Prinzip zu gestalten. Erst eine aktive Freigabe, bei der über deren Auswirkung aufgeklärt wird, kann die Nutzenden in die Lage versetzen, zu verstehen, welche Folgen ihre Entscheidung jeweils hat.

Dies gilt nicht nur für Software auf klassischen Computern, sondern auch für die Gestaltung komplexer Systeme wie zum Beispiel die sogenannten intelligenten Stromnetze, bei denen ein Abgleich von Verbrauchsdaten- und Produktionsmengen zu einer effizienteren Ressourcennutzung beitragen soll (zu *Privacy by Design* siehe auch den Beitrag von Schaar in diesem Band, S. 363 ff.). Die technisch anstehenden Veränderungen hin zu einer Verlagerung von Daten in die → *Cloud* werden bei der Verbraucherseite auf Ablehnung stoßen, wenn sie keine effektiven Kontrollmechanismen über ihre Daten erhält.

Für die digitale Welt ist es auch unerlässlich, Wege zu suchen, neben einer rechtsverbindlichen Version auch eine maschinenlesbare Version der Datenschutzbedingungen verpflichtend einzuführen. Nur mittels technischer Hilfsmittel können die Verbraucherinnen und Verbraucher in die Lage versetzt werden, in der digitalen Welt informierte, aber auch in der Realität praktikable Entscheidungen zu treffen (siehe auch den Beitrag von Roßnagel in diesem Band, S. 331 ff.).

Es besteht also umfassender Handlungsbedarf, um Verbraucherdaten angemessen zu schützen und die Menschen wieder in die Lage zu versetzen, selbst zu bestimmen, wer mit ihren Daten wie umgeht – und das auch noch handhabbar zu gestalten. Denn eines ist sicher: Es ist niemandem zuzumuten, sich den ganzen Tag mit dem Schutz seiner Daten zu beschäftigen. Hier die notwendige Klarheit für eine Entscheidungsfindung zu schaffen und die Durchsetzung der eigenen Rechte zu ermöglichen, ist die dringlichste Aufgabe, die vom Gesetzgeber angegangen werden muss. Nur durch die Festschreibung dieser Prinzipien können Verbraucherinnen und Verbraucher die Rolle einnehmen, die ihnen in der Konstruktion informationeller Selbstbestimmung zugedacht ist.

Anmerkungen

1 Telekommunikationsgesetz (TKG) und Telemediengesetz (TMG).
2 Landesbeauftragter für den Datenschutz und die Informationsfreiheit NRW, NRW-Datenschutzbeauftragter schließt Verfahren gegen die Easycash GmbH mit einem Bußgeld von 60 000 Euro ab, Pressemitteilung vom 12.9.2011, im Internet unter https://www.ldi.nrw.de/mainmenu_Service/submenu_Pressemitteilungsarhiv/Inhalt/PM_Datenschutz/Inhalt/2011/Easycash/Easycash.php
3 Das Wohnumfeld-*Scoring* vergleicht Daten beispielsweise anhand der Postleitzahl.
4 Übereinkommen über das auf vertragliche Schuldverhältnisse innerhalb der EU anzuwendende Recht (Übereinkommen von Rom), es trat am 1.4.1991 in Kraft.

Christoph Fiedler

Freiheit und Grenzen der Datenverarbeitung am Beispiel adressierter Werbung

Was die Meinungs- und Pressefreiheit für die Demokratie ist, ist die Werbefreiheit für die Marktwirtschaft. So wie die Freiheit politischer Kommunikation für den Kampf der Politikerinnen um die Wahlentscheidung der Bürger unverzichtbar ist, so ist die Freiheit kommerzieller Kommunikation für den Wettbewerb der Unternehmen um die Kaufentscheidung der Verbraucher konstituierend. Ohne Meinungsfreiheit gibt es keine wettbewerbsorientierte Politik, und ohne Werbefreiheit existiert keine wettbewerbsorientierte Wirtschaft.

Dass eine freie Wirtschaft mit Wettbewerbs- und Werbefreiheit staatlich gelenkten Wirtschaftssystemen nachhaltig überlegen ist, kann nach dem derzeitigen Stand der Geschichte nicht ernsthaft bezweifelt werden. »Wer ausgerechnet der Wirtschaft die Freiheit nehmen will, wird immer sehr viel mehr verlieren als gewinnen.«[1] Schon die Ressourcen und Chancen, die freie Wirtschaftssysteme ohne Rückgriff auf staatliche Sozialleistungen den Menschen zur Verfügung stellen, sind trotz vieler Probleme in aller Regel um ein Vielfaches größer. Hinzu kommt, dass bislang nur Gesellschaften mit funktionierender Marktwirtschaft in der Lage waren, durch Zwangsabgaben aus dem im freien Markt erwirtschafteten Mehrwert »die für ein menschenwürdiges Leben erforderlichen Sozialleistungen zu erwirtschaften«.[2]

Kann man noch weiter gehen und mutmaßen, funktionierende Marktwirtschaften, und also auch Werbung, seien Bedingungen einer funktionierenden Demokratie? Dass zumindest Elemente freier Marktwirtschaft offenbar auch ohne Demokratie funktionieren können, ist jedenfalls kein Gegenbeweis. Und wer funktionierende Demokratien ohne funktionierende freie Marktwirtschaft sucht, wird nicht schnell fündig.

1 Werbeformen und ihr datenschutzrechtlicher Bezug

Die für eine erfolgreiche Teilnahme am wirtschaftlichen Wettbewerb nötige Werbung ist so vielfältig wie die Produkte und Kommunikationssituationen der jeweiligen Gesellschaft. Und so unterschiedlich die

Werbeformen, so unterschiedlich ist auch ihre datenschutzrechtliche Relevanz. Während einige Werbeformen ohne die Verarbeitung personenbezogener Daten unmöglich sind, kommen andere ohne jedes personenbezogene Datum aus.

Werbung ohne datenschutzrechtliche Relevanz

Keinerlei personenbezogene Daten werden beispielsweise für folgende Werbeformen benötigt:
- Anzeigen in Zeitungen und Zeitschriften,
- Werbespots im Rundfunk,
- Plakate,
- viele Werbebanner im Internet.

Eine Ökologie-, Jagd-, Fahrrad- oder Autozeitschrift enthält zum Beispiel dem Thema entsprechende und damit auf das Leserinteresse bedarfsgerecht zugeschnittene Werbung. Dieses Ziel wird durch den redaktionellen Kontext der Werbung gesteuert, ohne dass personenbezogene Daten der Leserinnen und Leser verarbeitet werden. Auch die Abonnenten einer solchen Zeitschrift können nicht argumentieren, sie hätten mit der Bestellung unter Angabe von Namen und Adresse nicht darin eingewilligt, die Seiten mit Anzeigenwerbung oder Anzeigenbeilagen zu erhalten.

Nichts anderes gilt für eine Vielzahl digitaler Medien, in denen etwa Bannerwerbung passend zum Kontext der redaktionellen Inhalte und ohne Verarbeitung von Nutzerdaten erfolgt.

In all diesen Fällen mag es Leserinnen oder Leser geben, die die jeweiligen Medien lieber ohne Werbung konsumieren wollen. Ein Recht darauf kann ihnen jedoch nicht eingeräumt werden, ohne damit die Rechte der Medienwirtschaft zur freien Gestaltung von Medien und Werbung zu verletzen. Der Medienverzicht und Umstieg auf werbefreie Medien ist die richtige Antwort dieser kleinen Minderheit radikaler Werbegegner.

Adressierte Werbung

Unter adressierte Werbung fallen beispielsweise
- persönlich adressierte Briefe oder Werbeemails,
- Katalogzusendungen an namentlich genannte Personen,
- Werbeanrufe.

Adressierte Werbung verarbeitet schon mit dem Namen und der Adresse personenbezogene Daten der umworbenen Personen. Die Frage nach deren Rechten, über die Verwendung ihrer Daten zu bestimmen (Selbstbestimmung) und über die Verwendung der Daten ausreichend informiert zu werden (Transparenz der Datenverarbeitung), ist datenschutzrechtlicher Natur (siehe auch den Beitrag von Dix in diesem Band, S. 290 ff.).

Hinzu kommt der Aspekt, inwieweit ein Werbemittel unabhängig von der Frage der Adressierung die Persönlichkeitssphäre berührt. So verlangt deutsches Wettbewerbsrecht für Werbeanrufe bei Verbraucherinnen und Verbrauchern eine Einwilligung schon wegen der Beeinträchtigung der Privatsphäre durch die Lästigkeit des Anrufs. Dieses Einwilligungserfordernis ist unabhängig vom Datenschutzrecht. Demgegenüber sind etwa die Werbeformen des adressierten Briefes oder des Haustürbesuches wettbewerbsrechtlich von keiner Einwilligung abhängig.

2 Adressierte Werbung und Datenschutz

Zurück zum Datenschutz: Zur Realisierung des Selbstbestimmungsrechts – zum Beispiel über die Verwendung der Adresse zu Werbezwecken – stehen zwei grundsätzlich unterschiedliche Wege zur Verfügung.

Widerspruchslösung: *Opt-out*

Die Verarbeitung personenbezogener Daten zu Werbezwecken kann zulässig sein, wenn die beworbene Person das Recht hat, dieser Verarbeitung jederzeit zu widersprechen, und sowohl über die beabsichtigte Datenverarbeitung als auch über ihr Widerspruchsrecht informiert wird. Dies bezeichnet man auch als *Opt-out*. Die Widerspruchslösung gilt beispielsweise, wenn Unternehmen ihre Kundschaft anschreiben, um für eigene oder fremde Produkte zu werben: Eine Krankenversicherung etwa wirbt für eine zusätzliche Pflegeabsicherung oder ein Motorradzubehörhändler bietet seinen Kunden eine Motorradzeitschrift im Auftrag des Verlages an. Immer ist die Kundin bei Vertragsschluss über die Absicht der Verwendung ihrer Daten für Werbezwecke und über ihr Widerspruchsrecht zu informieren; ein weiterer Hinweis auf ihr Widerspruchsrecht muss bei jeder werblichen Ansprache erfolgen. Daneben gibt es ein Recht auf Auskunft über gespeicherte Daten (siehe auch den Beitrag von Dix in diesem Band, S. 290 ff.).

Einwilligungslösung: *Opt-in*

Demgegenüber ist eine vorherige Einwilligung der Beworbenen insbesondere erforderlich, wenn ein Unternehmen Adresslisten an andere Unternehmen weitergeben will, die neben der Kundeneigenschaft nach zusätzlichen Merkmalen wie etwa »Einkauf im letzten halben Jahr« sortiert werden[3] (vgl. hierzu auch den Beitrag von Lüke in diesem Band, S. 154 ff.).

3 Informationelle Selbstbestimmung und kommerzielle Kommunikation

Das informationelle Selbstbestimmungsrecht wird nicht nur durch eine vorherige Einwilligung, sondern auch durch eine Widerspruchsmöglichkeit gewahrt.

Soweit es um Daten geht, die einem Unternehmen bei Vertragsschluss anvertraut werden, kann die Nutzung der Daten zu Werbezwecken von vornherein durch Widerspruch unterbunden werden. Darauf ist bei Vertragsschluss hinzuweisen. Darüber hinaus steht es den Verbraucherinnen und Verbrauchern frei, jeden weiteren Werbebrief durch einen Widerspruch zum Letzten zu machen. Auf diese Möglichkeit muss schließlich jeder Werbebrief hinweisen.

Nicht nur das informationelle Selbstbestimmungsrecht der Beworbenen genießt den Rang eines Grundrechts. Auch die Freiheit der werbenden Unternehmen zu kommerzieller Kommunikation ist grundrechtlich geschützt und benötigt praktikable Entfaltungsmöglichkeiten. Diese sind bei einer Widerspruchslösung auch deshalb vorhanden, weil die größte und wichtigste Gruppe der umworbenen Bürgerinnen und Bürger in der Frage des Werbeinteresses weder kategorisch ablehnend noch bejahend gestimmt ist. Uninteressante Werbung wird von den meisten Personen ignoriert oder als lästig empfunden, interessante Werbung wird jedoch bemerkt, als Information verarbeitet und begrüßt. Was interessant ist und was nicht, erscheint je nach individuellem und gesellschaftlichem Kontext, nach Situation und Fragestellung ganz unterschiedlich.

Bei einer Widerspruchslösung kann der engagierte Werbefeind sich von adressierter Werbung weitestgehend befreien; andererseits geht aber auch der erhebliche Nutzen für eine sehr viel größere Zahl von Bürgerinnen und Bürgern wie für den wirtschaftlichen Wettbewerb nicht verloren.

Adressierte Werbung ist für Wirtschaft und Verbraucherseite wichtig

Wie so häufig ist es jedoch schwierig, in Diskussionen mit wenigen Protestierenden den Vorteil für die vielen Schweigenden zu belegen. Dennoch dürfte hier ein Schlüssel für die Frage adressierter Werbung liegen. So hängen beispielsweise von der brieflichen Leserwerbung bis zu einem Fünftel der Abonnementauflage und der entsprechenden Leserinnen und Leser einiger hochwertiger Zeitungen und Zeitschriften ab.

Der Verlust dieser Möglichkeit zur Leserwerbung hätte sehr negative Auswirkungen auf die Auflagenentwicklung, auf die Anzahl der Zeitungsleserinnen und -leser und auf die Möglichkeiten der Finanzierung des Titels. Die Werbebriefe einer Wirtschaftszeitung etwa an die Kunden eines Markenartiklers sind aber nicht nur für die Presse wichtig. Dass auch für ihre Adressaten die Vorteile überwiegen, belegt das Verhältnis der Widerspruchsraten gegenüber den positiven Antworten.

So erhält etwa eine Publikation auf 100 000 Angeschriebene circa eine bis zwei Beschwerden; im Durchschnitt der Verlage dürften es 0,5 bis 10 ablehnende Äußerungen auf 100 000 Briefe sein. Gleichzeitig reagieren aber bis zu circa 2 Prozent, also 2 000 der angeschriebenen Personen, mit der Entscheidung, die Zeitung regelmäßig lesen und deshalb abonnieren zu wollen.[4] Dem Einwand, dass nicht nur diejenigen, die sich tatsächlich beschweren, von der Werbung negativ berührt sein mögen, muss entgegnet werden, dass auch nicht nur diejenigen, die letztlich regelmäßige Zeitungsleserinnen oder -leser werden, das Angebot mit Interesse und ohne Ablehnung zur Kenntnis genommen haben.

Das Beispiel verdeutlicht zudem einen der Gründe, warum adressierte Werbung auch an Nicht-Kunden für ein Produkt unverzichtbar sein kann: Presseabonnements sind wie Spenden erklärungsbedürftige Produkte ohne Ladenlokal; sie müssen potenziellen Lesern und Leserinnen in einem ruhigen Moment erläutert werden. Dass für solche Angebote die Möglichkeit des Anschreibens erst nach ausdrücklicher vorheriger Zustimmung nicht genügt, hat übrigens der Bundestag in der Datenschutznovelle 2009

dadurch zum Ausdruck gebracht, dass er politische Parteien und sonstige Spendenorganisationen bei ihrer adressierten Spendenwerbung von vielen Datenschutzrestriktionen freistellte.[5]

Digitale Werbung

Auch für einen Teil der digitalen Werbung ist letztlich allein eine Lösung angemessen, die den Betroffenen informierte Wahlmöglichkeiten belässt. Das gilt beispielsweise dann, wenn statistisch geschätzte Interessen der unbekannten Nutzer von Internet-Browserprofilen für Werbezwecke verwendet werden. Die Nutzenden können dabei die Profilbildung und -verwendung durch einfache Einstellungen in ihren Endgeräten steuern. Bei einer solchen Datenverarbeitung zu Werbezwecken überwiegen die Vorteile auch für die Nutzerinnen. Die Werbung ist hier noch nicht an Personen adressiert und soll es auch nicht sein.

Ein angemessenes Verhältnis zwischen legitimem Datenschutz und legitimer Datennutzung darf nicht durch fast schon populistische Verzerrungen zu Lasten kommunikativer Notwendigkeiten freier und marktwirtschaftlicher Demokratien gestört werden. Weder die adressierte Werbung noch die Einblendung von Werbebannern (bei der frühere Nutzungsschritte im Internet-Browser verarbeitet werden, die aber keiner Person zugeordnet sind) sollen oder können Menschen überwachen, unterdrücken oder auch nur zum Erwerb bestimmter Produkte zwingen. Wer solchen groben oder selbst raffinierten Profilen »die Wirkung von Zwangsmitteln beimisst, der leugnet im Grunde die Fähigkeit der Individuen zur Selbstbestimmung«[6].

4 Datenskandale dürfen legitime Nutzung nicht hindern

Eine weitere Gefahr für viele Wirtschaftszweige besteht in der verbreiteten Gleichsetzung rechtmäßiger Formen der Datenverarbeitung mit illegalen und vielfach sogar kriminellen Machenschaften. Skandalöse Verstöße gegen angemessene Gesetze führen dann nicht zu dem besserem Vollzug des unverändert richtigen Gesetzes, wohl aber zu öffentlichkeitswirksam beschlossenen Gesetzesverschärfungen, die diejenigen, die sich ohnehin nicht an die Gesetze halten, kaum oder gar nicht, wohl aber die Gesetzestreuen treffen.

Anmerkungen

1 Joachim Gauck, zitiert nach Martina Fietz, Der falsche Kandidat, in: Focus Online vom 22.6.2010, im Internet unter http://www.focus.de/politik/deutschland/bundespraesident/tid-18745/joachim-gauck-der-falsche-kandidat_aid_522254.html.
2 A. a. O.
3 In den Worten der Datenschutzbehörden: »Übermittlung von nach mehr als einem Merkmal selektierten Adressen« (Beschluss des Düsseldorfer Kreises vom 26./27.11.2009).
4 Alle Zahlen aus 2009 (Quelle: Verband Deutscher Zeitschriftenverleger, VDZ).
5 Diese Regelung findet sich in § 28 Absatz 3 Satz 2 Nr. 3 BDSG.
6 Hans Peter Bull (erster Bundesdatenschutzbeauftragter, Anm. d. Verf.), Angstmache statt Aufklärung, in: Frankfurter Allgemeine Zeitung vom 17.10.2009, S. 8.

Gerd Billen

»Meine Daten gehören mir«

Die Kommunikationsbeziehungen zwischen Verbraucherseite und Wirtschaftsunternehmen unterliegen seit Jahren einem starken Wandel. Die direkte persönliche Beziehung zu der fast sprichwörtlichen »Tante Emma« in ihrem Laden an der Ecke ist weitgehend dem Besuch großer Supermärkte oder *Onlineshops* gewichen, die ihre Kundinnen und Kunden nur noch über gezielte Werbung erreichen.

Kundenbindung findet über Werbung statt. Diese muss am besten auf die verborgenen oder offensichtlichen Wünsche der Verbraucherinnen und Verbraucher ausgerichtet sein. Um diese Wünsche zu erfahren, hat sich die Wirtschaft einige Maßnahmen einfallen lassen wie beispielsweise

- Kundenkarten,
- Kundenbindungssysteme mit Bonusprogrammen,
- Preisausschreiben und andere Glücksspiele.

So werden die individuellen Konsumgewohnheiten und viele weitere private Daten erfasst. Die moderne Form der Kundendurchleuchtung ist die Analyse des Kommunikations-, Klick- und Surf- sowie Bewegungsverhaltens mit Computer und → *Smartphone*.

1 Das Ende der »informationellen Fremdbestimmung«?

Jahrelang war es selbstverständlich, dass Unternehmen diese Daten unbegrenzt auswerteten, für Werbezwecke nutzten und an andere Unternehmen weiter verkauften. Diese persönlichen Daten gehörten also faktisch den Firmen. Rechenschaft über die Speicherung, Auswertung, Nutzung und den Verkauf der Daten wurde nicht gelegt. Allenfalls wenn sich Menschen von Werbung belästigt fühlten, wurde ihnen ein Widerspruchsrecht und die Aufnahme in unverbindliche Sperrlisten zugestanden.

Diese Selbstverständlichkeit fand ein Ende, als spätestens im Sommer 2008 plötzlich bundesweit klar wurde, wie mit den Kundendaten oft umgegangen wird. Offensichtlich hatte sich eine Schattenwirtschaft etabliert, die Kundendaten nicht nur zu seriöser Werbung nutzte, sondern damit schwunghafte Geschäfte betrieb, manipulierte und verschleierte.

Alle zuständigen Bundesministerien – für Inneres, Justiz, Wirtschaft und Verbraucherschutz – waren sich damals unabgesprochen darüber einig, dass diese »informationelle Fremdbestimmung« beendet werden sollte, indem die Nutzung von Konsumdaten für Zwecke des Marketings von der ausdrücklichen Einwilligung der Verbraucherinnen und Verbraucher abhängig gemacht werden sollte (siehe zur Einwilligung auch den Beitrag von Hartge in diesem Band, S. 280 ff.). Was Daten- und Verbraucherschützer seit vielen Jahren forderten, schien plötzlich greifbar nah: Transparenz und tatsächliche Wahlfreiheit für Verbraucherinnen und Verbraucher, was mit ihren Daten geschieht.

Verhinderte Reformen

Den öffentlichen Bekenntnissen zu mehr Verbraucherdatenschutz folgte hinter den Kulissen in Berlin eine massive Einflussnahme der betroffenen Werbewirtschaft auf die Politikerinnen und Politiker der Regierungsparteien, der diese wenig entgegenzusetzen hatten. Es wurden – teilweise fern jeder Realität – Schreckensszenarien gezeichnet, wonach die Einführung des Einwilligungserfordernisses die freie Marktwirtschaft bedrohe. Als negative Folgen wurden unter anderem ein massiver Anstieg der Arbeitslosigkeit und das Wegbrechen von Steuereinnahmen benannt. Ohne größere öffentliche Diskussion beschloss dann der Bundestag ein Gesetz[1], wonach alles – mehr oder weniger – beim Alten bleiben sollte. Die Profilbildung mit fremden Daten wurde ein wenig eingeschränkt; die Transparenzpflichten wurden ein wenig verschärft.

2 Informationelle Selbstbestimmung in der Privatwirtschaft

Seit dieser Debatte steht die Frage auf der Tagesordnung, wem die Verbraucherdaten gehören. Ein Blick in das 25 Jahre zuvor vom Bundesverfassungsgericht gefällte Volkszählungsurteil (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.) gibt eine klare Antwort: Den Menschen steht ein Recht auf informationelle Selbstbestimmung zu; sie haben das Recht selbst festzulegen, wer was wann bei welcher Gelegenheit über sie weiß – auch in der Privatwirtschaft. Die Debatte hierzu verschärft sich, seit immer mehr Internetfirmen unser Verhalten im Netz analysieren und daraus Sozial-, Finanz-, Bewegungs-, Interessen- und Kommunikationsprofile erstellen. Diese Profile werden dann für raffinierte Werbung genutzt. Diese Werbung verspricht – nach elektronischer Analyse – ungefragt

unsere geheimsten, oft unbewussten Wünsche zu befriedigen. Letztlich geht es aber nicht um Wunschbefriedigung, sondern um Konsumanreize und wirtschaftliche Interessen. Dies ist zunächst nichts Verwerfliches, basiert doch unser Wirtschaftssystem hierauf.

Intransparente Datenverarbeitung durch die Werbewirtschaft

Kritikwürdig wird das Vorgehen, wenn wir als Verbraucherinnen und Verbraucher dabei übervorteilt und über den Tisch gezogen werden. Auf Grund der Komplexität der Datenverarbeitungen haben wir kaum noch eine Chance, die Verarbeitungsprozesse hinter der Werbung zu überblicken. Werbung jedoch, die transparent ist und den Markt durchschaubar macht, stärkt die Verbraucherseite und die seriösen Unternehmen. Nicht die zügellose Werbefreiheit ist für die Marktwirtschaft lebensnotwendig, sondern informative und rechtlich begrenzte Werbung, die kontrolliert wird und kritisiert werden kann. Davon sind wir in vieler Hinsicht meilenweit entfernt: Entgegen den klaren gesetzlichen Anforderungen erhalten wir meist keine Informationen über

- die Herkunft der verwendeten Daten,
- die Art der Auswertung der Daten,
- die mögliche Weitergabe der Daten oder
- das Recht, Widerspruch einzulegen.

Dies kann nicht den personell unterbesetzten Datenschutzaufsichtsbehörden und Verbraucherzentralen angelastet werden, die von solchen Verstößen nur in extremen Einzelfällen Kenntnis erlangen. Dafür verantwortlich sind Branchen, in denen Regelverstöße so lange zum marktkonformen Verhalten gezählt werden, so lange sich diese Verstöße finanziell lohnen. Und dies ist – leider – im Werbebereich immer noch sehr oft der Fall.

3 Selbstverpflichtungen der Werbewirtschaft

Die Unternehmen können auch eine andere Form der Kundenbindung praktizieren: Indem sie die potenzielle Kundschaft gut über ihre Produkte sowie über die Kundendatenverarbeitung informieren, schaffen sie Vertrauen in ihre Produkte und in das Unternehmen insgesamt. Auf diesem Weg bieten sie die Voraussetzung dafür, dass mit einem guten Gefühl konsumiert wird und dass ihnen Kundendaten freiwillig überlassen werden. Bisher wehrte sich die Wirtschaft mit Händen und Füßen selbst gegen freiwillige vertrauensbildende Maßnahmen: So wären beispielsweise →Datenschutzaudits und Gütesiegel – von qualifizierten und unabhängigen Stellen durchgeführt und vergeben – ein Mittel, mit dem Unternehmen ihre Kundschaft von der eigenen Qualität überzeugen könnten (siehe den Beitrag von Bock in diesem Band, S. 310 ff.). Doch nur schleppend kommt die Gründung der auf dieser Idee basierenden »Stiftung Datenschutz« voran, die ähnlich der Stiftung Warentest in Sachen Datenschutz die Guten von den Schlechten im Wettbewerb trennen soll.

Besonders ausgeprägt ist der Unwillen zur Transparenz bei den ausgeklügelten Profilbildungs- und → *Scoring*-Verfahren. Das Ergebnis eines solchen Verfahrens entscheidet zum Beispiel darüber, welche Produkte uns angepriesen werden, welche Vertragskonditionen gelten sollen und welchen Preis oder welche Zinsen wir zu zahlen haben.

4 Widerspruchsrecht durch fehlende Informationen vereitelt

Der Verweis auf die Möglichkeit, gegen die Nutzung der Daten Widerspruch einzulegen, ist häufig nicht ehrlich gemeint: Werden wir Verbraucher – was bisweilen gesetzeswidrig ganz unterlassen wird – über unser Widerspruchsrecht informiert, so bleibt oft unklar, wo wir wie unseren Widerspruch erklären können. Häufig müssen wir dabei Medienbrüche überwinden, wenn zwar die Einwilligung zur Werbenutzung elektronisch erklärt werden kann, nicht aber der Widerspruch.

Überwinden wir alle diese Hindernisse, so wissen wir immer noch nicht, welche vertraglichen Nachteile sich daraus ergeben können. Die Datenschutzbehörden ebenso wie die Verbraucherzentralen können ein Lied davon singen, wie trotz erklärtem Widerspruch die Datennutzung und Werbebelästigung fortgeführt werden. Wenig motivierend ist zudem die Vorstellung, dass unsere Daten möglicherweise von einem Unternehmen an andere Unternehmen weiterverkauft wurden und wir dort auch

widersprechen müssten. Zwar gibt es unternehmensübergreifende Widerspruchslisten, etwa die sogenannte Robinsonliste[2], doch werden diese von vielen Unternehmen nicht als verbindlich anerkannt. Schlimmer noch: Manche Unternehmen bieten die Aufnahme in angebliche Widerspruchslisten gegen Geld an. Dies geschieht jedoch nicht nur, um sich zu bereichern und um die Verbraucherseite zu übervorteilen, sondern um auf diese Weise an noch mehr Daten für Werbezwecke oder für illegale Kontoabbuchungen zu gelangen.

Verstärkte Transparenz im Verbraucherbereich ist überfällig

Verbraucherdaten werden von Unternehmen schon lange als wirtschaftliches Gut behandelt. Sie werden erhoben und genutzt, ohne dass die Verbraucherinnen und Verbraucher hieran angemessen beteiligt werden. Diese Praxis wird – hoffentlich – nicht mehr lange beibehalten werden können. Abmahnungen von Verbraucherzentralen gegen übervorteilende Allgemeine Geschäftsbedingungen, Datenschutzbußgelder wegen unzureichender Transparenz und des Nichtbeachtens des Betroffenenwillens nehmen zahlenmäßig bei der konventionellen Werbung zu und haben auch vor Gericht zunehmend Bestand.

Bei der telekommunikativen Werbung ist die Rechtslage eigentlich klar: Hier wird bei personifizierter Werbung fast immer die explizite Einwilligung der Betroffenen gefordert. Doch gerade hier werden diese Anforderungen massenhaft ignoriert oder dadurch umgangen, dass die Verantwortlichen von außerhalb der Europäischen Union aktiv sind und sich so der Rechtskontrolle entziehen. Auf diese Weise haben – auch über die europäischen Kundinnen und Kunden – Milliardenunternehmen wie *Google* oder *Facebook* ihr Vermögen angehäuft.

Insofern nehmen das Bewusstsein und der Widerstand von Verbraucher- und Datenschützern zu. Schon mittelfristig ist es realistisch, dass die »informationelle Fremdbestimmung« bei der kommerziellen Werbung in eine informationelle Selbstbestimmung der Verbraucherseite umgekehrt werden kann, und dass diese auch tatsächlich technisch darüber verfügen kann, wer was wann mit ihren Daten macht. Mündige Verbraucherinnen und Verbraucher wollen keine einseitige Manipulation, sondern wechselseitige Kommunikation. Von dieser Art der Kommunikation, die auf Vertrauen und Transparenz basiert, profitieren letztlich beide Seiten – Unternehmens- und Verbraucherseite – und damit auch die freie Marktwirtschaft.

Anmerkungen

1 Gemäß § 28 Absatz 3 BDSG gilt seit dieser Änderung: Werden listenmäßig zusammengestellte Daten ohne Einwilligung der Betroffenen für Zwecke der Werbung weitergegeben, muss dies dokumentiert werden. Aus der Werbung muss eindeutig hervorgehen, welche Stelle die Daten erstmalig erhoben hat (siehe auch →Listenprivileg).

2 Die Robinsonliste ist eine Liste, in die sich Personen, die keine unerwünschte Werbung erhalten möchten, kostenfrei eintragen können. Weitere Informationen im Internet unter http://www.robinsonliste.de.

Franz-Joseph Bartmann

Der kalkulierte Patient

Die heutige Medizin versetzt uns aufgrund des wissenschaftlichen Fortschritts und neuer Technologien in die Lage, Krankheiten in einem frühzeitigen Stadium zu erkennen. Zu diesen neuen Technologien zählen unter anderem hochauflösende Bildgebungsverfahren wie beispielsweise

- Computertomographie,
- Magnetresonanztomographie sowie
- Verfahren der Präimplantationsdiagnostik (PID).

1 Gefahr der Stigmatisierung

Diese Methoden erlauben es, Krankheiten möglichst früh zu diagnostizieren. Es ist heute sogar wahrscheinlich, dass durch neue genetische und molekularbiologische Behandlungsverfahren Defekte des menschlichen Genoms[1] bereits im Vorfeld einer wirklichen Erkrankung repariert werden können.

Beim momentanen Stand der Therapiemöglichkeiten bedeutet dies aber auch, dass Menschen, die noch keine Krankheitssymptome zeigen, bereits als potentiell behandlungsbedürftig gelten könnten. Manche Menschen kämen womöglich schon mit dem Siegel »zukünftig Kranker« zur Welt.

Dazu ein Beispiel: Die PID ermöglicht eine Beurteilung der Entwicklungsfähigkeit und genetischen Ausstattung bei künstlich befruchteten Embryonen, noch bevor sie in den Körper der Frau übertragen werden. Dabei werden die Chromosomen gezielt daraufhin untersucht, ob genetisch eine Veranlagung für bestimmte Krankheiten vorliegt, die beispielsweise in der Familie gehäuft aufgetreten sind. Es kann also sein, dass ein Kind zur Welt kommt und den Eltern und Ärzten ist bereits bekannt, dass es später mit einer gewissen Wahrscheinlichkeit erkranken wird. Dieses Kind gilt dann schon von Geburt an als »potenziell krank«.

Moderne Medizin basiert auf der Verarbeitung enormer Datenmengen

Erhöht wird diese Gefahr einer frühzeitigen, und möglicherweise unnötigen Stigmatisierung dadurch, dass Hochleistungsmedizin eng an digital

gesteuerte Prozesse gekoppelt ist, die mit der Generierung ungeheurer Datenmengen einhergehen. Dadurch entstehen zwangsläufig Datensammlungen, die standardisiert verwaltet und abgefragt werden können. Damit wird einerseits die rasche Verfügbarkeit und Reproduzierbarkeit gewährleistet, die für die Nutzung im Falle einer individuellen erkrankten Person unverzichtbar ist. Auf der anderen Seite bedeutet dies: Ohne eine adäquate Zugangsbarriere nimmt das Risiko eines unberechtigten Datenzugriffs Dritter zum Nachteil des noch »gesunden Patienten« zu. Die Folgen für die Privatsphäre der betroffenen Personen sind dabei unüberschaubar, der Geheimhaltungsschutz des Arzt-Patienten-Kontaktes wäre durchbrochen.

Beispielsweise würde eine Person, die als »potentiell krank« gilt, Schwierigkeiten haben, eine Krankenversicherung oder vielleicht sogar eine feste Anstellung zu erhalten, wenn die Krankenkasse oder der zukünftige Arbeitgeber davon wüssten.

Gentests durch private Firmen

In diesem Zusammenhang ist auch zu erwähnen, dass mittlerweile immer mehr Unternehmen Gentests nicht nur für Ärzte, sondern auch im Auftrag von privaten Personen durchführen. Deshalb gilt es, neben der sorgfältigen Abwägung von Chancen und Risken medizinischer Entwicklungen immer auch Aspekte des Datenschutzes zu beachten. Medizinischer Fortschritt darf nicht zum Preis des Verlustes der persönlichen Identität und Integrität der Patientinnen und Patienten erkauft werden. Allerdings haben die elektronische Datenerfassung und -übermittlung im etablierten Medizinbetrieb und hier vor allem in der Verwaltung bereits ein Ausmaß erreicht, welches das Recht auf informationelle Selbstbestimmung und die Wahrung des Arztgeheimnisses erheblich gefährdet. Obwohl – oder möglicherweise sogar weil – vieles von dem auf klaren gesetzlichen Vorgaben basiert, wird das in der Öffentlichkeit bisher kaum als Problem wahrgenommen. Dieser Beitrag geht auf einige kritische Entwicklungen in diesem Bereich näher ein.

2 Datenverarbeitung durch Krankenkassen

Da die Ressourcen der Krankenkassen grundsätzlich begrenzt sind, kann auch in der gesetzlichen Krankenversicherung die Höhe der Einnahmen niemals alle denkbaren Ausgaben abdecken. Selbst unter Berücksichtigung aller Wirtschaftlichkeitsmaßnahmen öffnet sich die Schere zwischen den

vorhandenen (und immer teureren) Behandlungsmöglichkeiten und den verfügbaren finanziellen Mitteln immer weiter. Dieser Konflikt führt zu einer stetig steigenden Reglementierung und Bürokratisierung des Medizinbetriebes und zu damit verbundenen Änderungen im medizinischen Betrieb. Betroffen ist davon nicht nur der Arzt oder die Ärztin (der »Leistungserbringer«), die diese Daten erfassen, verwalten und gegebenenfalls weiterleiten müssen. Auch die Patientinnen und Patienten sollten wissen, dass Daten über ihre Erkrankungen und die dadurch ausgelösten Leistungen mittelbar oder unmittelbar an ihre Krankenkasse oder gegebenenfalls den Medizinischen Dienst der Krankenkassen weitergeleitet werden. Zunehmend verlangt die Sozialgesetzgebung eine Datenfülle und Datenqualität, die unmittelbare Verknüpfungen zu einem Krankheitsfall und damit einer bestimmten Person nicht nur ermöglicht, sondern geradezu erzwingt.

Eine der konkreten gesetzlichen Forderungen lautet: »Die an der vertragsärztlichen Versorgung teilnehmenden Ärzte und die übrigen Leistungserbringer sind verpflichtet, die für die Erfüllung der Aufgaben der Krankenkassen sowie der kassenärztlichen Vereinigungen notwendigen Angaben, die aus der Erbringung, der Verordnung sowie der Abgabe von Versicherungsleistungen entstehen, aufzuzeichnen und gemäß den nachstehenden Vorschriften den Krankenkassen, den kassenärztlichen Vereinigungen oder den mit der Datenverarbeitung beauftragten Stellen mitzuteilen.«[2] Zu Letzteren zählen beispielsweise die Rechenzentren der Apothekerverbände, in denen alle Daten zu Verordnungen und Abgaben erfasst und ausgewertet werden.

Datenübermittlung durch Kassenärztliche Vereinigungen

Zur Art und Qualität der Daten heißt es des Weiteren: »Für die Abrechnung der Vergütung übermitteln die Kassenärztlichen Vereinigungen im Wege elektronischer Datenübertragung oder maschinell verwertbar auf Datenträgern den Krankenkassen für jedes Quartal für jeden Behandlungsfall (…) Daten«[3] zu Arzt und Patient, zu Art und Umfang der Behandlung, den dabei entstehenden Kosten und eventuellen Zuzahlungen.

Noch sind die Kassen in aller Regel aufgrund mangelhafter technischer Ausstattungen nicht in der Lage, alle Möglichkeiten einer derart umfänglichen Datensammlung zu nutzen. Für die nahe Zukunft ist allerdings zu erwarten, dass – über die bereits etablierten Auffälligkeits- und Zufälligkeitsprüfungen hinaus – die Daten in Steuerungssystemen erfasst werden und damit auch das unmittelbare Leistungsgeschehen vor Ort beeinflussen. Nur die wenigsten Patientinnen und Patienten dürften zudem wissen,

dass von ärztlicher Seite eine gesetzliche Meldepflicht besteht, wenn die Verletzung mittelbar oder unmittelbar durch einen Unfall oder eine Handlung Dritter verursacht wurde. In diesen Fällen kann die Kasse ihre Zahlungsverpflichtung auf Unfall- oder Haftpflichtversicherungen übertragen.

Datenverarbeitung bei privaten Krankenversicherungen

Besondere Probleme in Hinblick auf die Datenverarbeitung und den Datenschutz treten schließlich bei privaten Krankenversicherungen auf. Anders als die gesetzliche Krankenversicherung kennt die »Private« keine Mitversicherung von Familienangehörigen: Jedes Mitglied wird individuell nach seinem Alter und Erkrankungsrisiko bei Versicherungseintritt eingestuft. Entsprechend muss bereits bei Antragstellung jeder Versicherungswillige seine Krankheitsbiografie offenlegen. Unrichtige Angaben führen zum Versicherungsausschluss. Die Versicherung kann auch bestimmte Krankheiten und/oder Diagnosen vom Versicherungsschutz ausschließen. Die versicherte Person unterzeichnet bei Versicherungsabschluss eine schriftliche Einwilligungserklärung zur Entbindung der ärztlichen Schweigepflicht, so dass jederzeit auch Krankenunterlagen zu Prüfzwecken von der Krankenversicherung eingefordert werden können.

Die meisten Ärztinnen und Ärzte sowie Krankenhäuser bedienen sich bei der Rechnungsstellung für privat Versicherte inzwischen halböffentlicher oder privater Unternehmen. Jene gelangen dabei zwangsläufig in den Besitz von sensiblen Krankendaten, ohne dass dies vielen Versicherten als Datenschutzproblem bewusst wird. Es bleibt daher festzuhalten, dass mögliche Vorteile einer privaten gegenüber der gesetzlichen Krankenversicherung mit einem zumindest teilweisen Verzicht auf das Arzt-Patienten-Geheimnis und den gesetzlich zugesicherten Datenschutz erkauft werden.

Datenverarbeitung im Rahmen des Kollektivvertragssystems

Den Kassenärztlichen Vereinigungen obliegt im Regelfall die Sicherstellung der ambulanten Versorgung und die Verteilung der in jährlichen Verhandlungen ausgehandelten Budgetsumme an niedergelassene Ärzte und Psychotherapeuten. Sie sind föderal auf Länderebene organisierte Körperschaften öffentlichen Rechtes, also Trägerinnen hoheitlicher Aufgaben, die ansonsten dem Staat zukämen. Das System der Verhandlungsvollmacht der Kassenärztlichen Vereinigungen mit den Krankenkassen nennt man auch das Kollektivvertragssystem. Innerhalb dieses Kollektivvertragssystems gibt es seit Januar 2002 bei einigen besonders häufig vorkommenden

und daher kostenrelevanten Erkrankungen (beispielsweise Brustkrebs oder Diabetes) die Möglichkeit einer speziellen Versorgung, die für Ärzteschaft und Patientenseite eine besondere Verbindlichkeit beinhalten.

Dazu ein Beispiel: Das Konzept der sogenannten *Disease Management Programme*[4] *(DMP)* setzt auf eine verstärkte Patientenverantwortung, aber auch auf eine hohe Standardisierung der Behandlung, die zu einem maximalen Behandlungserfolg mit möglichst minimierten Kosten führen soll. Da mit der Durchführung der *DMP* nach dem Willen des Gesetzgebers die Kassen beauftragt sind, dürfen diese ganz offiziell und gesetzlich legitimiert die Daten erheben und verarbeiten, die »zur Gewinnung von Versicherten sowie zur Vorbereitung und Durchführung von *DMP* erforderlich sind.« Die Patienten und Patientinnen müssen – nach umfassender Aufklärung durch die Kasse – schriftlich ihre Zustimmung erteilen. Dadurch unterwerfen sie sich einer laufenden Kontrolle ihres Verhaltens und der vereinbarten Kooperation im Hinblick auf ihre jeweilige Erkrankung durch ihre Krankenkasse. Ihre Vorteile liegen im Versprechen einer standardisierten und damit häufig verbesserten Überwachung und Behandlung ihrer chronischen Erkrankung.

Datenübermittlung aufgrund von Behandlungsverträgen zwischen Ärzteschaft und Krankenkassen

In Hinblick auf den Datenschutz von allerhöchster Brisanz sind Behandlungsverträge, die von Krankenkassen mit Ärzten oder Arztgruppen unmittelbar ohne Einbeziehung der kassenärztlichen Vereinigungen geschlossen werden. Auch diese Form der Versorgung wurde vom Gesetzgeber im Sozialgesetzbuch besonders privilegiert. Das Wettbewerbsstärkungsgesetz von 2007 beinhaltet eine verpflichtende Option für die Kassen, ihren Patientinnen und Patienten eine hausarztzentrierte Versorgung anzubieten. Damit soll sichergestellt werden, dass – wie zu Zeiten des Krankenscheines vor 1995 – bei gesundheitlichen Problemen zunächst immer die Hausärztin bzw. der Hausarzt aufgesucht wird. Von dort wird dann gegebenenfalls die fachärztliche Überweisung oder die Einweisung ins Krankenhaus veranlasst. Mit der Wahrnehmung dieser hausärztlichen Lotsenfunktion sollen unnötige und teure Facharztbesuche vermieden und damit Kosten eingespart werden.

Datenübermittlung durch Hausarztpraxen

Für die Hausärzteschaft ist diese Form der Versorgung attraktiv, da ihre Position in der Gesundheitsversorgung aufgewertet wird. Die jetzt unmittelbar von den Kassen an die Hausarztorganisationen ausgezahlte

Honorarsumme wird von der jährlich mit den kassenärztlichen Vereinigungen ausgehandelten Gesamtvergütung abgezogen – im Fachjargon: bereinigt. Das grundsätzliche Problem besteht nun in der Honorarverteilung innerhalb der Hausarztverbände. Diese erfolgt nämlich im Regelfall nicht über ärztliche oder öffentlich bestellte Organisationen, sondern durch privatwirtschaftliche Auftragnehmer.

Erstmals werden somit sensible Patientendaten nicht nur von Körperschaften des öffentlichen Rechts, die allesamt dem Sozialgeheimnis unterliegen, bearbeitet und gespeichert. Die vertragsschließenden Hausarztverbände und deren private Auftragnehmer können den Datenschutz nicht auf dem erforderlichen Niveau garantieren. Die Krankenkassen auf der anderen Seite erfassen in diesem Verfahren ebenfalls deutlich mehr Daten als gesetzlich zulässig. Datenschützer haben obergerichtlich klären lassen, dass diese Art der Vertragsgestaltung datenschutzrechtlich unzulässig ist.[5]

Datenübermittlung durch Krankenhäuser

Die Daten, die bei einer Krankenhausaufnahme unmittelbar an die Krankenkasse weiterzuleiten sind, stehen dem bisher Erwähnten in nichts nach. Bei Zweifeln an der Zahlungsverpflichtung hat der Medizinische Dienst der Krankenversicherungen das Recht auf Einsicht in alle Behandlungsunterlagen. Dies hat zu einem grundsätzlichen Wandel der Positionierung des Krankenhauses im sozialen Netz der Daseinsvorsorge geführt. Aus einer karitativen Grundmotivation mit dem Anspruch auf menschliche Zuwendung und Pflege im Gesundungsprozess sind wirtschaftlich kalkulierende Unternehmen entstanden, die in dem kürzest möglichen Zeitraum hochtechnologische Leistungen zur Behandlung einsetzen und alles Weitere der ambulanten Versorgung überlassen (müssen).

3 Die elektronische Gesundheitskarte

Als 1995 die Krankenversicherungskarte den bis dahin gebräuchlichen Krankenschein in Papierform ablöste, war das Echo hierauf in der Öffentlichkeit durchaus geteilt.

Massiver Widerspruch kam vor allem aus der Ärzteschaft, die bereits damals den »gläsernen Patienten« entstehen und die ärztliche Schweigepflicht gefährdet sah. Dabei waren es weniger die sogenannten Stammdaten, die die Zugehörigkeit des Karteninhabers zu der ausgebenden Krankenkasse beinhalteten, sondern vielmehr später hinzugekommene

Daten zum Zuzahlungsstatus und zur Teilnahme an speziellen Versorgungsprogrammen, die datenschutzrechtliche Bedenken tatsächlich rechtfertigten.

Diese zusätzlichen Daten erlauben beispielsweise indirekt Rückschlüsse auf die Bonität und den Gesundheitszustand eines Karteninhabers und sind ohne notwendige Einwilligung durch persönliche Identifikationsnummer (PIN) oder anderweitige Freigabe von handelsüblichen Lesegeräten auslesbar.

Auch ist nicht gewährleistet, dass Kartenbesitz und rechtmäßige Inhaberschaft der Karte identisch sind. Immer wieder hat dies in den vergangenen Jahren zu meist unberechtigten Vorwürfen des Abrechnungsbetruges geführt, weil Leistungen mit Karten Verstorbener oder als verloren gemeldeten Karten erbracht und abgerechnet wurden.

Neben dem dadurch erzeugten wirtschaftlichen Schaden zu Lasten der Solidargemeinschaft entstehen den Krankenkassen darüber hinaus Kosten in zweifacher Millionenhöhe durch eine notwendige Neuausstellung von Krankenversicherungskarten bei Namens- oder Wohnortwechsel eines Versicherten oder bei einer Änderung der Versicherungsinhalte.

Folgerichtig hat der Gesetzgeber bereits 2004 im Sozialgesetzbuch die Entwicklung und Ausgabe einer elektronischen Gesundheitskarte verfügt. Bei dieser Karte können Daten verändert, nachträglich ergänzt oder die Nutzung der Karte gesperrt werden. Durch ein Lichtbild auf der Karte und die Nutzung einer PIN wird gleichzeitig die Rechtmäßigkeit des Kartenbesitzes sichergestellt. Die Prüfung der Kartengültigkeit mit gleichzeitiger Aktualisierung der jeweils bei der Krankenkasse hinterlegten Stammdaten erfolgt automatisch beim Einlesen der Karte anlässlich eines Arztbesuches.

Funktionen der neuen Gesundheitskarte

Diese Verbesserung der administrativen Funktion ist jedoch nur ein kleiner, vom notwendigen Entwicklungsaufwand her eher einfacher Teil der beabsichtigten Kartenfunktionen. Die Karte selbst soll Daten zu ärztlichen Verordnungen in elektronischer und maschinenlesbarer Form und Notfalldaten aufnehmen, die mit Hilfe eines elektronischen Arztausweises lesbar gemacht und in der Akutbehandlung genutzt werden können. Darüber hinaus soll sie die sichere Übermittlung von Krankheitsdaten (elektronischer Arztbrief), die fall- und einrichtungsübergreifende Verfügbarkeit wesentlicher Befunde und Maßnahmen (elektronische Patientenakte) und letztendlich eine aus Patientensicht erkennbare Auflistung der veranlassten Leistung und dadurch entstandener Kosten sicherstellen. Die Patientinnen und Patienten sollen die Karte auch für eigene Zwecke nutzen können, indem sie ihnen

wichtig erscheinende Daten in einem eigenen Datenfeld eingeben können oder sie etwa von ihrem behandelnden Arzt dorthin übertragen lassen.

Datenübertragung im Rahmen der elektronischen Gesundheitskarte

Die aus Patientensicht weitaus wichtigste Funktion ist jedoch die automatische Verschlüsselung aller Daten, die mit Hilfe der elektronischen Gesundheitskarte vermittelt werden. Nur von Patientenseite selbst können diese Daten mit Hilfe eines individuellen Schlüssels und mit Hilfe eines elektronischen Heilberufsausweises (HBA) für den behandelnden Arzt lesbar gemacht werden. Dadurch ist sichergestellt, dass die Patientinnen und Patienten in einer ansonsten kaum überschaubaren und kontrollierbaren elektronischen Datenlandschaft jederzeit die Verfügungsgewalt über ihre Daten behalten. Zumindest einige der in den vorherigen Abschnitten dargestellten datenschutzrechtlichen Probleme in der medizinischen Versorgung wären hierdurch lösbar. Von daher ist zu wünschen, dass die Ende 2011 begonnene Ausgabe dieses neuen Ausweises durch die Krankenkassen rasch zu einem erfolgreichen Abschluss gebracht werden kann.

4 Biodatenbanken und wissenschaftliche Forschung

Bereits zu Beginn dieses Beitrages wurde auf das hohe Gefährdungspotenzial großer Datensammlungen im Hinblick auf das informationelle Selbstbestimmungsrecht der Patientinnen und Patienten hingewiesen. Daten können auch ohne ihr Wissen und ihre Kenntnisnahme zu anderen als nur Versorgungszwecken benutzt werden. Dies ist in der Sozialgesetzgebung zwar mit Strafe bedroht. Immer wieder werden jedoch Fälle bekannt, in denen Teile der medizinischen Wissenschaft des Missbrauchs von Behandlungsdaten zu Forschungszwecken überführt werden, wobei den handelnden Personen häufig die Unrechtmäßigkeit ihres Vorgehens gar nicht bewusst ist.

Unter Beachtung bestimmter Vorgaben ist eine derartige Datennutzung sogar legal und kann zur Erzielung neuer Erkenntnisse zum Nutzen künftiger Patientinnen und Patienten beitragen. Ein ständiges Hinterfragen des ärztlichen Handelns zwecks rechtzeitiger Korrektur möglicher Fehlentwicklungen ist deshalb unverzichtbar. Die Grenzen zwischen einfacher Qualitätskontrolle und aktiver Forschung sind dabei durchaus fließend. Im Zweifel sollte lieber einmal zu viel als einmal zu wenig die Arbeit der Ethikkommissionen[6] in Anspruch genommen werden.

Sammlung genetischer Proben zu Forschungszwecken

Von wachsender Bedeutung sind sogenannte Biodatenbanken, in denen auf nationaler und internationaler Ebene mit Personendaten verknüpfte genetische Informationen oder Gewebeproben gesammelt werden. Die meisten derzeit existierenden Biodatenbanken dienen in erster Linie Forschungszwecken. Entweder werden die Materialien zur eigenen Forschung genutzt oder anderen zur Verfügung gestellt. Gerade bei Datenbanken, die genetischen Forschungszwecken dienen, ist die Größe der Kohorten[7] von entscheidender Bedeutung für das Forschungsergebnis. Nationale Datenbanken, vor allem in England und Skandinavien, beherbergen mittlerweile Daten und Materialien von 500 000 Menschen und mehr. Aber auch in Deutschland sind Datenbanken im Aufbau, die zur Erforschung häufiger chronischer Erkrankungen wie Diabetes, Krebs, Herz-Kreislauf und Demenzerkrankungen dienen sollen. Die sogenannte Helmholtz-Kohorte[8] soll in der Endphase beispielsweise 200 000 Personen umfassen.

Gesetzliche Grundlagen für Biodatenbanken

In letzter Zeit sind politische Forderungen nach einem umfassenden Biobanken-Gesetz laut geworden.[9] Das 2010 in Kraft getretene Gendiagnostikgesetz spart den Umgang mit genetischen Daten zu Forschungszwecken nämlich völlig aus. Auch der Deutsche Ethikrat forderte im Juni 2009 eine eigene Regelung, die den spezifischen Anforderungen an den rechtlichen Schutz der in Biobanken vorhandenen Proben und Daten Rechnung trägt. Der Umgang mit Daten aus genetischen Untersuchungen zu Forschungszwecken wird zwar durch einzelne Bestimmungen des Bundesdatenschutzgesetzes (BDSG) erfasst. Doch sind nach Meinung der verantwortlichen Politikerinnen und Politiker die schutzbedürftigen Interessen der Betroffenen im BDSG nicht deutlich genug formuliert. Diese Forderungen gewinnen dadurch besonders an Gewicht, dass der Bund selbst in der Finanzierung derartiger Datenbanken mit nicht unerheblichen Geldmitteln beteiligt ist.

Allerdings steht zu befürchten, dass durch den massiven Trend zur internationalen Vernetzung, der aus wissenschaftlicher Sicht sinnvoll und erforderlich ist, eine nationale Gesetzgebung keinen entscheidenden Einfluss bei möglicherweise zentralen Verstößen entfalten dürfte. Hier muss auch die internationale Gemeinschaft Regelungen schaffen.

Anmerkungen

1 Als Genom bezeichnet man den einfachen Chromosomensatz einer Zelle, der deren Erbmasse darstellt.
2 Siehe V. Sozialgesetzbuch (SGB V, Gesetzliche Krankenversicherung), § 294 – Pflichten der Leistungserbringer.
3 Siehe V. Sozialgesetzbuch (SGB V), § 295 Abs. 2 – Abrechnung ärztlicher Leistungen; eine vergleichbare Regelung auch in SGB V, § 297 – Zufälligkeitsprüfungen.
4 Wörtlich übersetzt: Krankheits-Management-Systeme.
5 Beschluss des OVG Schleswig-Holstein vom 12. Januar 2011, Az. 4 MB 56/10.
6 Ethikkommissionen sind nach jeweiligem Landesrecht bei Ärztekammern und/oder Hochschulen etablierte Einrichtungen, in denen Vertreterinnen und Vertreter aus Naturwissenschaft, Medizin, Rechtswissenschaft und Theologie über die Rechtmäßigkeit eingereichter Forschungsvorhaben urteilen. Häufig geht es dabei um die Erprobung neuer Medikamente und Behandlungsmethoden, aber zum Beispiel auch um die Lebendspende bei Organtransplantationen oder den Import und den Einsatz embryonaler Stammzellen in der Grundlagenforschung.
7 Als Kohorte bezeichnet man in diesem Zusammenhang die untersuchte Bevölkerungsgruppe bzw. die entsprechende Datensammlung.
8 Die Helmholtz-Kohorte ist die bislang größte bundesweite Bevölkerungsstudie. Sie soll neue Erkenntnisse über die Ursachen von häufigen multifaktoriellen Erkrankungen wie beispielsweise Krebs, Diabetes, Demenz und Herz-Kreislauf-Erkrankungen bringen. Über zehn bis zwanzig Jahre werden die Teilnehmenden regelmäßig medizinisch untersucht und unter anderem zu ihren Lebensgewohnheiten befragt. Dazu dienen speziell ausgearbeitete Fragebögen zu Themen wie Persönlichkeit, Lebensstil, Stress, Ernährung, körperliche Aktivität, Medikamentenkonsum und sozialökonomischer Status. Weiterhin werden regelmäßig Blutproben entnommenen und in einer Bioprobenbank gelagert. Weitere Informationen im Internet unter http://www.helmholtz.de/forschung/gesundheit/aktuelle_einblicke/archiv_der_einblicke/wer_bleibt_gesund/.
9 Anm. d. Red.: Zuletzt stellten die SPD-Fraktion (BT-Drucksache 17/3868) sowie die Fraktion Bündnis 90/Die Grünen (BT-Drucksache 17/3790) Anträge, die ein solches Gesetz zum Gegenstand hatten. Die Anträge wurden im März 2012 von der Regierungskoalition abgelehnt.

Wolfgang Däubler

Die kontrollierten Belegschaften

1 Die Ausgangssituation

Wer morgens das Betriebsgelände betritt, wird im 21. Jahrhundert nicht mehr von einem Pförtner begrüßt, der die »Zu-Spät-Kommenden« auf einer Liste vermerkt. Heute steckt man einen maschinenlesbaren Ausweis in einen Schlitz. Auf diese Weise wird sekundengenau erfasst, wann beispielsweise die Personalnummer 4713 den Eingangsbereich durchschritten hat.

Am Arbeitsplatz angekommen, wird der PC eingeschaltet. Dies wird genauso erfasst wie das weitere Tun: Mails abgerufen und beantwortet, ein Redemanuskript etwa für den Chef entworfen, im Internet nach einer Zugverbindung gesucht. Dazwischen wird telefoniert – mit welcher Nummer und wie lange wird im Rechner festgehalten. An allen modernen Computern lässt sich eine Kamera aktivieren, die das Gesicht der vor dem PC sitzenden Person zeigt: Ein freudiger Ausdruck spricht dafür, dass sie heute gut drauf ist, eine grimmige Miene eher fürs Gegenteil. Beim Mittagessen wird mit dem Firmenausweis bezahlt. Der Computer »weiß«, dass Person X immer nur das »Diätessen« nimmt, was für eine etwas empfindliche Verdauung spricht. Auch lässt sich unschwer feststellen, wer regelmäßig als nächste oder übernächste Person bezahlt. Auf diese Weise kann ermittelt werden, mit wem X normalerweise zu Mittag isst. Handelt es sich bei ihm etwa um den in der Direktionsetage wenig geschätzten Betriebsratsvorsitzenden, entstehen höchst »interessante« Informationen.

Datenverarbeitung durch die Personalabteilung

Die Personalabteilung verfügt über eine Menge anderer Daten. Das Bewerbungsschreiben ist dort noch vorhanden, gegebenenfalls auch das Abiturzeugnis und das Hochschuldiplom, aber auch jeder Urlaubsantrag befindet sich in der Akte und jede krankheitsbedingte Fehlzeit ist vermerkt. War jemand im Laufe eines Jahres länger als sechs Wochen krank, wird ihm ein »Eingliederungsmanagement« angeboten, das der Krankheit auf den Grund gehen und gegebenenfalls Abhilfe schaffen will. Lässt die betreffende Person sich darauf ein, werden viele Angaben über ihren

Gesundheitszustand, über ihre Lebensgewohnheiten – beispielsweise Rauchen und Trinken – sowie über ihren Ärger am Arbeitsplatz festgehalten. In vielen großen Firmen gibt es die »elektronische Personalakte«[1]: Alle Urkunden werden eingescannt, die übrigen Angaben von vornherein nur elektronisch erfasst. Oft existiert auch ein Nebeneinander von traditioneller und elektronischer Personalakte.

Erkenntnisse aus der Kombination von Beschäftigtendaten

Werden die Daten über die Arbeitstage im Büro und die Daten aus der Personalabteilung zusammengeführt, so kennt man die Stärken und Schwächen der Beschäftigten, ihre Gewohnheiten und ihre Verhaltensweisen in höchst präziser und umfassender Weise. In vielen Betrieben wird das Bild noch sehr viel dichter, die Pixelzahl gewissermaßen noch um einiges höher. In der Produktion lässt sich nicht selten sekundengenau feststellen, wie weit bestimmte Arbeitsprozesse gediehen sind oder wo sich eine bestimmte anzuliefernde Ware gerade befindet. Natürlich ist auch bekannt, wer dafür verantwortlich ist, dass alles reibungslos läuft. Bisweilen werden Videokameras angebracht, die eigentlich vor Diebstahl schützen sollen, die aber ganz nebenbei auch das Arbeitsverhalten erfassen können. Für Außendienst-Mitarbeiterinnen und -Mitarbeiter gibt es »Ortungssysteme«; über → *Global-Positioning-System (GPS)* oder das mitgeführte Handy wird ermittelt, wo sich das Fahrzeug zu einem bestimmten Zeitpunkt befindet. Das lässt Rückfragen zu, an die bisher niemand gedacht hat: Weshalb stand Ihr Fahrzeug eine halbe Stunde lang auf dem Rastplatz rechts neben der Autobahn? Warum haben Sie nicht den direkten Weg zum Kunden gewählt? Was hatten Sie auf dem Supermarkt-Parkplatz zu suchen? Die »Videokamera im Weltraum« macht's möglich.

Einen »gläsernen« Beschäftigten zu schaffen, ist technisch gesehen kein Problem mehr. Die Frage ist nur, ob von dieser Möglichkeit Gebrauch gemacht werden darf oder ob das geltende Recht solche Praktiken verbietet.

2 Rechtliche Grenzen der Überwachung von Beschäftigten

Ein kluger Arbeitgeber oder eine kluge Arbeitgeberin wird von den beschriebenen Möglichkeiten lediglich einen sehr sparsamen Gebrauch machen. Nur wer keinerlei Vertrauen zu seinen Beschäftigten hat, wird die Techniken umfassend einsetzen. Damit ist die Gefahr verbunden, nur

noch völlig »stromlinienförmige« Beschäftigte zu haben, die unter gar keinen Umständen negativ auffallen wollen. Auf Probleme hinzuweisen oder gar bessere Lösungen vorzuschlagen, wird ihnen allzu riskant erscheinen. In einem Callcenter, wo die geführten Telefongespräche an fünf Tagen in der Woche vollständig aufgezeichnet werden, kursierte der Spruch: »Heute ist wieder Stasi-Tag«, weil man per Indiskretion am Morgen erfahren hat, dass mal wieder alles auf Band festgehalten wird. Das schafft jedoch keine konstruktive Arbeitsatmosphäre.

Nun gibt es aber leider keine Sicherheit, dass alle Arbeitgeberinnen oder Arbeitgeber das tun, was eigentlich auch in ihrem eigenen langfristigen Interesse liegt. Vielmehr wird es immer Fälle geben, wo nach dem Motto gehandelt wird: je intensiver die Überwachung, umso stärker der Einsatz des Einzelnen bei der Arbeit. Diese Haltung findet sich insbesondere in Bereichen, wo nur Standardtätigkeiten verlangt werden, bei denen die Motivation der Beschäftigten eine relativ geringe Rolle spielt. Wer nicht »spurt«, kann unschwer durch einen anderen ersetzt werden.

Für die Überwachung im Betrieb gibt es zwei wesentliche rechtliche Grenzen.

Das Persönlichkeitsrecht der Beschäftigten

Zunächst muss das Persönlichkeitsrecht der Beschäftigten respektiert werden. Das Sammeln und Speichern von Informationen über den Einzelnen ist deshalb nicht beliebig zulässig. Vielmehr muss die Arbeitgeberseite das Bundesdatenschutzgesetz (BDSG) beachten, das nach einem Gesetzentwurf der Bundesregierung[2] durch eine Reihe von Sondervorschriften zum Beschäftigtendatenschutz ergänzt werden soll. Durch seinen heutigen § 32 Abs. 2 sind auch handschriftliche Notizen der Arbeitgeberseite und der von ihm Beauftragten erfasst. Dies kann bei Bewerbungs- und Weiterförderungsgesprächen erhebliche Bedeutung gewinnen, da die Betroffenen auf diese Weise auch unsachliche Randbemerkungen zur Kenntnis bekommen können. Der Arbeitsvertrag enthält im Übrigen nach der Rechtsprechung des Bundesarbeitsgerichts (BAG) die stillschweigende Verpflichtung der Arbeitgeberseite, auf die Persönlichkeitssphäre der Beschäftigten Rücksicht zu nehmen.

Darüber hinaus greift in fast allen Fällen der Erfassung und Verarbeitung von Daten ein Mitbestimmungsrecht des Betriebsrats (vgl. auch Abschnitt 4 dieses Beitrags). Dieser muss daher zustimmen, einseitige Handlungen der Arbeitgeberseite sind rechtswidrig und unwirksam. Nur wenn beide Voraussetzungen erfüllt sind – das Verhalten lässt sich nach

dem BDSG rechtfertigen und das Mitbestimmungsrecht des Betriebsrats ist gewahrt – liegt eine rechtmäßige Datenerhebung oder Datenverarbeitung vor.

3 Das Bundesdatenschutzgesetz als Schranke

Nach § 32 Absatz 1 Satz 1 BDSG dürfen Beschäftigtendaten nur dann erhoben, verarbeitet und genutzt werden, wenn dies für die Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses »erforderlich« ist. Andere Beschäftigte wie beispielsweise freie Mitarbeiterinnen und Mitarbeiter, Ein-Euro-Kräfte oder Auszubildende sind gleichgestellt. Es muss ein unmittelbarer Bezug zur Arbeit gegeben sein; was damit nicht in Zusammenhang steht, darf die Arbeitgeberseite nicht interessieren. Dies gilt beispielsweise für Freizeitbeschäftigungen und die familiäre Situation, aber auch für das in der Kantine gewählte Essen. Selbst wenn der Bezug zur übernommenen Tätigkeit da ist, wird verlangt, dass das Informationsinteresse der Arbeitgeberseite schwerer wiegt als der Eingriff in die Persönlichkeitssphäre der Beschäftigten – nur dann ist die Datenverarbeitung »erforderlich«. Daran fehlt es beispielsweise, wenn von Arbeitgeberseite mit Hilfe einer Kamera das Mienenspiel und die Stimmung der Beschäftigten »eingefangen« wird. Dies kann zwar für die Arbeitsorganisation irgendwie nützlich sein, aber die Dauerbeobachtung ist ein zu schwerer, übermäßiger Eingriff in die Sphäre des Einzelnen.

Daten von Bewerberinnen und Bewerbern

Was »erforderlich« ist, wurde im Verhältnis zu Bewerbern und Bewerberinnen bereits zu einer Zeit bestimmt, als es noch nicht einmal den Begriff des Datenschutzes gab. Das BAG entwickelte in den 1950er Jahren den folgenden Grundsatz: Die Arbeitgeberseite darf nur nach solchen Dingen fragen, an deren Kenntnis ein berechtigtes, billigenswertes und schutzwürdiges Interesse besteht. Dies wurde in Bezug auf Vorstrafen konkretisiert: Nur wenn sie sich auf dem in Aussicht genommenen Arbeitsplatz wiederholen können, war die Frage zulässig. Wer sich etwa als Fahrer bewirbt, kann nach Straßenverkehrsdelikten, wer sich als Jugendpfleger betätigen möchte, kann nach Sittlichkeitsdelikten gefragt werden. Ohne Bedeutung war es deshalb, als eine Bewerberin ihre Vorstrafe wegen eines politischen Delikts (konkret: Fortführung des verbotenen sozialistischen Jugendverbands Freie Deutsche Jugend,

FDJ) verschwieg, weil sie lediglich eine völlig unpolitische Tätigkeit bei einer Bausparkasse ausüben wollte.

Schutz vor Diskriminierungen

Unzulässig sind insbesondere Fragen, die nach dem normalen Lauf der Dinge zu einer Diskriminierung führen. Dies gilt etwa für die Frage nach der Schwangerschaft (da sie Frauen benachteiligt), ebenso wie für die nach der Anerkennung als schwerbehinderte Person; die Antwort würde nichts über die tatsächlichen Fähigkeiten des Bewerbers oder der Bewerberin aussagen, aber eine Diskriminierung wegen Behinderung ermöglichen.

In beiden Fällen darf jemand die Unwahrheit sagen, ohne dass die Arbeitgeberseite später den Arbeitsvertrag anfechten kann, weil sie getäuscht worden sei oder sich geirrt habe. Manche sprechen insoweit von einem »Recht zur Lüge«.

Zulässig ist dagegen, die Eignung für den Arbeitsplatz zu ermitteln und dabei auch die gesundheitliche Verfassung des Bewerbers oder der Bewerberin einzubeziehen; selbst wenn sich dabei eine Behinderung herausstellt, könnte sie grundsätzlich berücksichtigt werden. Niemand darf außerdem wegen seiner ethnischen Zugehörigkeit benachteiligt werden; dass etwa jemand türkischer Herkunft ist, darf im Arbeitsleben keine Rolle spielen. In der Praxis dürfte dieser Grundsatz allerdings nicht immer beachtet werden, ist doch die nationale Herkunft häufig schon am Namen erkennbar. Ähnlich verhält es sich mit einem Rückgriff auf soziale Netzwerke wie beispielsweise *Facebook*. Folgt man einer verbreiteten Auffassung in der juristischen Literatur, ist dies nach geltendem Recht nicht erlaubt. Der aktuelle Gesetzentwurf des Bundesinnenministeriums will es jedoch grundsätzlich gestatten. Der praktische Unterschied ist allerdings nicht sehr groß, weil ein Verbot nicht wirklich kontrolliert werden kann: Wie will man beweisen, dass jemand gerade deshalb nicht eingestellt wurde, weil er im Netz etwas provokativ geschrieben hatte, er würde gerne mal eine Veröffentlichung von Bin Laden lesen? Die Personalabteilung wird offiziell nichts über die Recherche im Netz erzählen und einfach zu dem Ergebnis kommen, die Person habe im Vorstellungsgespräch den »weniger überzeugenden« Eindruck gemacht.

Beschäftigtendaten

Im Verhältnis zu Beschäftigten gelten dieselben Grundsätze, soweit ein vergleichbares Informationsbedürfnis besteht. Dies kann insbesondere bei Versetzungen und Beförderungen der Fall sein. Daneben ist die Arbeitge-

berseite verpflichtet, zahlreiche Daten über die Beschäftigten an die Sozialversicherung oder staatliche Stellen zu übermitteln.

Weiter taucht bisweilen das Problem auf, dass Arbeitgeber wissen möchten, ob jemand alkoholkrank oder drogenabhängig ist. Hat dies – was auf Dauer kaum in Betracht kommt – keinerlei Auswirkungen auf die Arbeit, gehört es zur Privatsphäre und bleibt schon deshalb außen vor. Können sich dagegen betriebliche Folgen einstellen, darf gleichwohl nicht jeder, sondern nur derjenige Beschäftigte untersucht werden, bei dem konkrete Verdachtsmomente wie eine »Fahne« oder eine offensichtlich geminderte Reaktionsfähigkeit bestehen.

Die Arbeit im Betrieb gibt die Möglichkeit, dass Beschäftigte nicht nur befragt, sondern dass besondere technische Mittel eingesetzt werden, um ihr Verhalten zu überwachen. Früher hat man beispielsweise sogenannte Einwegscheiben benutzt, die nur den Durchblick in einer Richtung gestatteten: Wer in einer Halle arbeitete, konnte so von einem Beobachtungsposten aus genau ins Visier genommen werden, ohne zu wissen, wann und ob dies gerade zu einem bestimmten Zeitpunkt geschah. Heute werden andere Methoden verwendet, die umfassendere Erkenntnisse ermöglichen.

Videoüberwachung

Besondere Aufmerksamkeit hat die Videokamera gefunden, die sich nicht nur in Supermärkten und Tankstellen findet. Soweit es sich um öffentlich zugängliche Flächen oder Räume handelt, greift § 6b BDSG ein, wonach Daten im Grunde nur zur Abwehr von Straftaten erhoben werden dürfen. Auch müssen sie schnell wieder gelöscht werden. Bei anderen Räumen wie einem Büro oder einer Werkshalle fehlte bislang eine gesetzliche Regelung.

Das BAG hat schon frühzeitig entschieden, dass der Einsatz von Videogeräten nicht allein deshalb erfolgen darf, um »ordentliches Arbeiten« sicherzustellen; dies wäre ein übermäßiger Eingriff in die Persönlichkeitssphäre.

Anders verhält es sich, wenn es um Gefahrenabwehr geht, wenn beispielsweise das Lager durch Videokameras gegen Einbrüche gesichert wird. Dies ist unbestritten legal, wobei die »nebenbei« anfallenden Daten über das Arbeitnehmerverhalten ohne besonderen Grund nicht ausgewertet werden dürfen und auch rasch wieder zu löschen sind. § 32e des Regierungsentwurfs für einen Beschäftigtendatenschutz (BDSG-E) bestätigt dies mittelbar und will gleichzeitig die heimliche Videoüberwachung verbieten.

Überwachung der Kommunikation

Der heimliche Einbau eines Abhörgeräts am Arbeitsplatz ist unzulässig und strafbar, doch ergeben sich im Zusammenhang mit dem Telefonieren und anderen Formen der Telekommunikation (wie dem Versenden und Empfangen von E-Mails) zahlreiche Zweifelsfragen. Während das Erfassen der »äußeren Telefondaten« – das heißt mit welchem Anschluss wurde wann und wie lange telefoniert – in aller Regel bei Dienstgesprächen als unproblematisch angesehen wird, ist dies beim »Mithören« – also der direkten Kenntnisnahme des Inhalts – anders. Es ist nur ausnahmsweise im »überwiegenden Arbeitgeberinteresse« zulässig. Ein solches wurde vom BAG dann angenommen, wenn die ganze Arbeit am Telefon erfolgt und bei neu Eingestellten nur durch Mithören ermittelt werden kann, ob sie in angemessener Weise mit der Kundschaft umgehen und über die nötige Sachkunde verfügen.

Dies ist am Beispiel des Reservierungszentrums einer Fluggesellschaft entschieden worden, gilt aber für alle Callcenter. Eventuell könnte das »Mithören« auch dann erlaubt werden, wenn innerhalb eines kurzen Zeitraums mehrere Beschwerden eingehen und so eine »Qualitätskontrolle« naheliegt. Weiter zu gehen und das Mithören »stichprobenartig oder anlassbezogen« generell zuzulassen, wie dies § 32i Absatz 2 Satz 2 BDSG-E will, ist nicht zu rechtfertigen. Hier hilft auch der obligatorische Hinweis wenig, dass »irgendwann in nächster Zeit« eine Kontrolle stattfinden soll.

Kontrolle von E-Mails und Internetnutzung

Ob dieselben Grundsätze auch für die dienstliche Nutzung von E-Mail und Internet gelten, ist in der Rechtsprechung noch nicht geklärt. Das Telekommunikationsgesetz (TKG) geht von einem einheitlichen »Telekommunikationsgeheimnis« aus, so dass kein Grund für eine Differenzierung besteht. Beispielsweise darf der Chef also nicht einfach die E-Mails des Mitarbeiters lesen, es sei denn, er wäre selbst mit angeschrieben oder auf den Verteiler gesetzt worden. Nicht anders als bei Briefen kann er allerdings verlangen, dass ihm die Korrespondenz vollständig vorgelegt oder per E-Mail weitergeleitet wird.

Private Nutzung von Internet und Telefon am Arbeitsplatz

Soweit privates Telefonieren oder privates Surfen erlaubt ist, sind die dabei anfallenden Daten für den Arbeitgeber tabu. Eine Ausnahme gilt nur für Abrechnungszwecke. Muss der einzelne Beschäftigte die Privatgespräche

bezahlen, können die verbrauchten Gebühreneinheiten festgehalten werden, doch darf die Nummer des Angerufenen nicht vollständig, sondern nur in der Weise gespeichert werden, dass man die drei oder vier letzten Ziffern unterdrückt. Andernfalls wäre das Telekommunikationsgeheimnis verletzt.

Zulässigkeit des Einsatzes von Ortungssystemen

Ob und in welchem Umfang der Einsatz von Ortungssystemen zulässig ist, hat die Rechtsprechung noch nicht entschieden. § 32g BDSG-E will den Einsatz dann erlauben, wenn dies aus bestimmten Anlässen für den betrieblichen Ablauf erforderlich ist und schutzwürdige Interessen des Beschäftigten nicht entgegenstehen. Für Beschäftigte im Außendienst ist eine solche Überwachung mit einem Verlust jener Freiheit verbunden, die diese Tätigkeit für viele attraktiv macht: Bisher sind sie in zeitlicher Hinsicht selbstbestimmt und müssen niemandem Rechenschaft abgeben, weshalb sie etwa beim Kunden X erst nachmittags um halb vier aufkreuzten und außerdem eine etwas ungewöhnliche Route mit dem Auto gewählt haben. Ob es wirklich ein überwiegendes Arbeitgeberinteresse gibt, daran etwas zu ändern, wird man bezweifeln müssen: Wenn es darum geht, mehrere Fahrzeuge zu koordinieren oder kurzfristig umzuleiten, können etwa Handys ausgegeben werden, auf denen die Fahrerinnen und Fahrer jederzeit erreichbar sein müssen.

Diese Techniken stellen nur die wichtigsten Beispiele der Erhebung von Beschäftigtendaten dar. Daneben ist etwa bei der Zugangskontrolle an biometrische Methoden (*fingerprint* oder »Gesichtskontrolle«) zu denken (siehe zu Biometrie auch die Beiträge von Hansen, S. 78 ff. und von Bock, S. 310 ff. in diesem Band). Auch lässt sich der Warenfluss mit Hilfe von →RFID-*Tags* kontrollieren, wobei Lesegeräte festhalten, wann welcher Gegenstand welchen Punkt passiert. Mittelbar werden so auch die dort tätigen Beschäftigten überwacht.

Einwilligung der Betroffenen als Grundlage?

Können Beschäftigte wirksam einwilligen, dass ihre Daten in weiterem Umfang Verwendung finden als es Gesetze und Rechtsprechung zulassen? Können sie bei einer Einstellungsuntersuchung den Arzt oder die Ärztin von der Schweigepflicht entbinden? Kann der Beschäftigte das »Mithören« seiner Gespräche generell erlauben? Die Einwilligung des Betroffenen kann zwar grundsätzlich die Möglichkeiten der Datenverarbeitung

erweitern, doch muss sie nach § 4a BDSG »freiwillig« erfolgen (siehe auch den Beitrag von Hartge in diesem Band, S. 280 ff.). Für Arbeitnehmerinnen oder Arbeitnehmer ist es häufig schwierig, eine von der Arbeitgeberseite gewünschte Einwilligung abzulehnen, weil sie (zu Recht oder zu Unrecht) schlechtere Aufstiegschancen in der Zukunft oder Sanktionen wie Versetzungen befürchten. In aller Regel kann daher nur dann von »Freiwilligkeit« die Rede sein, wenn die Datenverarbeitung den Beschäftigten Vorteile bringt, wenn jemand beispielsweise in die »Nachwuchsförderungsdatei« aufgenommen wird.

Grenzüberschreitende Übermittlung

Besondere Probleme ergeben sich, wenn Daten von Beschäftigten ins Ausland übermittelt werden (siehe auch den Beitrag von Körner in diesem Band, S. 426 ff.). Dies ist insbesondere bei globalen Großkonzernen der Fall. Unproblematisch ist, wenn sich der Empfänger in einem anderen Mitgliedstaat der Europäischen Union (EU) befindet. Da aufgrund der EU-Datenschutzrichtlinie[3] das Datenschutzrecht der einzelnen Länder weitestgehend übereinstimmt, wird nach denselben Grundsätzen wie im Inland verfahren. Es macht also rechtlich keinen Unterschied, ob Daten von Hamburg nach Stuttgart oder von Hamburg nach Lissabon übermittelt werden.

Bei Staaten, die nicht Mitglieder der EU sind (sogenannte Drittstaaten), ist die Sache komplizierter. Soweit ihr Datenschutzniveau von der EU-Kommission als gleichwertig anerkannt ist, gelten dieselben Grundsätze wie innerhalb der EU. Ist diese Voraussetzung nicht gegeben, muss die Aufsichtsbehörde den Datentransfer genehmigen. Davon wird aber eine Ausnahme gemacht, wenn die beteiligten Unternehmen einen Mustervertrag der EU übernehmen, der einen ausreichenden Datenschutz gewährleistet, oder wenn ein internationaler Konzern eine verbindliche Selbstverpflichtung abgibt, ein angemessenes Datenschutzniveau zu praktizieren. Im Verhältnis zu den Vereinigten Staaten von Amerika (USA) gilt die sogenannte → *Safe-Harbor*-Regelung: Hat das Empfängerunternehmen bestimmte Datenschutzgrundsätze anerkannt, wird es wie ein dem EU-Recht unterliegendes Unternehmen behandelt. Andernfalls wird auch hier eine Genehmigung oder eine Abmachung benötigt.

4 Mitbestimmungsrechte des Betriebsrates

Der Betriebsrat hat ein Mitbestimmungsrecht bei der »Einführung und Anwendung technischer Systeme, die dazu bestimmt sind, Verhalten und Leistung der Arbeitnehmer zu überwachen« (§ 87 Absatz 1 Nr. 6 BetrVG). Dabei kommt es nach der Rechtsprechung nicht auf die Kontrollabsicht der Arbeitgeberseite an, da bereits eine bloße »Eignung zur Überwachung« genügt. Soll eine Videoanlage beispielsweise nur gegen Einbruch schützen, ändert dies nichts an der Mitbestimmung, da ja auch das Verhalten von Beschäftigten im Bild festgehalten werden kann. Außerdem ist nicht erforderlich, dass der technische Vorgang selbst zu Aussagen über Verhalten und Leistung führt; es genügt, wenn diese mit Hilfe von sogenanntem Zusatzwissen möglich sind. Wird beispielsweise nur erfasst, dass eine Ware losgeschickt wurde, aber nicht angekommen ist, so genügt es, dass sich aus Schichtplänen, Listen etc. ergibt, wer für den Transport im konkreten Fall verantwortlich war.

Betriebsrat und Arbeitgeberseite müssen verhandeln. Lassen sich Meinungsverschiedenheiten nicht ausräumen, entscheidet eine Einigungsstelle mit einem unparteiischen Vorsitzenden. Handelt die Arbeitgeberseite ohne Zustimmung des Betriebsrats, kann dieser ihr durch einstweilige Verfügung des Arbeitsgerichts untersagen lassen, die fragliche Maßnahme aufrecht zu erhalten. Die Videokamera muss dann wieder abgebaut, das Mithören der Telefongespräche ausgesetzt werden. Um einen solchen Antrag bei Gericht zu stellen, muss der Betriebsrat aber zu einer gewissen Konfrontation mit der Arbeitgeberseite bereit sein. Diese Voraussetzung ist in der Praxis nicht immer gegeben. Auch wird nur etwa die Hälfte aller Beschäftigten durch einen Betriebsrat oder – im öffentlichen Dienst – durch einen Personalrat vertreten, der vergleichbare Befugnisse in diesem Bereich besitzt.

Viele Beschäftigte sind daher nur auf das BDSG verwiesen. Sie werden noch weniger als ein Betriebsrat bereit sein, sich mit der Arbeitgeberseite »anzulegen«. Sie können sich (wie übrigens auch der Betriebsrat) an die Person des oder der betrieblichen Datenschutzbeauftragten wenden, doch sind die Aussichten auf Abhilfe ungewiss: Diese Person ist letztlich von der Arbeitgeberseite eingesetzt, so dass sie vom BAG als dessen »Gewährsmann« bezeichnet wurde (die deshalb die Datenverarbeitung im Betriebsratsbüro nicht kontrollieren darf). Als wirklicher Ausweg steht lediglich die Möglichkeit zur Verfügung, die Aufsichtsbehörde für den Datenschutz einzuschalten (siehe auch den Beitrag von Kamp/Thomé in diesem Band, S. 298 ff.). Sie existiert in jedem Bundesland und muss plausibel darge-

legten Datenschutzverstößen nachgehen. Ihre Verantwortung ist groß: Je gründlicher sie arbeitet, umso stärker wird der Datenschutz in der Praxis an Bedeutung gewinnen.

Anmerkungen

1 Als elektronische Personalakte bezeichnet man Software, mit deren Hilfe Dokumente aus der Personalakte (beispielsweise Atteste) verwaltet werden können.
2 Bundesregierung, Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, BR-Drs. 535/10 vom 3.9.2010. Der Gesetzentwurf (BDSG-E) differenziert zwischen Bewerbern und Beschäftigten sowie zwischen Erhebung und Verarbeitung einschließlich Nutzung von Daten. Seine Verabschiedung ist derzeit (Stand: Juli 2012) ungewiss, zumal das Bundesinnenministerium weitgehende Änderungsvorschläge gemacht hat.
3 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24.10.1995.

Roland Wolf

Beschäftigtendatenschutz ist Teil guter Unternehmensführung

Der Schutz persönlicher Daten von Beschäftigten gehört heute wie selbstverständlich zum Arbeitsrecht. Beschäftigtendatenschutz ist eine Notwendigkeit, ebenso wie die Einhaltung anderer nationaler und internationaler Vorschriften. Schon das bis zum 1. September 2009 geltende Bundesdatenschutzgesetz (BDSG) – ohne die entsprechenden Ergänzungen zum Beschäftigtendatenschutz[1] – bot hierfür eine Grundlage. Alle tatsächlichen oder vermeintlichen Datenskandale, die die Republik im Jahr 2009 bewegt haben, sind unter der Herrschaft des BDSG aufgeklärt worden. Dessen ungeachtet entschieden sich Regierung und Parlament im Sommer 2009 dafür, den Beschäftigtendatenschutz in einer eigenständigen Vorschrift klarzustellen.

Diese Regelung in § 32 BDSG ist jedoch missglückt. Sie bedarf der gesetzlichen Ergänzung und Änderung. Das Vorhaben, klare und rechtssichere Regelungen durch eine Novelle des Bundesdatenschutzgesetzes zu schaffen, ist daher zu begrüßen. Der Gesetzentwurf der Bundesregierung[2] (BDSG-E) aus dem Jahr 2010 in seiner ursprünglichen Fassung verfehlte dieses Ziel.

1 Der geltende Beschäftigtendatenschutz

Die geltende Rechtslage ist für Arbeitgeber, Beschäftigte und Betriebsräte schwer verständlich. Weder Revisions- noch Rechtsabteilungen, weder Datenschutzbeauftragte der Betriebe noch die einzelnen Personalabteilungen können sicher sagen, nach welchen Kriterien sich der Datenschutz im Unternehmen richtet. Dies liegt vor allem an der unklaren Diktion von § 32 BDSG. An wenigen Beispielen sei dies im Folgenden verdeutlicht.

»Erforderlichkeit« der Datenerhebung ist zu unbestimmt

Nach § 32 Absatz 1 BDSG ist eine Datenerhebung, -verarbeitung und -nutzung zulässig, wenn sie erforderlich ist. Was der Gesetzgeber dadurch regeln wollte, ergibt sich nicht eindeutig aus der Norm, sondern aus der

Gesetzesbegründung. Der Begriff der Erforderlichkeit ist dem Grunde nach ein Begriff des öffentlichen Rechts. Erforderlich ist danach das mildeste Mittel, das geeignet ist, um den gewünschten Erfolg zu erzielen. Schon diese Beschreibung zeigt, dass es sich im Regelfall um die Beschreibung eines Eingriffs des Staates gegenüber seinen Bürgern und Bürgerinnen handelt. Dies gilt auch im Datenschutzrecht, soweit es das Verhältnis zwischen Staat und Bürgern betrifft (beispielsweise bei der Telekommunikationsüberwachung). Wo es um das Verhältnis von Vertragspartnern geht, trifft diese Vorstellung jedoch nicht zu. Der Vertrag ist kein Eingriff in Rechtsbeziehungen.

Daher muss der Vertrag die Messlatte für die Rechtmäßigkeit der Datenerhebung, -verarbeitung und -nutzung sein. Die vor dem 1. September 2009 maßgebliche Vorschrift bestimmte, dass Datenerhebung, -nutzung und -verarbeitung der Erfüllung des Vertrages dienen. Dies war deutlich verständlicher, denn es gab den Vertragsparteien Handlungsmuster an die Hand, mit denen sie ihren Vertrag ausgestalten konnten.

Ein Blick in die Gesetzesbegründung zu § 32 BDSG macht schnell deutlich: Dies ist auch weiterhin gemeint. Der Gesetzgeber wollte nur den Grundsatz der Datensparsamkeit nochmals betonen (siehe zum Grundsatz der Datensparsamkeit auch den Beitrag von Heckmann in diesem Band, S. 267 ff.). Dieser Grundsatz ist wichtig und berechtigt. Klarer wäre dies geworden, wenn es an anderer Stelle nochmals herausgestrichen, im Übrigen aber an der bekannten und sinnvollen Wortwahl vor dem 1. September 2009 festgehalten worden wäre.

Verhinderung von Kriminalität und Korruption muss möglich sein

Ebenso umstritten wie die Bedeutung von § 32 Absatz 1 BDSG als Spezialgesetz für die nähere Ausgestaltung des Arbeitsvertrages war lange Zeit die Frage, was hinsichtlich der Kriminalitätsbekämpfung (und noch wichtiger: der Kriminalitäts- und Korruptionsverhinderung) in den Unternehmen zu gelten habe. Mittlerweile dürfte klar sein: Der neu eingefügte § 32 BDSG hat einen engen Anwendungsbereich. Die wichtige Frage der Korruptions- und Kriminalitätsvermeidung richtet sich weiter nach den allgemeinen Vorschriften (insbesondere § 28 Absatz 1 Satz 1 Nummern 2 und 3 BDSG). Diese Klärung war notwendig, weil die Anforderungen an die Verfolgung von Straftaten höher sind als die Anforderungen, die das Gesetz an die Verhinderung von Straftaten stellt. Die im Interesse von Arbeitgeber- und Arbeitnehmerseite notwendige Korruptionsbekämpfung bleibt möglich. Die Unsicherheit zum Beispiel in den Revisions- und/oder

→ *Compliance*-Abteilungen der Unternehmen war und ist aber noch immer groß. Ihr muss durch eine gesetzliche Klarstellung abgeholfen werden.

2 Für ein praktikables, rechtssicheres und zukunftsfähiges Datenschutzrecht

Die Novellierung des Datenschutzes im Arbeitsverhältnis ist daher richtig, darf aber nicht auf Basis eines Missverständnisses geschehen. Die Einhaltung von Gesetzen und die Kontrolle, ob Gesetze und vertragliche Verpflichtungen eingehalten werden (subsumiert unter dem Oberbegriff der → *Compliance*) einerseits sowie die Einhaltung von Datenschutzvorschriften andererseits ist kein Widerspruch. Datenschutz ist Teil unternehmensinterner *Compliance*. Im Rahmen von Überprüfungen muss der Beschäftigtendatenschutz gewährleistet bleiben, er darf die Einhaltung und die Überprüfung der Einhaltung von gesetzlichen und vertraglichen Vereinbarungen und Vorschriften dementsprechend auch nicht behindern; Datenschutz ist kein Täterschutz. Gefordert und notwendig ist vielmehr das harmonische Zusammenspiel von Datenschutz und unternehmensinterner Einhaltung von Normen sowie vertraglichen Bestimmungen.

Dies ist nicht allein ein praktisches, es ist auch ein rechtliches Gebot. Nationale und internationale Vorschriften verlangen von Unternehmen, dass sie sowohl die Einhaltung der von ihnen selbst aufgestellten Regeln als auch staatlich festgelegter Normen überprüfen und kontrollieren. Das gilt nicht nur, aber in besonderer Weise für die Bekämpfung von Korruption. Vor diesem Hintergrund ist daher die Behauptung höchst unredlich und falsch, die Wirtschaft hätte ein Interesse daran, den Beschäftigtendatenschutz gesetzlich nicht zu regeln. Klare, rechtssichere Regelungen sind vielmehr von großem Interesse für Arbeitgeber und Unternehmen. Nur solche Vorschriften bieten die Grundlage für die richtige Anwendung und Auslegung bestehender Vorschriften.

Dem Grunde nach ist es gleichgültig, ob dies in einem eigenständigen Beschäftigtendatenschutzgesetz[3] oder innerhalb des BDSG[4] geschieht. Für die Regelung innerhalb des BDSG spricht allerdings, dass dies die Zahl der Rück- und Querverweisungen deutlich mindern kann. Insbesondere könnten dadurch mehrdeutige, verschiedenartige Interpretationen des Rechts ausgeschlossen werden.

3 Datenschutz ist Teil unternehmensinterner *Compliance*

Vor dem Hintergrund der Notwendigkeit einer rechtsklaren und eindeutigen Regelung des Beschäftigtendatenschutzes, die den Datenschutz als Teil der unternehmensinternen → *Compliance* sicherstellt, wahrt und unterstützt, bedarf der vorliegende Gesetzentwurf der Bundesregierung an verschiedenen Stellen der Nachjustierung und Präzisierung. Die Formulierungshilfen des Bundesministeriums des Inneren (vom 7.9.2011, Anm. d. Red.) gehen daher in die richtige Richtung. Der Entwurf war in seiner ursprünglichen Fassung nicht geeignet, die Anforderungen an ein modernes Datenschutzrecht zu erfüllen. Seine Fortentwicklung im parlamentarischen Verfahren ist daher unverzichtbar.

Betriebsvereinbarung als wichtiges Regelungsinstrument

Auch eine gelungene gesetzliche Regelung vermag häufig nicht ausreichend die betrieblichen Notwendigkeiten und Gegebenheiten abzubilden. Vielfach bedarf sie der Ergänzung durch Betriebsvereinbarungen, die daher im Datenschutz eine besondere Rolle spielen. Schon bisher wurden Kollektivvereinbarungen entsprechend Artikel 2 Einführungsgesetz zum Bürgerlichen Gesetzbuch als Rechtsvorschriften im Sinne von § 4 BDSG angesehen, die ein Abweichen von den Regelungen des BDSG ermöglichen. Formal schien das sogar die vorgesehene Neuregelung zu bestätigen; tatsächlich aber wurde gleichzeitig ein Abweichen von gesetzlichen Vorgaben weitgehend ausgeschlossen. Ist schon diese Art der Gesetzgebung mehr als fragwürdig, sind die Konsequenzen noch gefährlicher. Daher ist es richtig, dass die Formulierungshilfen von dieser Fehlentwicklung Abstand nehmen und die Betriebsvereinbarung in vielen Fällen wieder als Regelungsinstrument für die Praxis vorgesehen werden soll. Ihre praktische Abschaffung in § 32 l BDSG-E hätte die bisherige Praxis faktisch zum Leerlauf gebracht.

Dasselbe gilt für die Einwilligung des einzelnen Arbeitnehmers. Gerade die Einwilligung als privatautonomer Akt ist ein Markenzeichen des Ver-

tragsrechts. Ihr pauschaler weitgehender Ausschluss wäre nicht begründet und würde die Akzeptanz des Datenschutzes durch die Beschäftigten senken, da es sie faktisch entmündigen würde.

Maßnahmen zur Aufdeckung von Straftaten

Sahen die ersten Entwürfe des federführenden Innenministeriums noch vor, dass eine gezielte Videoüberwachung in nicht öffentlich zugänglichen Räumen möglich sein müsse, soll der Arbeitgeberseite dieses Aufklärungsinstrument aus der Hand genommen werden. Eine solche nicht offene Videoüberwachung wird von den Unternehmen schon heute allenfalls dann eingesetzt, wenn eine andere Form der Aufklärung nicht möglich ist, jedoch ein hinreichend konkreter Tatverdacht in einem bestimmten Bereich des Unternehmens – beispielsweise der Kasse – besteht. Das Fehlen anderweitiger Aufklärungsmöglichkeiten kann unterschiedliche Gründe haben. Von der bisherigen Rechtsprechung wurde die verdeckte Videoüberwachung unter diesen engen Voraussetzungen bisher für zulässig erklärt. Liegt ein konkreter Tatverdacht vor und sind andere Aufklärungsmittel erschöpft, sollte diese Form der Überwachung weiter zulässig sein.

Durchgesetzt wurde das Verbot der gezielten Videoüberwachung mit dem Argument, Ruhe-, Schlaf- und andere Sozialräume sollten nicht der Überwachung durch Arbeitgeber offen stehen; dies gilt besonders für Umkleideräume. Die gezielte Videoüberwachung wird damit unzulässigerweise mit Voyeurismus gleichgesetzt. Das Schreckensbild ist der »Chef als Spanner«. Das geht schlicht an der Sache vorbei. Die Videoüberwachung in Umkleidekabinen und dementsprechenden Sozial- und Ruheräumen war schon bisher verboten und sollte auch zu keinem Zeitpunkt durch die Novellierung des Bundesdatenschutzgesetzes zulässig werden. Niemand will Voyeurismus fördern. Warum allerdings die gezielte Videoüberwachung im Lagerraum der Überwachung in der Umkleidekabine gleichgestellt sein soll, ist unverständlich. Es gibt kein Recht auf absolute Intimität in Lagerräumen. Dies ist anerkannt für die offene Videoüberwachung, es muss in schwerwiegenden Verdachtssituationen genauso für die gezielte Videoüberwachung gelten.

Verhinderung von Vertrags- und Gesetzesverstößen

Ob bewusst oder unbewusst lässt der BDSG-E in gefährlicher Weise unbestimmt, was die Verhinderung von Pflicht-, Vertrags- und Gesetzesverstößen anlangt. So soll beispielsweise die nicht offene Datenerhebung, das heißt eine Datenerhebung, von der der Betroffene nichts weiß, nur zulässig sein, wenn

Straftaten oder Pflichtverstöße vorliegen, die eine Kündigung aus wichtigem Grund ermöglichen würden.[5] Auch wenn in den Formulierungshilfen das Tatbestandsmerkmal gestrichen wurde, findet es sich jetzt in der Begründung. Das ist nicht zielführend. Der Begriff der Straftat erschließt sich dem geneigten Leser noch, der schwerwiegende Pflichtverstoß, der eine außerordentliche Kündigung rechtfertigen würde, demgegenüber kaum mehr. Selbst versierte Arbeitsrechtler – seien es Richter, Wissenschaftler, Advokaten, Verbands- oder gar Gewerkschaftsjuristen – können nicht mehr mit hinreichender Sicherheit prognostizieren, wann eine wirksame außerordentliche Kündigung angenommen werden kann.

Datenabgleiche sind notwendig, um Fehlverhalten aufzudecken

Datenanalysen und der Vergleich von Daten sind notwendig, um Fehlverhalten zu erkennen und auf Abhilfe hinzuwirken. Dies geschieht heute schon vielfach automatisiert, ohne dass es zu einer Beeinträchtigung der Persönlichkeit des Betroffenen kommt. Der gezielte Abgleich von Daten ist daher für die Verteidigung der Rechtsordnung auch in Unternehmen unverzichtbar. Ein solcher Datenabgleich muss sowohl präventiv wie repressiv, also zur Aufdeckung wie zur Verhinderung von Pflichtverstößen möglich bleiben.

Um einen zu starken Eingriff in die Rechte der Beschäftigten zu verhindern, kann man erwägen, einen solchen Datenabgleich in einem ersten Schritt →pseudonymisiert durchzuführen und bei der Auflösung von Treffern den Datenschutzbeauftragten hinzuzuziehen. Eine weitere Beschränkung durch Verfahrensvorschriften würde die Bekämpfung von Pflichtverstößen erheblich erschweren.

4 Konzerndatenschutz

Ein Thema, das seit Jahren die wissenschaftliche und praktische Diskussion über den Beschäftigtendatenschutz bestimmt, ist die Frage, wie mit dem Datenschutz in Unternehmensverbänden, insbesondere in Konzernen,[6] umzugehen ist. Es ist erfreulich, dass hier offenbar auch im Bundestag Bewegung in diese wichtige Diskussion gebracht wird. Natürlich stellen sich bei der Thematik viele Fragen, eines ist aber auch sicher: Unternehmen mit engen Verflechtungen handeln nicht wie unverbundene Arbeitgeber. Daher ist es unverzichtbar, eine Regelung zu finden, die einen unbürokratischen Austausch von Beschäftigtendaten in solchen Situationen ermöglicht.

5 Unklare Regelungen beeinträchtigen das Arbeitsverhältnis

Ein guter Beschäftigtendatenschutz ist ein wichtiges Ziel. Die vorstehenden Beispiele, die sich fortsetzen lassen, zeigen die Risiken einer bürokratischen Überregulierung. Die Klarstellung des geltenden Beschäftigtendatenschutzes im Bundesdatenschutzgesetz ist notwendig; er bedarf klarer Konturen. Neue Unsicherheiten, Ungenauigkeiten und Risiken gehen nicht allein zu Lasten der Arbeitgeberseite. Sie gehen ebenso zu Lasten von Beschäftigten und der Rechtssicherheit. Ein moderner Beschäftigtendatenschutz versteht sich als Teil der Unternehmens-*Compliance* und sieht sich zu dieser nicht im Widerspruch. Dies gilt es bei der weiteren rechtspolitischen Diskussion zu berücksichtigen.

Anmerkungen

1 § 32 Abs. 1 Satz 1 BDSG wurde im Jahr 2009 in das BDSG aufgenommen und beinhaltet den Grundsatz: »Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist«.

2 Bundesregierung, Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, BR-Drs. 535/10 vom 3.9.2010; im Internet unter http://www.bundesrat.de/cln_152/nn_6906/SharedDocs/Drucksachen/2010/0501-600/535-10,templateId=raw,property=publicationFile.pdf/535-10.pdf.

3 So wie im Antrag »Gesetzentwurf zum effektiven Schutz von Beschäftigtendaten vorlegen« (BT-Drs. 17/7176) der SPD-Fraktion vom 27.9.2011 vorgesehen.

4 So der Regierungsentwurf zum Beschäftigtendatenschutz (s. Anm. 2).

5 Siehe § 32e Abs. 3 S. 2 BDSG-E.

6 Bei der Datenverarbeitung in Konzernen stehen Fragen der Zulässigkeit und der Grenzen für die Auftragsdatenverarbeitung und die Weitergabe personenbezogener Daten im Vordergrund. Vor allem multinationale Konzerne, in denen sich IT-Abteilungen, konzerneigene Hardware (Speicherort für Daten) oder Personalabteilungen in anderen Ländern als die Beschäftigten befinden, müssen dabei nationales, europäisches und internationales Datenschutzrecht beachten. Die Zulässigkeit der Datenweitergabe hängt stark von der Unternehmensstruktur, der Art der zu verarbeitenden Daten (Personenbezug, Anonymisierbarkeit) und dem datenschutzrechtlichen Status der Drittländer ab.

Martina Perreng

Datenschutz ist ein Grundrecht – auch im Arbeitsverhältnis

Seit den sogenannten Datenskandalen bei mehreren bekannten Unternehmen ist der Beschäftigtendatenschutz zu einem politischen Thema geworden. Zuvor hatten die Gewerkschaften jahrelang erfolglos versucht, gesetzliche Regelungen zum Datenschutz im Arbeitsverhältnis durchzusetzen. Lediglich der Koalitionsvertrag der ersten rot-grünen Bundesregierung aus dem Jahr 1998 enthielt ein solches Vorhaben, das allerdings nicht umgesetzt wurde. Auch auf europäischer Ebene gab es Ende der 1990er Jahre Initiativen, die zum Ziel hatten, verbindliche Vorgaben für gesetzliche Regelungen zum Beschäftigtendatenschutz in den Mitgliedstaaten zu entwickeln. Ein angeblich bereits erarbeiteter Entwurf für eine entsprechende Richtlinie wurde jedoch nie offiziell vorgestellt.

1 Immer weniger Datenschutz im Arbeitsverhältnis

Unter anderem hat das Bundesarbeitsgericht (BAG) geurteilt, dass das Recht auf Schutz personenbezogener Daten als Bestandteil des allgemeinen Persönlichkeitsrechts auch im Arbeitsverhältnis gilt.[1] Das Bundesverfassungsgericht hat außerdem bereits in seinem Volkszählungsurteil[2] betont, dass dem Datenschutz aufgrund der fortschreitenden Technologisierung eine immer größer werdende Bedeutung zukommt und dass dieser besonders gewahrt werden muss (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.). Statt einer Stärkung ist jedoch eine Schwächung des Datenschutzes zu beobachten. Neue Technologien haben dazu beigetragen, dass der Schutz persönlicher Daten insbesondere im Arbeitsverhältnis immer weiter ausgehöhlt wurde. Ein Grund hierfür liegt darin, dass die modernen Kommunikationsmittel ganz neue Möglichkeiten der Überwachung und der Datensammlung bieten.

Hinzu kommt, dass nicht zuletzt aufgrund der Terroranschläge vom 11. September 2001 von staatlicher Seite der Zugriff auf persönliche Daten erheblich erweitert wurde. Im Zusammenhang mit der Terrorbekämpfung sind beispielsweise die Möglichkeiten der Videoüberwachung im öffentlichen Raum sowie die Erfassung von Kontendaten deutlich ausgeweitet

worden. Durch internationale Vereinbarungen hat sich die Bundesrepublik Deutschland außerdem verpflichtet, sogenannte Passagierdaten an die Vereinigten Staaten von Amerika zu übermitteln[3] und in bestimmten, sogenannten sicherheitsrelevanten Bereichen, Beschäftigte überprüfen zu lassen.

Durch diese Entwicklungen ist ein gesellschaftliches Klima entstanden, in dem das Recht auf Privatsphäre hinter vermeintlichen oder tatsächlich vorhandenen höherrangigen Interessen des Staates oder der Allgemeinheit zurücktritt.

2 Datenschutz ist in vielen Unternehmen zweitrangig

Dieses gesellschaftliche Klima bleibt nicht ohne Wirkung auf den Datenschutz im Arbeitsverhältnis.

Zum einen bieten die gesteigerten technischen Möglichkeiten auch in der Arbeitswelt zahlreiche Gelegenheiten, Daten zu erheben, zu speichern und zu verwenden. Zum anderen bewirken das gesellschaftliche Klima einer vermeintlichen oder tatsächlichen Überwachungsnotwendigkeit und eine allgemeine Achtlosigkeit im Umgang mit Daten, dass sämtliche technischen Möglichkeiten zur Überwachung und Kontrolle auch tatsächlich ausgeschöpft werden.

Ob die persönlichen Daten der Beschäftigten tatsächlich notwendig sind, um einen Betrieb zu führen, ist in diesem Zusammenhang oft zweitrangig. Der Grundrechtsschutz scheint grundsätzlich bedeutungslos. Nur so ist es auch zu erklären, dass es überhaupt zu den sogenannten Datenskandalen gekommen ist. Durch die Presse wurde bekannt, dass in mehreren deutschen Unternehmen beispielsweise folgende Maßnahmen zur Überwachung unrechtmäßig durchgeführt wurden:

- massenhafte Datenabgleiche,
- Abhören von Telefonaten,
- Überwachung von Beschäftigten, um Diebstähle zu verhindern,
- Bluttests.

Diese Vorfälle sind jedoch nur Beispiele für eine grundsätzliche Haltung: Es scheint ein Grundbedürfnis vieler Arbeitgeber zu sein, so viele Informationen wie nur irgend möglich über Beschäftigte zu sammeln. Nicht vertrauensvoller Umgang, sondern Totalkontrolle scheint in vielen Unternehmen das Ziel zu sein. Dass einige der Unternehmen scheinbar einsichtsvoll ihr Verhalten geändert und ausgezeichnete betriebliche Vereinbarungen zu einem wirksamen Persönlichkeitsschutz im Arbeitsverhältnis

entwickelt haben, darf nicht darüber hinwegtäuschen, dass die Mehrheit der Unternehmen, vor allem dort, wo es keine Betriebs- und Personalräte gibt[4], dem Datenschutz im Arbeitsverhältnis bestenfalls eine untergeordnete Rolle einräumt.

3 Forderungen für transparenten Beschäftigtenschutz

Ein Grund für die zahlreichen Verletzungen des Datenschutzes in vielen Unternehmen ist die völlig unzureichende gesetzliche Regelung des Beschäftigtendatenschutzes. Das Bundesdatenschutzgesetz (BDSG) ist zwar im Prinzip auf das Arbeitsverhältnis anwendbar und es existiert eine differenzierte Rechtsprechung in diesem Bereich, die bestehende Rechtslage ist jedoch nicht transparent.

Sowohl für die Arbeitgeberseite als auch für Beschäftigte und Betriebsräte sind die Regelungen nur schwer zu handhaben. Deshalb wären transparente Vorschriften in einem eigenständigen Gesetz dringend notwendig.

Ein wirksames Beschäftigtendatenschutzgesetz müsste insbesondere nachfolgend aufgeführte Vorschriften enthalten.

Verbot der gezielten Beobachtung und Überwachung

Der Begriff der Überwachung sollte in diesem Zusammenhang weit zu verstehen sein. Folgende Maßnahmen sollten insbesondere verboten werden:

- Video- und Tonaufnahmen,
- direktes Ausspähen,
- Abgleich von Daten (insbesondere von Daten, die zum persönlichen Bereich gehören wie Kontonummern oder der Postverkehr),
- Kontrolle von Telefongesprächen,
- Erstellen von Bewegungsprofilen.

Nur wenn der begründete Verdacht einer strafbaren Handlung oder einer schwerwiegenden Schädigung der Interessen des Unternehmens vorliegt oder bei einer konkreten Gefährdung könnte eine Überwachung im Einzelfall zulässig sein. Dies setzt auch voraus, dass ein Eingreifen von Polizei und Staatsanwaltschaft nicht möglich oder nicht zumutbar ist. Eine solche Überwachung bedürfte zusätzlich der Zustimmung der betrieblichen Interessenvertretung und des betrieblichen Datenschutzbeauftragten. Der Eingriff in das allgemeine Persönlichkeitsrecht müsste also so gering wie möglich gehalten werden.

Verbot des Zugriffs auf Kommunikationsdaten

Wichtig ist, dass Beschäftigte vor einer ausufernden Überwachung ihrer Kommunikation geschützt werden. Eine Ausnahme würde auch hier einen konkreten Missbrauchsverdacht voraussetzen. Ein Beispiel dafür wäre, dass sich jemand Zugang zu rechtsextremen Webseiten über den Server des Arbeitgebers verschafft.

Ebenso müsste die Kontrolle der Kommunikation unter Beteiligung der betrieblichen Interessenvertretung erfolgen.

Fragerecht der Arbeitgeberseite und medizinische Untersuchungen

Personen, die sich um einen Arbeitsplatz bewerben, sollen davor geschützt werden, dass ihnen im Rahmen des Bewerbungsverfahrens Fragen gestellt werden, die in einer Bewerbungssituation grundsätzlich unzulässig sind (so zum Beispiel die Frage nach einer möglichen Schwangerschaft). Es sollte daher der Grundsatz gelten, dass nur tätigkeitsbezogene Fragen zulässig sind. Alle Fragen, die das private Leben des Bewerbers oder der Bewerberin betreffen, sollten verboten sein. Darüber hinaus sollte die Person, die sich um eine Stelle bewirbt, das Recht haben, unzulässige Fragen falsch zu beantworten, ohne negative Konsequenzen befürchten zu müssen.

Ärztliche Untersuchungen sollten nur im Rahmen von sogenannten Schutzgesetzen (beispielsweise nach dem Jugendarbeitsschutzgesetz), also zum Schutz der potentiellen Beschäftigten, zulässig sein. Das grundsätzliche Verbot ärztlicher Untersuchungen müsste ausdrücklich auch die Entgegennahme von »unverlangt« überlassenen Untersuchungsdaten umfassen. Drogen- und Alkoholtests sollten nur angeordnet werden, wenn konkrete Anhaltspunkte für einen Missbrauch vorliegen und der Missbrauch zu einer Gefährdung des Unternehmens führen könnte.

Besondere Vorschriften für Beschäftigte, die gleichzeitig zur Kundschaft der Arbeitgeberseite gehören

Ein besonderes datenschutzrechtliches Problem tritt auf, wenn eine Person nicht nur Beschäftigte, sondern gleichzeitig auch Kundin eines Unternehmens ist (wie etwa Beschäftigte eines Krankenhauses als Patienten, Beschäftigte einer Bank als Bankkundinnen und -kunden).

In diesen Fällen wird eine Fülle unterschiedlicher Daten über die betreffende Person erhoben. Zum Beispiel würde die Bank Informationen darüber führen, wie viel Geld eine Angestellte auf ihrem Konto hätte. Daher müssten insbesondere Vorschriften über die Verwahrung und den Zugang zu deren Kundendaten geschaffen werden. Nur so würde verhindert, dass sich die Arbeitgeberseite unzulässigerweise Informationen verschafft, die mit dem Arbeitsverhältnis in keinem Zusammenhang stehen (zum Beispiel über den Kontostand der Angestellten).

Verbandsklagerecht zur besseren Rechtsdurchsetzung

Zur Wahrung der Rechte der Beschäftigten müsste ein Verbandsklagerecht[5] eingeführt werden. Es ist derzeit nicht zu erwarten, dass allzu viele Beschäftigte ihr Recht auf Wahrung des allgemeinen Persönlichkeitsrechts selbst gerichtlich geltend machen, da sie befürchten, dass sie durch eine Klage ihren Arbeitsplatz verlieren könnten.

Schadensersatz und Strafbarkeit

Außerdem müsste ein Anspruch auf Schadensersatz gesetzlich geregelt werden, wenn durch die Verletzung der Verbote materieller Schaden entstanden ist. So etwa, wenn eine Person im Einstellungsgespräch eine von der Arbeitgeberseite gestellte unzulässige Frage wahrheitsgemäß beantwortet hat und sie daraufhin die gewünschte Stelle nicht bekommt.

Daneben müssten Entschädigungsansprüche (Schmerzensgeld) in das Gesetz aufgenommen werden, die so hoch sind, dass sie eine »abschreckende« Wirkung entfalten.

Und schließlich: Die Verletzung der gesetzlichen Vorschriften zum Beschäftigtendatenschutz müsste als Straftatbestand aufgenommen werden. Nur so kann sichergestellt werden, dass Datenschutz in den Unternehmen genügend Beachtung findet.

4 Gesetzliche Neuregelung sollte eigenständig sein

Die oben genannten Regelungen stellen Forderungen dar, die die Rechte der Beschäftigten stärken sollen. Von all dem sind wir jedoch weit entfernt. Es war zwar ein richtiger Schritt, dass die Politik unter der Federführung des damaligen Bundesinnenministers Wolfgang Schäuble entschieden hat, gesetzliche Regelungen zu schaffen, die den Datenschutz im Arbeitsverhältnis verbessern sollen. Ob der neu geschaffene § 32 BDSG[6] hierbei hilfreich ist oder nicht, wurde in der Fachliteratur eifrig diskutiert. Eins steht jedoch fest: Bereits mit § 32 BDSG wurde deutlich gemacht, dass die Datenerhebung, -verwendung und -speicherung im Arbeitsverhältnis besonderen Bedingungen unterworfen ist und nur eingeschränkt zulässig sein kann.

Alle Beteiligten am damaligen Verfahren waren sich aber auch darüber einig, dass es bei dieser Neuregelung nicht bleiben sollte. Ein im Bundesministerium für Arbeit und Soziales erarbeiteter Entwurf, der in die richtige Richtung ging, konnte in der letzten Legislaturperiode nicht mehr in den Bundestag eingebracht werden. Richtig wäre es gewesen, dem damaligen Ansatz zu folgen und den Beschäftigtendatenschutz in einem eigenständigen Gesetz zu regeln, statt das BDSG zu ergänzen. Sicherlich hätte ein solches Gesetz einige Verweise auf das BDSG enthalten müssen. Eine eigenständige gesetzliche Regelung wäre jedoch transparenter gewesen und hätte Wertungswidersprüche verhindern können, die durch eine Regelung innerhalb des BDSG zwangsläufig entstehen.

Mangelnde Freiwilligkeit der Einwilligungen im Arbeitsverhältnis

Als Beispiel für solche Wertungswidersprüche sei die Einwilligung der Beschäftigten als Rechtfertigung für Datenerhebung, -verwendung und -speicherung genannt. Im allgemeinen Datenschutzgesetz ist geregelt, dass Personen freiwillig in die Verarbeitung persönlicher Daten einwilligen können.[7] Dies hat zur Folge, dass die Verarbeitung der Daten rechtmäßig ist. Die Einwilligung stellt einen sogenannten Erlaubnistatbestand dar (siehe auch den Beitrag von Hartge in diesem Band, S. 280 ff.).

Im Arbeitsverhältnis kann die Einwilligung der Beschäftigten jedoch keine Datenverarbeitung rechtfertigen, oder mit anderen Worten: erlauben. Aufgrund der Abhängigkeit im Arbeitsverhältnis und der strukturellen Unterlegenheit der Beschäftigten kann von einer Freiwilligkeit der Einwilligung, die die Arbeitgeberseite verlangt, im Prinzip nie ausgegangen werden. Beschäftigte werden tendenziell

immer in Datenerhebungen einwilligen. Denn sie müssen befürchten, dass sie andernfalls ihren Job verlieren.

5 Gesetzentwurf zum Beschäftigtendatenschutz darf nicht die Arbeitgeberseite bevorzugen

Gleichwohl hat sich die Bundesregierung im Jahr 2010 dafür entschieden, in einer erheblichen Ergänzung des § 32 BDSG Regelungen zum Beschäftigtendatenschutz zu schaffen. Doch bereits der Ansatz dieses Entwurfs[8] (BDSG-E) ist falsch. Sowohl im Koalitionsvertrag als auch in der Gesetzesbegründung kann man nachlesen, dass beabsichtigt wurde, mit dem BDSG-E einen Ausgleich zwischen den Interessen der Arbeitgeberseite, die in der Korruptionsbekämpfung und der Einhaltung von → *Compliance*-Anforderungen bestehen, und den Interessen der Beschäftigten an der Wahrung ihres Rechts auf informationelle Selbstbestimmung zu schaffen. Bereits aus dieser Formulierung geht die Schieflage des BDSG-E eindeutig hervor: Nicht dem Grundrechtsschutz wird Vorrang gegeben, sondern der Grundrechtsschutz wird mit den (wirtschaftlichen) Interessen der Unternehmen und Betriebe gleichgestellt.

Aber nicht einmal dieser Gleichrang findet sich im Gesetzestext wieder. Tatsächlich geht es in diesem Entwurf vor allem darum, den Grundrechtsschutz von Beschäftigten einzuschränken und der Arbeitgeberseite weitgehende Befugnisse zur Datenerhebung, -speicherung und -verwendung einzuräumen. Dies soll anhand von Beispielen verdeutlicht werden:

- **Fragerecht**
  Der Arbeitgeberseite wird unter anderem ein weitgehendes Fragerecht bei der Einstellung eingeräumt – sogar Fragen nach einer Schwangerschaft und ganz allgemein nach der Gesundheit sind zugelassen, wenn die Arbeitgeberseite sie für erforderlich hält.
- **Daten von Bewerberinnen und Bewerbern**
  Internetrecherchen über Bewerberinnen und Bewerber sowie Nachfragen bei Dritten werden erlaubt. Im allgemeinen Datenschutzrecht (also im BDSG) gilt jedoch der Grundsatz der Direkterhebung, das bedeutet, dass Menschen selbst Informationen über sich preisgeben sollen und nicht Dritte.
- **Ärztliche Tests**
  Ärztliche Untersuchungen können im laufenden Arbeitsverhältnis angeordnet werden. Es genügt, dass die Arbeitgeberseite Zweifel an der dauerhaften Eignung der Person für die Tätigkeit behauptet. Und wer sollte diese Zweifel widerlegen?

- **Screenings und umfassende Überwachung**
  Der anlasslose Abgleich von Beschäftigtendaten soll ebenso zulässig sein wie eine fast unbeschränkte (verdeckte) Videoüberwachung, wenn von Arbeitgeberseite nur auf den Umstand hingewiesen wird, dass im Betrieb Videoüberwachung stattfindet. Dies kann etwa durch ein Schild am Eingang erfolgen.

6 Grundrechtsschutz muss angemessene Bedeutung erhalten

Damit aber nicht genug: Die Politik diskutiert über weitere Einschränkungen des Grundrechts auf informationelle Selbstbestimmung im Beschäftigungsverhältnis. So gibt es Überlegungen, Betriebsvereinbarungen auch zur Verschlechterung des gesetzlichen Standards zuzulassen und die individuelle Einwilligung als Rechtfertigung für Datenerhebung, -verwendung und -speicherung ausdrücklich zuzulassen. Betriebsvereinbarungen können jedoch nicht über höchstpersönliche Rechte[9] verfügen. Hinzu kommt, dass der Betriebsrat und die Arbeitgeber nicht auf Augenhöhe verhandeln. Betriebsräte sind nur in einem eng begrenzten Rahmen und mit Hilfe von Einigungsstellen in der Lage, die Rechte der Beschäftigten durchzusetzen.

Arbeitnehmerdatenschutz hat längst nicht den Stellenwert, den er haben müsste. Es wäre Aufgabe des Gesetzgebers, dafür zu sorgen, dass der Grundrechtsschutz im Arbeitsverhältnis endlich eine angemessene Bedeutung erhält. Der Gesetzesentwurf der Bundesregierung ist aber der falsche Ansatz. Er stellt den Grundrechtsschutz hinter die Interessen der Arbeitgeber und bleibt in weiten Teilen hinter der Rechtsprechung des BAG zurück.

Anmerkungen

1 Urteil 1 ABR 43/81 vom 6.12.1983.
2 BVerfGE 65,1; Az. 1 BvR 209/83 u. a.
3 Diese Verpflichtung ergibt sich aus dem sogenannten *Passenger Name Record* (PNR)-Abkommen mit den Vereinigten Staaten von Amerika (USA). Die Europäische Union hat sich darin im Jahr 2007 verpflichtet, die Namen von Flugreisenden in die USA an dortige Behörden zu übermitteln. Im Jahr 2011 fand eine Überarbeitung des ursprünglichen Abkommens statt, in dem auf Kritik der Datenschutzbeauftragten hin Vorschriften über die Speicherdauer aufgenommen wurden. Das Abkommen wurde im Frühjahr 2012 erneuert.

4 Nur in etwa der Hälfte der deutschen Unternehmen gibt es Betriebsräte, denn zur Einführung eines Betriebsrates besteht gesetzlich keine Pflicht.
5 Eine Verbandsklage erlaubt es bestimmten Interessenvertretern, eine Klage zu erheben, obwohl diese nicht selbst betroffen sind. Verbandsklagen stellen somit eine Ausnahme von dem Grundsatz dar, dass man vor Gericht nur die Verletzung eigener Rechte einklagen kann.
6 § 32 Abs. 1 S. 1 BDSG normiert folgenden Grundsatz: »Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist.« Diese Vorschrift wurde 2009 in das BDSG aufgenommen.
7 § 4a BDSG.
8 Bundesregierung, Entwurf eines Gesetzes zur Regelung des Beschäftigtendatenschutzes, BR-Drs. 535/10 vom 3.9.2010, im Internet unter http://www.bundesrat.de/cln_152/nn_6906/SharedDocs/Drucksachen/2010/0501-600/535-10,templateId=raw,property=publicationFile.pdf/535-10.pdf.
9 Höchstpersönliche Rechte sind solche Rechte, die man nur persönlich und nicht durch einen Vertreter ausüben kann.

Jan-Hinrik Schmidt

Persönliche Öffentlichkeiten und informationelle Selbstbestimmung im *Social Web*

Viele der gegenwärtigen Debatten um Datenschutz, informationelle Selbstbestimmung und die verschwimmenden Grenzen zwischen Privatsphäre und Öffentlichkeit lassen sich auf Entwicklungen im Bereich der *online*-basierten Kommunikation zurückführen, die mit der Chiffre → Web 2.0 zusammengefasst werden. Dies umfasst so unterschiedliche Anwendungen wie die → *Wikipedia*, *YouTube,* → *Blogs,* → *Twitter, Facebook* oder studiVZ (vgl. → *Social Media*). Ihnen gemeinsam ist, dass sie bestimmte Nutzungsweisen unterstützen. Genauer gesagt, sie senken die technischen Hürden dafür, sich mit den eigenen Interessen, Erlebnissen, Kompetenzen oder Meinungen zu präsentieren, soziale Beziehungen zu pflegen und neu zu knüpfen sowie gemeinsam mit anderen Informationen, Kultur- und Wissensgüter aller Art zu bearbeiten, zu teilen und zu verbreiten.

Dieser Beitrag[1] diskutiert die Verbindungen zwischen dem Web 2.0 und Fragen des Datenschutzes sowie der informationellen Selbstbestimmung aus einer kommunikationssoziologischen[2] Perspektive, die die Nutzung von Medien in ihrem gesellschaftlichen Kontext betrachtet. Dazu wird in einem ersten Schritt am Beispiel von → Netzwerkplattformen gezeigt, wie die Kombination von spezifischen Nutzungsweisen und kommunikationstechnischer Architektur zur Entstehung eines neuen Typs von Öffentlichkeit führt. In einem zweiten Schritt wird diskutiert, welche Herausforderungen sich daraus für Datenschutz und informationelle Selbstbestimmung ergeben.

1 Praktiken des Web 2.0

Je nach technischen Optionen und Spielräumen der *Online*-Anwendungen sowie je nach kommunikativen Bedürfnissen gibt es teils erhebliche Unterschiede in der Nutzung des Internets. Das Einstellen eines Videos auf *YouTube* ist etwas anderes als das Recherchieren in der → *Wikipedia*, der Austausch via E-Mail unterscheidet sich von Konversationen über einen → *Messenger*-Dienst (wie zum Beispiel *ICQ*) oder im Kommen-

tarbereich eines → *Weblogs*. Allerdings lassen sich drei zentrale Facetten solcher Nutzungspraktiken unterscheiden, die anwendungs- und nutzungsübergreifend auftreten und mit grundlegenden Orientierungen und Handlungsanforderungen korrespondieren, die nicht auf das Internet beschränkt sind.[3]

Identitäts-, Beziehungs- und Informationsmanagement

- Praktiken des *Identitätsmanagements*, die Bestandteil der Selbstauseinandersetzung einer Person sind: Das Darstellen, wer jemand ist und was eine Person ausmacht, aber auch das Erkunden von und Experimentieren mit Lebens- und Biographieentwürfen.
- Praktiken des *Beziehungsmanagements*, die Bestandteil der Sozialauseinandersetzung einer Person sind: Die Pflege bestehender und das Knüpfen neuer Beziehungen, über die Menschen ihre eigene Position im sozialen Gefüge einer Gesellschaft finden und etablieren, beispielsweise die Zugehörigkeit zu spezifischen Subkulturen oder Lebensstilgemeinschaften.
- Praktiken des *Informationsmanagements*, die Bestandteil der Sachauseinandersetzung einer Person sind: Das Orientieren in der Welt, indem persönlich relevante Informationen aufgefunden und übernommen sowie in bestehende Wissensbestände eingeordnet werden, aber auch das Teilen und Erweitern dieser Wissensbestände mit anderen.

Diese drei Handlungsweisen sind auch von Bedeutung für die Grenzziehung zwischen Privatsphäre und Öffentlichkeit, was sich gerade am Beispiel von →Netzwerkplattformen wie *Facebook*, studiVZ, Lokalisten, *XING* oder Wer-kennt-wen näher verdeutlichen lässt. Diese Art von Internet-Anwendung, auch als *Social Network Site*, »Soziales Netzwerk« oder »*Community*-Plattform« bekannt, ist erst vor wenigen Jahren populär geworden, gilt aber inzwischen als prototypische Anwendung des Web 2.0 (siehe auch den Beitrag von Wagner/Gebel/Brüggen in diesem Band, S. 226 ff.).

Präsentation und Selbstoffenbarung auf Profilseiten

Netzwerkplattformen basieren darauf, dass Menschen Aspekte ihrer selbst auf einer Profilseite zugänglich machen, also zum Beispiel Namen und Wohnort, oder auch musikalische Vorlieben, politische Orientierungen oder Freizeitinteressen. Diese Preisgabe von Facetten der eigenen Person – psychologisch auch als Selbstoffenbarung bezeichnet – lässt sich als Aus-

druck des Identitätsmanagements verstehen, weil die Nutzenden durchaus bewusst gestalten können, welche Informationen sie zugänglich machen, beispielsweise:

- Welches Foto wähle ich als Profilbild?
- Wie viele und welche Kontaktinformationen stelle ich ein?
- Welchen thematischen Gruppen – die anschließend auch auf meinem Profil angezeigt werden – trete ich bei?

Diese Formen des Identitätsmanagements über Profilangaben werden von den jeweiligen Plattformvorgaben zu einem gewissen Grad gerahmt: Eine Plattform wie *XING* beispielsweise, die sich auf die berufliche Selbstdarstellung spezialisiert, macht in der Profilmaske andere Vorgaben (beispielsweise berufliche Kenntnisse oder bisherige Arbeitgeber) als etwa die Plattform studiVZ, die sich an junge Erwachsene richtet, die unter anderem Angaben zu ihrem Studienfach und belegten Vorlesungen machen können. Dadurch werden jeweils andere Handlungssphären nahegelegt – hier berufliches kontra studentisches Umfeld – die auch Erwartungen an eine angemessene Form der Selbstpräsentation beinhalten. Das Identitätsmanagement auf Netzwerkplattformen erfordert also zumindest einen gewissen Grad an Reflexion, welche Personenkreise dort adressiert werden.

Authentizität als Leitbild in Netzwerkplattformen

Die selektive Preisgabe von Informationen für bestimmte Personenkreise bleibt aber nach wie vor an die »echte Identität« gekoppelt. Anders als in der Anfangszeit des Internets, als Vorstellungen von → *Virtual Reality* und → *Cyberspace* nahelegten, dass Menschen *online* ihren Körper hinter sich lassen und in komplett neue Identitäten schlüpfen könnten, gilt auf den Netzwerkplattformen wie in vielen anderen Web 2.0-Anwendungen Authentizität als Leitbild. Das absichtlich auf Täuschung angelegte Fake-Profil gilt daher als Abweichung. Menschen treten unter ihrem echten Namen auf, und sie geben (in unterschiedlichem Umfang) personenbezogene Daten von sich preis, weil sie mit anderen Personen kommunizieren, auffindbar für Freundinnen und Freunde sowie Bekannte sein, und unter Umständen auch neue Personen kennenlernen möchten, die ähnliche Interessen teilen. Anders ausgedrückt: Das Identitätsmanagement ist somit nicht vom Beziehungsmanagement zu trennen, genauso wie die eigene persönliche Identität nicht von der Einbettung in soziale Beziehungen zu trennen ist, sondern erst im Wechselspiel von individuell-persönlichen Merkmalen und sozialen Zugehörigkeiten entsteht.

Das Internet verändert Gruppenbildungen

Sowohl die Formen, in denen sich gesellschaftliche Gruppen organisieren, als auch die sozialen Zusammenhänge, in denen Menschen ihre Identität herausbilden, haben sich im Laufe der letzten Jahrzehnte grundlegend verändert. Zeitlich stabile, auf Traditionen gegründete und oft örtlich gebundene Gruppen – man denke beispielsweise an das Arbeitermilieu oder das katholische Milieu – haben gegenüber flexiblen, interessengeleiteten und ortsübergreifenden Bindungen relativ gesehen an Gewicht verloren.

Das Internet ist für diesen tiefgreifenden sozialen Wandel nicht ursächlich verantwortlich (denn er hat schon deutlich früher eingesetzt), unterstützt diese Entwicklungen aber und trägt zu ihrer Beschleunigung bei. Gerade Netzwerkplattformen versetzen Menschen in die Lage, solche sozialen Beziehungen zu pflegen und aufrecht zu erhalten, die über den Kreis der engen Freundschaften hinausgehen, ohne deswegen beliebig zu sein: ehemalige Klassenkameraden, frühere Nachbarn, Bekannte aus dem Sportverein oder Kirchenchor, berufliche Kontakte oder auch bislang persönlich Unbekannte, mit denen man aber ein bestimmtes Hobby teilt.

Es ist dieses erweiterte soziale Netzwerk, das Menschen auf Plattformen wie *Facebook* oder Wer-kennt-wen abbilden können – und nur so ist zu erklären, dass beispielsweise zwölf- bis 24-jährige Nutzende von Netzwerkplattformen bei einer repräsentativen Umfrage Ende 2008 angaben, im Durchschnitt 130 Kontakte auf der von ihnen meist genutzten Plattform zu haben.[4] Auch wenn die Software diese Kontakte als »Freunde« bezeichnet, handelt es sich nur bei einem kleinen Anteil um enge soziale Beziehungen; die Mehrzahl dieser Kontakte sind zwar persönlich bekannt, aber eben auf einem Spektrum der sozialen Nähe angesiedelt, das von guten Bekannten über Freunde von Freunden bis zu Menschen reicht, die man zufällig bei einer Party, einem Konzert oder einer anderen gemeinsamen Aktivität getroffen hat.

2 Persönliche Öffentlichkeiten

Die beschriebenen Merkmale von Identitäts- und Beziehungsmanagement im Web 2.0 – die Präsentation von Facetten der eigenen »echten« Identität für einen Kreis von Personen, die zum überwiegenden Teil nicht völlig unbekannt sind – lassen einen neuartigen Typ von Öffentlichkeit entstehen, den man als »persönliche Öffentlichkeit« bezeichnen kann. Er unterscheidet sich in dreierlei Hinsicht von den journalistisch hergestellten massenmedialen Öffentlichkeiten:

Persönliche Relevanz: Informationen werden dort nach Kriterien der persönlichen Relevanz ausgewählt, anstatt nach journalistischen Nachrichtenfaktoren, die auf die gesellschaftliche Relevanz eines Themas abzielen.

Ein Publikum, das aus sozialen Kontakten besteht: Die Nutzenden richten sich – zumindest ihrer Intention nach (siehe unten) – an ein Publikum, das aus sozialen Kontakten besteht, anstatt an das verstreute, unbekannte, unverbundene Publikum, das die Massenmedien adressieren.

Modus des »Konversation Betreibens«: In persönlichen Öffentlichkeiten wird im Modus des »Konversation Betreibens« kommuniziert, also um Dialog, Austausch oder Feedback zu erhalten, anstatt den eher in eine Richtung verlaufenden Modus des »Publizierens« zu wählen. Die Trennung zwischen »Sender«- und »Empfänger«-Rollen, die die Massenkommunikation ausmachen, wird dadurch tendenziell aufgehoben.

Kommunikative Architektur persönlicher Öffentlichkeiten

Neben diesen kommunikationssoziologischen Merkmalen sind persönliche Öffentlichkeiten zusätzlich noch durch eine bestimmte »kommunikative Architektur« gekennzeichnet, die sich auf Merkmale der zugrundeliegenden und die Kommunikation erst ermöglichenden Software gründet. Zwar existieren zahlreiche, auch grundlegende Unterschiede in der Funktionsweise und den zur Verfügung gestellten Optionen und Limitationen, beispielsweise zwischen verschiedenen Netzwerkplattformen, oder auch zwischen → *Weblogs* einerseits und → *Microblogs* (wie etwa → *Twitter*) andererseits. Dennoch lassen sich einige übergreifende Gemeinsamkeiten identifizieren.

Dazu gehört erstens, dass viele der gegenwärtig populären Anwendungen auf Metaphern wie dem *Stream*[5] oder dem → *Feed* aufbauen: Sie liefern konstante und hoch dynamische Informationsflüsse, die aus der Zusammenführung von zahlreichen individuellen Status-Updates, *Twitter*einträgen oder Blogeinträgen entstehen. In dem Maße, wie Nutzende sich ihre Quellen zum Beispiel durch die gezielte Auswahl von abonnierten → *RSS-Blog-Feeds* oder anderen *Twitter-Accounts* selbst zusammenstellen, entwickeln sie auch ein höchst personalisiertes System von Informationsfiltern. Es bietet einen Einblick in das *Real-Life-Web*, also in die (nahezu) in Echtzeit geäußerten Eindrücke, Meinungen, Neuigkeiten oder Empfehlungen von Menschen (oder auch Marken, Unternehmen oder politischen Parteien).

Zweitens zeichnet sich die Architektur von persönlichen Öffentlichkeiten durch bestimmte Merkmale aus, die sie mit anderen Formen *online-*

basierter Kommunikation gemeinsamen haben.[6] Sie sind dauerhaft, weil Texte oder Fotos, Kommentare oder Meinungen auch Tage, Wochen oder Jahre später noch abrufbar sind. Sie sind kopierbar, weil die in digitaler Form vorhandenen Texte, Bilder, Videos usw. ohne Qualitätsverlust (und damit möglicherweise unbemerkt) kopiert, an anderer Stelle wieder eingefügt oder unbegrenzt häufig vervielfältigt werden können.

Damit zusammenhängend sind *online*basierte Öffentlichkeiten auch skalierbar, also in ihrer Reichweite variabel, denn ein Text, ein Video oder ein Foto kann im Prinzip zehn oder zehn Millionen Menschen erreichen (anders als etwa bei Zeitungen, deren Verbreitung wesentlich von der gedruckten Auflage mitbestimmt wird).

Schließlich sind *online*basierte Öffentlichkeiten durchsuchbar und Informationen können aggregiert werden, das heißt dass Informationen über eine Person oder ein Thema von ganz unterschiedlichen Stellen im Netz zusammen getragen werden können.

3 Informationelle Selbstbestimmung im Web 2.0

Die geschilderten Nutzungsweisen und ihre kommunikationstechnische Einbettung, die populäre Bereiche des gegenwärtigen Internets prägen, sind hochgradig relevant für Fragen nach Datenschutz und Privatsphäre: Im Grunde verändern Anwendungen wie *Facebook* oder *YouTube*, wie *Weblogs* oder *Twitter* derzeit die Art und Weise, wie Menschen personenbezogene Daten preisgeben. Es verschieben sich die Grenzen zwischen Privatsphäre und Öffentlichkeit. Diese Entwicklungen (die nicht allein auf das Web 2.0 beschränkt sind, wie zahlreiche andere Beiträge in diesem Band zeigen) lassen sich unter dem Begriff der informationellen Selbstbestimmung bündeln und für Schlussfolgerungen oder Handlungsempfehlungen greifbar machen.

Das Prinzip der informationellen Selbstbestimmung, das in den 1980er Jahren im Zuge der Volkszählungsdebatten vom Bundesverfassungsgericht geprägt wurde (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.), hat im Kontext des Web 2.0 eine dreifache Bedeutung.

Normative Bedeutung

Erstens ist informationelle Selbstbestimmung ein normatives Konzept, an dem sich das Handeln unterschiedlicher Akteure orientieren soll und muss. Als Bestandteil der verfassungsmäßigen Ordnung muss das Recht

auf informationelle Selbstbestimmung auch im *Social Web* gewährleistet sein. Es umfasst die Selbstbestimmung bzw. Kontrolle einer Person in dreifacher Hinsicht:

- über die von ihr selbst mitgeteilten Daten,
- über die sie betreffenden Daten, die andere Nutzende preisgeben,
- über die Daten, die beispielsweise Betreiber sammeln.

Weitergehende und spezifischere datenschutzrechtliche Bestimmungen und Regelungen einerseits, aber auch geteilte (wenngleich ungeschriebene) soziale Normen und Konventionen andererseits, geben einen zusätzlichen Handlungsrahmen ab. Sie drücken aus, was (sub-)kulturell als gewünschtes oder akzeptables Verhalten erwartet wird.

Situative Praxis

Zweitens ist informationelle Selbstbestimmung eine Praxis, die in konkreten Situationen ausgeübt wird: Nutzende betreiben informationelle Selbstbestimmung (und zwar mehr oder weniger kompetent, reflektiert, eventuell auch scheiternd), wenn sie sich in den vernetzten persönlichen Öffentlichkeiten des Web 2.0 bewegen. Erst dieser Blick auf die ausgeübte Praxis ermöglicht es, datenschutzrelevante Handlungsweisen jenseits (und unter Umständen auch in Widerspruch oder Abweichung von) rechtlich-sozialen Normen zu erfassen. Die Frage, was eine Person wem gegenüber in welcher Kommunikationssituation offenbart, welche Absichten und Ziele damit verbunden werden und welche Vorstellungen von Privatsphäre oder personenbezogenen Daten das Handeln jeweils anleiten, ist somit nur durch empirische Nutzungsforschung zu beantworten.

Kompetenz

Drittens ist informationelle Selbstbestimmung schließlich auch eine Kompetenz, also etwas, das jemand können muss bzw. sollte. Das eigenständige Wahrnehmen eines »Rechts auf Privatsphäre« setzt bestimmtes Wissen (beispielsweise über die mittel- und langfristigen Konsequenzen des eigenen informationsbezogenen Handelns) und Fertigkeiten (beispielsweise im Umgang mit technischen Optionen) voraus. Erst dadurch werden Nutzende zum Beispiel in die Lage versetzt, im Sinne einer »informierten Einwilligung« (unter Kenntnis von Umfang und Zweck) einer Verarbeitung der eigenen Daten zuzustimmen oder diese abzulehnen (siehe zur Einwilligung auch den Beitrag von Hartge in diesem Band, S. 281 f.).

Zudem berührt diese Vorstellung von informationeller Selbstbestimmung als Kompetenz auch die »informationelle Autonomie«[7], die eine Person in die Lage versetzt, eine freie Wahl von Quellen und Kommunikationsräumen vorzunehmen, um die eigenen Handlungsziele zu erreichen.

Informationelle Selbstbestimmung im Web 2.0 reicht über datenschutzrechtliche Aspekte hinaus

Um diesen zentralen Gedanken noch einmal besonders zu betonen: Informationelle Selbstbestimmung im Web 2.0 reicht über rein datenschutzrechtliche Aspekte des Handelns hinaus. Sie umfasst letztlich alle Fähigkeiten, Nutzungspraktiken und sozialen Rahmenbedingungen, die im Zuge der *online*basierten Kommunikation relevant sind.

Dies lässt sich beispielhaft an einem der wesentlichen Angelpunkte für die Grenzziehung zwischen Privatsphäre und Öffentlichkeit im Web 2.0 illustrieren: die Abstufung unterschiedlicher Varianten eines Publikums, von denen sich vier Arten unterscheiden lassen.

Intendiertes Publikum: Das intendierte Publikum ist derjenige Personenkreis, der den Nutzenden im Sinne eines »vorgestellten Empfängerkreises« ihrer Kommunikation im Allgemeinen vorschwebt und Themenwahl und -präsentation anleitet: Die eigenen Freunde und Bekannten in einem persönlichen Blog, die Kollegen und beruflichen Kontakte auf der Netzwerkplattform *XING* und so weiter.

Adressiertes Publikum: Das adressierte Publikum ist eine Teilmenge des intendierten Publikums, nämlich derjenige Personenkreis, der in einer spezifischen Situation tatsächlich erreicht werden soll; dieses kann beispielsweise durch das gezielte Ansprechen von → *Twitter-Followers* aus einer bestimmten Stadt wie etwa Hamburg oder auch das selektive Freigeben eines Fotos auf einer Plattform gesteuert werden.

Empirisches Publikum: Das empirische Publikum ist der Personenkreis, der tatsächlich von bestimmten Äußerungen oder Informationen Kenntnis nimmt; es kann sich vom intendierten wie vom adressierten Publikum unterscheiden, beispielsweise weil die eigenen Freunde das persönliche → *Weblog* nur sporadisch lesen oder ein Foto an bislang unbekannte Personen weitergeleitet wird.

Potentielles Publikum: Das potentielle Publikum ist schließlich derjenige Personenkreis, der prinzipiell technisch erreichbar wäre bzw. von den hinterlassenen Informationen Kenntnis erhalten könnte. Dies schließt den sprichwörtlichen Personalchef (siehe unten) ebenso ein, wie etwa die Plattformbetreiber. Die Größe des potentiellen Publikums ist vor allem

an die jeweiligen technischen Bedingungen einer Anwendung gekoppelt, beispielsweise in Hinblick auf die Dauerhaftigkeit der Kommunikation oder die Durchsuchbarkeit von Informationen.

Probleme bzw. Konflikte der informationellen Selbstbestimmung können vor allem dann entstehen, wenn – durch welche Gründe auch immer (etwa Unkenntnis, intransparente Software) – das intendierte und/oder adressierte Publikum nicht mit dem faktischen und/oder potentiellen Publikum übereinstimmt, also die eigene Selbstoffenbarung aus dem von den Nutzenden beabsichtigten Kontext gelöst und in einen anderen Kontext gestellt wird. Dies geschieht beispielsweise in dem oft zitierten Fall, dass ein Personalchef die *Facebook*-Profile von Bewerberinnen und Bewerbern durchstöbert und somit einen Einblick in Selbstdarstellungen gewinnt, die nicht an ihn adressiert waren. Gerade für Jugendliche sind es aber oft gar nicht die unbekannten Personen, sondern vielmehr die »bekannten, aber unangemessenen anderen«[8], die keinen Einblick in persönliche Informationen erhalten sollen. Gemeint sind damit beispielsweise Eltern, Lehrer oder ehemalige Freunde.

Gerade das Wissen um die Größe und Zusammensetzung des potentiellen Publikums ist somit ein entscheidender Faktor, um informationelle Selbstbestimmung tatsächlich auszuüben. Dies beinhaltet auch die Fähigkeit, mögliche zukünftige Erweiterungen des Publikums – zum Beispiel durch den Einfluss von Plattformbetreibern, bekannte oder unbekannte Dritte – mit in Betracht zu ziehen.

4 Leitbild der informationellen Selbstbestimmung

Dieser Beitrag soll grundlegende Entwicklungslinien der *online*basierten Kommunikation aus einer soziologischen Perspektive deutlich machen: Im Web 2.0 entsteht der neue Typ der persönlichen Öffentlichkeit, der Spannungen zwischen dem Wunsch nach Zugehörigkeit, Interaktion und Konversationen einerseits und dem Bedürfnis nach Privatsphäre sowie Datenschutz andererseits auf eine neue technische Grundlage stellt. Das Konzept der informationellen Selbstbestimmung kann in seinen drei Facetten – normative Richtschnur, ausgeübte Praxis und notwendige Kompetenz – weiterhin als Leitbild dazu dienen, wie wir gesellschaftlich mit diesen Veränderungen umgehen.

Ein solches Leitbild, das von konkreten technischen Anwendungen abstrahiert, ist auch deswegen nötig, weil der rasche medientechnische Wandel bereits jetzt absehbar macht, dass sich Fragen des Datenschutzes

und der Privatsphäre in Zukunft eher noch drängender stellen. Die Möglichkeiten, auf das Netz zuzugreifen, werden sich stetig vergrößern, weil es beispielsweise Modelle des → *Cloud Computing* ermöglichen, von beliebigen Zugangsgeräten auf Daten und Programme zugreifen zu können. Damit verbunden wird sich der Zugang zum Internet über mobile Endgeräte weiter verbreiten, wobei die geographische Position des Nutzenden (bewusst oder unbewusst) übertragen wird, was eine weitere Dimension von personenbezogenen Daten (nämlich: Wann ist eine Person wo?) zugänglich macht. Hinzu wird eine wachsende Zahl von »intelligenten« Alltagsgegenständen kommen, die etwa über → RFID-Chips an Datennetze angeschlossen sein werden (siehe auch den Beitrag von Hansen in diesem Band, S. 78 ff.).

Eine solche Mobilisierung und Allgegenwärtigkeit des Internets wird weitere Debatten über Datenschutz und Überwachung nach sich ziehen, die unter den Bedingungen des → *Ubiquitous Computing* oder → *Pervasive Computing* gesellschaftlich neu geregelt werden müssen. Sie werfen eine grundlegende Frage unserer Zeit auf: Wer kontrolliert und gestaltet die Architektur und Normen der (Web 2.0-)Technologien und der durch sie ermöglichten Interaktions- und Kommunikationsräume? Die Algorithmen, Voreinstellungen und Optionen, die in die Technologien einschrieben sind, beeinflussen in hohem Maße unsere Nutzungspraktiken. Wer aber hat Einfluss auf ihre Gestaltung, und welche Vorstellung von Sozialität, Transparenz oder Kontrolle haben Entwickler? Diese Fragen (siehe hierzu auch den Beitrag von Schaar in diesem Band, S. 363 ff.) sind nicht zuletzt deswegen so wichtig, weil sie letztlich die Kontrolle über die Gestaltung einer zentralen Technologie des 21. Jahrhunderts wieder in die Gesellschaft zurückverlagern helfen. Denn so sehr und so grundsätzlich das Internet unser individuelles wie gesellschaftliches Leben auch verändert, bleibt es letztlich doch immer von Menschen gestaltet – und gestaltbar.

Anmerkungen

1 Teile der hier entwickelten Gedanken wurden in einem Projekt gemeinsam mit Monika Taddicken, Claudia Lampert, Wiebke Loosen, Uwe Hasebrink und Leonard Reinecke entwickelt, denen ich für Anregungen herzlich danke.

2 Die Kommunikationssoziologie untersucht Zusammenhänge zwischen gesellschaftlichen Veränderungen und kommunikativen Abläufen.

3 Vgl. Jan-Hinrik Schmidt, Das neue Netz. Merkmale, Praktiken und Folgen des Web 2.0, Kostanz 2009; Ingrid Paus-Hasebrink/Jan-Hinrik Schmidt/Uwe Hasebrink, Zur Erforschung der Rolle des Social Web im Alltag von Heranwachsenden, in:

dies. (Hrsg.), Heranwachsen mit dem Social Web. Zur Rolle von Web 2.0-Angeboten im Alltag von Jugendlichen und jungen Erwachsenen. Berlin 2009, S. 13–40.

4 Vgl. Schmidt (2009) und Paus-Hasebrink/Schmidt/Hasebrink (2009) (Anm. 3); siehe auch Jo Bager, Die *Facebook*-Welt: enger vernetzt als die reale Welt, Heise Online vom 22.11.2011, im Internet unter http://heise.de/-1382686, wonach *Facebook*-Nutzende durchschnittlich 190 Freunde haben.

5 Von engl. *to stream*, dt. strömen; gemeint ist die Datenübertragung.

6 Vgl. Danah Boyd, Taken out of context. American teen sociality in networked publics. Berkeley 2008, im Internet unter http://www.danah.org/papers/TakenOutOfContext.pdf.

7 Vgl. Rainer Kuhlen, Die Konsequenzen der Informationsassistenten. Was bedeutet informationelle Autonomie oder wie kann Vertrauen in elektronische Dienste in offenen Informationsmärkten gesichert werden? Frankfurt/M. 1999.

8 Sonia Livingstone (engl.: »Known but inappropriate others«), Taking risky opportunities in youthful content creation. Teenagers' use of social networking sites for intimacy, privacy and self-expression, in: New Media & Society, Bd. 10 (Nr. 3/Juni 2008), S. 393-411, im Internet unter http://nms.sagepub.com/content/10/3/393.abstract.

Ulrike Wagner / Christa Gebel / Niels Brüggen

Privatsphäre als Verhandlungssache: Jugendliche in sozialen Netzwerkdiensten

In sozialen Netzwerkdiensten[1] mit persönlichen Informationen umzugehen und dabei dem Datenschutz und den Persönlichkeitsrechten Genüge zu tun, stellt eine Herausforderung dar. Das gilt nicht nur für Jugendliche – für diese aber in besonderer Weise (siehe auch den Beitrag von Spaeing/Spaeing in diesem Band, S. 249 ff.). So geben manche *Online*-plattformen kaum Hinweise auf die Tragweite der Veröffentlichung persönlicher Informationen und fordern die Nutzenden darüber hinaus implizit oder explizit dazu auf, sich mit umfangreichen Angaben zur eigenen Person einem großen Publikum zu präsentieren. Hinzu kommt, dass sogenannte »*Online*-Freunde«[2], die ja häufig auch »*Offline*-Freunde«[3] sind, durch zusätzliche Informationen (zum Beispiel Kommentare, Fotoverlinkungen und so weiter) dazu beitragen können, dass mehr Persönliches und damit auch mehr persönliche Daten bekannt werden, als den Betroffenen recht sein kann.[4]

1 Kompetenter Umgang mit sozialen Netzwerken

Technische Gegebenheiten, rechtliche Rahmenbedingungen, Interessen der Anbieter sowie soziale Normen – das sind die Bedingungen, auf die die Motive, das Wissen und die Fähigkeiten derjenigen treffen, die sich in *Online*netzwerken präsentieren und austauschen (siehe auch den Beitrag von Schmidt in diesem Band, S. 215 ff.). Ein kompetenter Umgang mit diesen Bedingungen stellt auch für Erwachsene eine Herausforderung dar; bei Jugendlichen kommen zusätzlich entwicklungstypische Motive (beispielsweise das Streben nach Selbstbestimmung, Identitätsentwicklung, Integration in die *Peergroup*[5], Erproben sozialer Beziehungen) sowie ihr teilweise noch begrenzter Erfahrungshorizont ins Spiel, wenn es um die Abschätzung von Risiken und die Suche nach Orientierungspunkten für das eigene Handeln und Verhalten in → sozialen Netzwerken geht.

Welche Positionen nehmen Jugendliche zu Fragen des Datenschutzes in *Online*netzwerken ein?

Die jugendlichen Nutzerinnen und Nutzer von sozialen Netzwerkdiensten bewegen sich hier in Spannungsfeldern und sind mit Problemen konfrontiert, für die sie individuell nach Lösungen suchen. Wie sie die Bedingungen der *Online*netzwerke wahrnehmen, wie sie sich zu Fragen des Datenschutzes und der Persönlichkeitsrechte in sozialen Netzwerkdiensten positionieren und wie sie vor diesem Hintergrund selbst mit den Gegebenheiten dieser Dienste umgehen, war Gegenstand einer empirischen Studie, deren wesentliche Ergebnisse in diesem Beitrag dargestellt werden.[6]

2 Präsentationsstrategien Jugendlicher in *Online*netzwerken

Beispielhaft für die Haltung nahezu aller Teilnehmerinnen und Teilnehmer der Studie steht die Aussage eines Jungen, die zeigt, dass die Jugendlichen selbst bestimmen wollen, wie sie mit persönlichen Informationen in sozialen Netzwerkdiensten umgehen. Dieser Jugendliche sagte: »Ich entscheid eben immer für mich selbst, ob ich was von mir zeigen möchte oder nicht.«[7]

Der Anspruch auf Entscheidungsfreiheit, der damit formuliert wird, trifft den Kern der aktuellen Debatte um die Wahrung der Privatsphäre in sozialen Netzwerkdiensten. Alle Befragten sind der Ansicht, dass es Informationen gibt, die schützenswert sind und entsprechend nicht oder nur für bestimmte Personen im Internet verfügbar gemacht werden sollten. Unterschiedliche Ansichten gibt es in der Frage, auf welche Informationen dies zutrifft und wie dies zu bewerkstelligen ist.

Balance zwischen erwartetem Nutzen und individuellem Schutzbedürfnis

Die Jugendlichen entwickeln im Umgang mit sozialen Netzwerkdiensten Handlungsweisen, die dadurch geprägt sind, dass die Jugendlichen eine Balance herstellen wollen. Es geht ihnen um ein ausgewogenes Verhältnis zwischen individuellen Nutzungsmotiven (Kommunikation mit anderen, Darstellung der eigenen Person) auf der einen Seite und unterschiedlich ausgeprägten Schutzbedürfnissen in Bezug auf persönliche Informationen auf der anderen Seite. Die Ausbalancierung dieser beiden Ansprüche ist keine leichte Aufgabe. Die Jugendlichen gehen ganz

unterschiedliche Wege, um dies zu erreichen. Dabei geraten sie allerdings auch in Widersprüche, die die Grenzen der Entscheidungsfreiheit und des selbstbestimmten Umgangs mit persönlichen Informationen markieren. Die Handlungsweisen der befragten Jugendlichen lassen sich zu drei Strategien zusammenfassen, wie Jugendliche sich selbst in sozialen Netzwerkdiensten darstellen.[8] Diese Präsentationsstrategien werden jeweils an einem Beispiel aus einer Fallstudie erläutert.

Präsentationsstrategie 1: Erkennbar, um *Offline*-Kontakte zu pflegen und zu erweitern

Beispielhaft für die erste Präsentationsstrategie steht eine 17-jährige Schülerin, die in der Studie unter dem Chiffre »facebook_10« geführt wurde. Sie nutzt *Online*netzwerke, um Kontakte zu erweitern und zu pflegen: »(…) Die meisten reden dann halt immer so (…) oder machen etwas aus über diese Netzwerke, und wenn du da nicht dabei bist, kannst du nicht mitreden (…). Giltst du dann quasi als uncool heutzutage, wenn du da nicht dabei bist.«[9]

Für »facebook_10« ist *facebook.com* ein zentraler Kommunikationsknoten ihres *Offline*-Soziallebens, den sie täglich nutzt. Damit Freunde, die sie *offline* kennenlernt, sie auf der Plattform finden, verwendet sie für ihr Profil ihren Realnamen. Allerdings hat sie den Zugriff auf die dort eingestellten Informationen auf bestätigte Freunde begrenzt. Damit will sie ausschließen, dass Informationen für »irgendwelche Leute, die dich nicht mögen« zugänglich sind. Und sie will verhindern, dass bei Fremden Missverständnisse durch fehlende Kontextinformationen entstehen. Ihre Freunde hält die 17-Jährige durch regelmäßige Pinnwandeinträge auf dem Laufenden, berichtet über Alltagsereignisse oder postet Videos, die ihr gefallen. In ihrem Profil offenbart sie ihrem Freundeskreis auch ihre politische Orientierung – eine Information, die andere Jugendliche, die ihr Profil ebenfalls auf Freunde begrenzen, dennoch aus Vorsicht vor möglicher Diskriminierung nicht in einem *Online*netzwerk veröffentlichen würden.

Profilzugriff auf Freunde beschränkt oder nur »öffentlichkeitstaugliche« Informationen

»Facebook_10« und fünf weitere Befragte, die vergleichbare Handlungsweisen zeigen, sind der an sozialer Einbettung orientierten »Strategie 1: erkennbar, um *Offline*-Kontakte zu pflegen und zu erweitern« zugeordnet. Es geht diesen Befragten vor allem darum, für ihren bereits bestehenden Bekannten- und Freundeskreis sichtbar zu sein und diesen über Interaktionen zu pflegen und zu erweitern. Diese Befragten machen sich für ihr soziales Umfeld erkenn-

bar, sind aber für Außenstehende nur mit Aufwand eindeutig identifizierbar. Während vier Befragte ihr Profil nur für Freunde öffnen, verzichten zwei auf diese Begrenzung, legen aber besonders viel Wert darauf, nur solche persönlichen Informationen einzubringen, die sie für vollkommen »öffentlichkeitstauglich« halten. Damit haben sie eine Gemeinsamkeit mit den Befragten, die der nachfolgend beschriebenen Strategie 2 zugeordnet sind.

Präsentationsstrategie 2: Erkennbar, um inhaltlichen Austausch zu fördern

Ein anderer 17-jähriger Schüler (genannt »myspace_3«) findet auf *myspace.com* nicht nur die Möglichkeit, Musik zu hören, sondern er kann sich hier auch mit Musikinteressierten und Musikschaffenden anfreunden und austauschen. Er sagt: »Ich weiß nicht, ob sich so jemand für mich interessiert, aber mir bringt es was, dass ich viele Künstler erst kennen gelernt habe (…), die ich dann gern auch mal live hören würde.«[10]

In diesem Austausch liegt für ihn das wichtigste Anliegen für die Beteiligung an dieser Plattform. Die wenigsten seiner Kontakte auf *myspace.com* kennt er persönlich. Dennoch legt er Wert darauf, auf der Plattform erkennbar zu sein und findet es wichtig, dass potenzielle Kontakte sich ein Bild von ihm machen können. Anfangs hatte er neben seinem Realnamen und seinem Wohnort nur verhältnismäßig wenig ins Profil eingestellt. Das erschien ihm später jedoch zu »unpersönlich« und er hat infolgedessen mehr persönliche Informationen sichtbar gemacht.

Veröffentlichung von Informationen nur über bestimmte Aspekte der eigenen Persönlichkeit

»Myspace_3« konzentriert sein Auftreten auf die Persönlichkeitsfacette »Musikfan«. Andere Facetten seiner Person will er dort nicht veröffentlichen und achtet beispielsweise darauf, möglichst keine privaten Fotos einzustellen. Den Zugriff auf die eingestellten Informationen schränkt myspace_3 nicht ein. Vielmehr verfährt er nach der Devise: Was nicht alle sehen dürfen, wird gar nicht erst hochgeladen.

Trotz seiner sehr kritischen und durchdachten Haltung zu Fragen des Datenschutzes gibt er dennoch vergleichsweise viele »harte Daten« an. So hat er nichts dagegen, dass über ein auf seinem Profil eingebundenes *Facebook*-Feld zusätzlich sein Geburtsdatum, seine *Messenger*-Kontaktdaten, seine (veraltete) Handynummer und Hinweise auf seine weiteren *Online*-Präsenzen in anderen sozialen Netzwerkdiensten bekannt werden. Dies erstaunt zunächst, da er sich über Fragen des Datenschutzes sehr informiert zeigt.

Den Kern der Problematik sieht er jedoch nicht in den Daten, die Nutzende in *Online*netzwerken über sich selbst einstellen, sondern in denjenigen Informationen, die andere unkontrolliert über die Betreffenden veröffentlichen können. So findet er es bedenklich, »dass man einfach keine eigene Privatsphäre hat, wenn man darauf achten muss, dass andere keine Fotos von einem machen, die dann vielleicht im Internet landen.«[11]

Trotz dieser Bedenken geht es »myspace_3« wie den anderen Befragten der Gruppe, die die Strategie 2 verfolgen, darum, mit Hilfe des *Online*netzwerkes ihre Interessen zu vertiefen und ihre Talente zu zeigen. Über ihre damit verbundenen Fähigkeiten und Kenntnisse können sie ihre Kompetenzen unter Beweis stellen und finden auf diesem Weg Gleichgesinnte, die diese zu schätzen wissen. Die Befragten wollen erkennbar sein und verzichten auf eine Verschleierung ihrer Identität, um inhaltliche Diskussionen rund um ihre Interessen und Talente führen zu können.

Präsentationsstrategie 3: Inkognito, um unbehelligt Erfahrungen zu machen

Die 14-jährige »jappy_5« ist der dritten Strategie zuzuordnen, bei der es um einen spielerisch-experimentellen Umgang mit den Plattformen geht, um dort unbehelligt Erfahrungen machen zu können.

»Jappy_5« gefällt es nicht, »von Wildfremden« angesprochen zu werden. Sie sagt: »Na, es gibt ja immer irgendwelche verrückten Leute, die sich dann da ein Profil machen, um irgendwelche Mädchen oder Jungs zu stalken (…), vielleicht suchen sie die und dann kommen die dahin (…), da macht man sich ja schon so Gedanken.«[12]

Auf *jappy.de* kann sie solche Kontaktversuche jedoch nicht vollkommen unterbinden, denn sie kann nur bestimmte Gruppen ausschließen, wie etwa männliche oder weibliche Nutzende oder Menschen bestimmten Alters. Es gibt jedoch einen Bereich, den sie nur für bestätigte Freunde reserviert hat. In ihrem Gästebuch tauscht sie, unsichtbar für die Plattformöffentlichkeit, im engeren Kreis der Freunde flapsige bis schnodderige Bemerkungen aus, weshalb dieses Gästebuch quasi als gemeinsamer Spielplatz fungiert.

Nutzung des Netzwerks unter Pseudonym

Für Fremde will »jappy_5« auch nicht als attraktive Jugendliche erkennbar sein, deshalb hat sie Falschangaben bei einer Reihe von Profildaten wie Körpergröße, Figur und Familienstand gemacht. Sie nutzt die Plattform unter einem → Pseudonym, in das sie ihren Vornamen integriert hat.

So haben Personen aus ihrem sozialen Umfeld einen Anhaltspunkt, während sie für Außenstehende nur mit größerem Aufwand zu identifizieren ist. Auch Fotos, die sie selbst zeigen, lädt sie gar nicht hoch, um sich für Fremde nicht erkennbar zu machen. Allerdings können diese dennoch leicht herausfinden, wie »jappy_5« aussieht, denn einige ihrer Freunde haben Fotos, auf denen sie erscheint, in ihre eigenen Fotogalerien eingestellt. Diese Fotos haben die Freunde auf das Profil von »jappy_5« verlinkt.

Die dritte Strategie kann als *spielerisch-experimentell* bezeichnet werden. Die Befragten, die dieser Gruppe zugeordnet wurden, bewegen sich unter einem Pseudonym in *Online*netzwerken. Sie spielen mit verschiedenen Rollen und erproben Handlungsweisen. Das »Gestalten der Persönlichkeit« ist dabei wesentliches Merkmal von teilweise stereotypen Weiblichkeitsinszenierungen und das Spielen mit Identitätsfacetten ist für die Befragten dieser Strategie charakteristisch. *Online*netzwerke sind für sie Räume, in denen ein »Probehandeln« vollzogen werden kann. Diese Befragten sind nur mit (teilweise erheblichem) Aufwand identifizierbar, denn sie wollen inkognito bleiben, um ungestört Erfahrungen zu machen.

3 Grenzen selbstbestimmten Handelns in sozialen Netzwerkdiensten

In *Online*netzwerken souverän zu handeln ist eine große Herausforderung, die nicht nur die Handlungsfähigkeit der Jugendlichen betrifft. Das individuelle Handeln wird, neben den Motiven und entwicklungstypischen Aufgaben der Jugendlichen, von den sozialen Regeln in diesen Netzwerken mitgeprägt. In ihnen stellt das Handeln der Anderen einen wichtigen Bezugspunkt für die jeweils eigenen Verhaltensweisen dar. Was und wie viel Jugendliche in *Online*netzwerken von sich zeigen, ist insbesondere von solchen Regeln und Normen beeinflusst, die in der Nutzungspraxis greifbar werden. Diese sind sehr unterschiedlich und nicht unbedingt widerspruchsfrei.

Nahezu alle Befragten sind der festen Überzeugung, dass jede oder jeder selbst dafür verantwortlich ist, was sie oder er in *Online*netzwerke einstellt. Daraus leiten sie die Regel ab, dass es sich nicht gehört, sich in das einzumischen, was andere auf der Plattform tun, solange es die eigenen Rechte nicht einschränkt. Damit weisen sie die Übernahme von Verantwortung für das Handeln anderer von sich.

Das Einverständnis einzuholen, wenn Rechte Dritter (beispielsweise das Recht am eigenen Bild) betroffen sind, wird von den Jugendlichen

nicht als unabdingbar wahrgenommen, unter anderem weil es ihnen zu aufwändig erscheint. Vielmehr gehen sie davon aus, dass die Entscheidung, was sie von anderen zeigen oder über sie äußern können, im eigenen Ermessen liegt. Dabei orientieren sie sich an ihrer Einschätzung, wann die Betroffenen verärgert sein könnten. Umgekehrt ist es ihnen durchaus wichtig, wie sie selbst von anderen dargestellt werden. Hier haben viele der Befragten erlebt, dass ihre Rechte zum Verhandlungsgegenstand wurden bzw. ihre Einwände gegen unliebsame Abbildungen übergangen wurden.

Falsche Angaben können unter bestimmten Umständen zwar dem Schutz der eigenen Person dienen oder der Attraktivität des Profils (oder, wenn es um das anzugebende Alter geht, die Teilnahme am Netzwerk erst ermöglichen); die soziale Erwartung besteht jedoch darin, zu wissen »mit wem man es zu tun hat«.

Die Jugendlichen begründen das Erfordernis, persönliche Informationen zu zeigen, etwa damit, dass sie selbst andere Nutzende anhand entsprechender Informationen einschätzen wollen. Dabei kann eine Dynamik entstehen, die zur Angabe von immer mehr Informationen anregt. Zugleich ist damit eine Dynamik sozialer Kontrolle verbunden, da die bzw. der einzelne Nutzende die Aktivitäten Anderer im Blick behalten muss, um zu wissen, was über die eigene Person veröffentlicht wird.[13]

Die Selbstbestimmung der Jugendlichen wird durch Netzwerkvorgaben eingeschränkt

Darüber hinaus sind dem individuellen Handeln Grenzen gesetzt, die die Möglichkeiten zur Selbstbestimmung einschränken, aber nur wenig von den Individuen zu beeinflussen sind. Dazu gehören zum einen die »Spielregeln«, die Anbieter sozialer Netzwerkdienste in ihren Allgemeinen Geschäftsbedingungen festlegen. Sie sind für die Nutzenden nicht immer verständlich. Dies betrifft beispielsweise Fragen nach der Verwertung der eigenen Daten durch Dritte und die Einhaltung gesetzlicher Regelungen. Zum anderen setzen die Anbieter den Rahmen, der unter anderem die Bandbreite der Mittel festlegt, mit denen Jugendliche sich artikulieren können: sei es in der Gestaltung eigener Profilseiten oder in der Präsentation eigener Werke wie Fotos oder Videos. Dieser mediale Rahmen beinhaltet auch implizite und explizite Aufforderungen, Informationen über die eigene Person oder über andere zu veröffentlichen, was ebenfalls Bereiche der Privatsphäre tangieren kann.

4 Ausgangspunkte für eine erfolgreiche pädagogische Arbeit

Die Jugendlichen betrachten *Online*netzwerke als Räume, in denen sie selbstbestimmt handeln können: Der Wunsch nach sozialer Zugehörigkeit einerseits und das Streben nach autonomem Handeln andererseits bilden die zentralen Motive. Es sind gerade die Ambivalenzen und Widersprüche im Handeln der Jugendlichen, die für die medienpädagogische Arbeit und Medienkompetenzförderung von zentraler Bedeutung sind.[14] Medienpädagogik zielt deshalb auf eine Sensibilisierung der Jugendlichen im Umgang mit persönlichen Informationen. Aus den skizzierten Ergebnissen ergeben sich die folgenden Ansatzpunkte und Leitlinien für die pädagogische Arbeit.

Mediale Erfahrungsräume und Motive der Heranwachsenden respektieren

Die Kenntnis der Medienerfahrungen und der Motivlagen von Jugendlichen wie auch deren Anerkennung sind die zentralen Voraussetzungen, um mit ihnen ins Gespräch zu kommen und darüber eine Sensibilisierung für Fragen der Persönlichkeitsrechte zu erreichen. Es ist wichtig, keine Tipps und Regeln zu vermitteln, die im Widerspruch zu den Erfahrungen der Jugendlichen stehen. Ein erfolgversprechender Weg könnte darin bestehen, mit den Jugendlichen gemeinsam Alternativen zu erarbeiten, wie sie datenschutzsensibel sein und dennoch ihre Handlungsziele auf den Plattformen erreichen können – etwa wenn es darum geht, Fotos einzubinden, auf denen andere zu sehen sind oder auf denen sie sich selbst präsentieren wollen.

Kontroll- und Erwartungsspiralen bewusst machen

Die Anerkennung durch die Anderen im Netzwerk bildet die Voraussetzung, um den Wunsch nach sozialer Zugehörigkeit erfüllen zu können. Um dies zu erreichen, müssen die Jugendlichen mehreren Erwartungshaltungen Genüge tun. Hier entsteht möglicherweise auch ein Druck, immer mehr über sich preisgeben zu müssen und somit mehr persönliche Daten zu nennen – eine Erwartung, die auch durch die Plattformbetreiber gestützt wird. Darüber hinaus ist es bei der Nutzung der Netzwerke nicht nur mit der Pflege des eigenen Profils und dem Interagieren mit Anderen getan. Die Beobachtung beziehungsweise Kontrolle dessen, was die anderen Mitglieder des eigenen Netzwerkes tun, ist ebenfalls ein Bestandteil der Nutzung, um informiert zu bleiben.

Entsprechend gilt es, Dynamiken des »Immer-mehr« sowie Dynamiken gegenseitiger sozialer Kontrolle gemeinsam herauszuarbeiten und der bewussten Reflexion zugänglich zu machen.

(Mit-)Verantwortungsbewusstsein stärken

Die Befragten bestehen vehement darauf, für ihr Handeln selbst verantwortlich zu sein und ihre eigenen Entscheidungen treffen zu können. Sie verknüpfen diesen Anspruch zumeist mit der Abgrenzung von einer Einmischung in das Handeln anderer. Hier gilt es zunächst, ihre Schutzbedürfnisse zu erkennen und zu thematisieren, um im nächsten Schritt Mitverantwortung für die Rechte anderer zu thematisieren. Dabei sind jene Punkte herauszuarbeiten, in denen sie zur Mitverantwortung aufgerufen sind, beispielsweise wenn Rechte anderer verletzt werden.

Soziale Netzwerkdienste bieten automatisierte Funktionen an, um beispielsweise problematische Inhalte zu melden. Diese ermöglichen es den Nutzenden grundsätzlich, für die Integrität der eigenen Person und die der Anderen einzustehen. Genau zu diesen Fragen müssen mit den Jugendlichen gemeinsam Handlungsoptionen erarbeitet werden, die ihren Bedürfnissen nach Schutz, aber auch nach sozialer Einbettung entsprechen. Mit Blick auf eine möglicherweise ausufernde gegenseitige Kontrolle der Nutzenden gibt es hier auch klare Grenzen der Mitverantwortung.

Beim Schutz der Privatsphäre Angebotsseite einbeziehen

Das Verständnis für die grundlegenden Strukturen der Angebote bildet das entscheidende Fundament, um das eigene Handeln reflektieren und soziale Netzwerkdienste bewerten zu können. Auf dieser Basis können gemeinsam entsprechende Qualitätskriterien für die Einschätzung der Plattformen entwickelt werden. Diese Kriterien müssen jedoch auch praxistauglich sein (zum Beispiel in Bezug auf die Motive und Fragen der Jugendlichen). Ein weiteres Ziel ist die Vermittlung von Kriterien für die Einschätzung relevanter Informationsquellen bezüglich Seriosität und Sachkompetenz.

In pädagogischen Handlungsfeldern ist dafür Sorge zu tragen, dass Privatsphäre nicht zur Privatsache einzelner Individuen gemacht wird. Konkret bedeutet dies, dass Jugendlichen Unterstützungsangebote bereitgestellt werden müssen, mit denen sie die Voraussetzungen für selbstverantwortliches Handeln (beispielsweise Wissen über Medienstrukturen und Nutzungsdynamiken) erkennen können. Nicht zuletzt geht es auch darum, Selbst- und Mitverantwortung zu stärken, damit die Bedingungen sozia-

len Miteinanders gemeinschaftlich getragen werden. Die Forderung nach Transparenz und Verantwortungsübernahme ist aber nicht nur an die Einzelnen und an die Pädagogik zu richten, sie ist als zentraler Qualitätsanspruch insbesondere an die Anbieter sozialer Netzwerkdienste heranzutragen.[15]

Anmerkungen

1 Mit sozialen Netzwerkdiensten sind Webanwendungen gemeint, die es den Benutzenden erlauben, ein virtuelles Netzwerk aus Kontakten aufzubauen, Beispiele sind *Facebook*, studiVZ usw., siehe auch → Netzwerkplattformen.

2 Als »*Online*-Freunde« werden solche Personen bezeichnet, die in sozialen Netzwerken als »Freunde« (das heißt Kontakte) dem eigenen Profil zugefügt wurden.

3 Als »*Offline*-Freunde« werden Personen bezeichnet, mit denen man enge soziale Kontakte pflegt, die hauptsächlich auf einer unmittelbaren Kommunikation von »Angesicht zu Angesicht« beruhen.

4 Ulrike Wagner/Niels Brüggen/Christa Gebel, Web 2.0 als Rahmen für Selbstdarstellung und Vernetzung Jugendlicher. Analyse jugendnaher Plattformen und ausgewählter Selbstdarstellungen von 14- bis 20-Jährigen, München 2009 (unter Mitarbeit von Peter Gerlicher und Kristin Vogel), im Internet unter http://www.jff.de/index.php?BEITRAG_ID=5808. Dabei handelt es sich um eine Analyse von jugendaffinen Plattformen und ausgewählten Selbstdarstellungen von Jugendlichen zwischen 14 und 19 Jahren, die 2008 im Auftrag der Bayerischen Landeszentrale für neue Medien (BLM) durchgeführt wurde.

5 Der Begriff bezeichnet eine Gruppe (beispielsweise im ähnlichen Alter oder mit gleichen Interessen), zu der eine Person sich zugehörig fühlt und die diese Person für sich als Bezugsgruppe wahrnimmt.

6 Vgl. Ulrike Wagner/Niels Brüggen/Christa Gebel: Persönliche Informationen in aller Öffentlichkeit? Jugendliche und ihre Perspektive auf Datenschutz und Persönlichkeitsrechte in Sozialen Netzwerkdiensten. München 2010, im Internet unter http://www.jff.de/studie_datenschutz. Es handelt sich um eine Teilstudie der Untersuchung »Das Internet als Rezeptions- und Präsentationsplattform für Jugendliche« im Auftrag der Bayerischen Landeszentrale für neue Medien (BLM). Durchgeführt wurden Einzelfallstudien mit elf Heranwachsenden aus dem Bundesgebiet mit überwiegend höherer Schulbildung. Grundlage für die Fallstudien waren leitfadengestützte Telefoninterviews (März 2010) und Analysen der zugehörigen persönlichen Profile in sozialen Netzwerkdiensten. Ferner fanden in Münchner Hauptschulklassen Gruppenerhebungen statt (Gruppeninterview anhand eines Szenarios, Diskussion von Statements zum Datenschutz), an denen 52 Schülerinnen und Schüler der achten und neunten Jahrgangsstufe teilnahmen (Mai 2010).

7 Anonymisierte Äußerung eines Jungen in einer Gruppenerhebung (Junge G2, 541), Wagner/Brüggen/Gebel (Anm. 6), S. 63.

8 Von den elf Fallstudien wies eine Person gleichermaßen Facetten der Strategie 1 wie der Strategie 2 auf und wurde deshalb beiden Strategien zugeordnet.
9 Facebook_10, 161, Wagner/Brüggen/Gebel (Anm. 6), S. 31.
10 Myspace_3, 34, Wagner/Brüggen/Gebel (Anm. 6), S. 36 ff.
11 Myspace_3, 153, Wagner/Brüggen/Gebel (Anm. 6), S. 38.
12 Jappy_5, 103, Wagner/Brüggen/Gebel (Anm. 6), S. 40.
13 Für eine Analyse der Dynamiken sozialer Kontrolle in sozialen Netzwerken siehe auch Anders Albrechtslund, Online Social Networking as Participatory Surveillance, in: First Monday, Band 13 (3/2008), im Internet unter http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2142/1949.
14 Diesen Ausgangspunkt nutzend verbindet das Modellprojekt »Webhelm – Selbstverantwortung im Web 2.0« die Förderung von Medienkompetenz mit den Themen Datenschutz, Persönlichkeitsrechte und Urheberrechte. Hierzu stehen auf der Plattform http://www.webhelm.de Hintergrundinformationen und methodische Anregungen für pädagogische Fachkräfte zur Verfügung.
15 Weitere Informationen bei: Helga Theunert, Medienkompetenz, in: Bernd Schorb/Günther Anfang/Kathrin Demmler (Hrsg.), Grundbegriffe Medienpädagogik (Praxis), München 2009, S. 199–204.

Franziska Bluhm

Privatsphärenverlust im digitalen Alltag?

1 Vorteile eines digitalen Alltags

Ein neuer Job, ein guter Gedanke, eine unfassbar schlechte Fernsehsendung – ich bin nicht die Einzige, die solche Dinge nicht nur ihrem engsten Freundeskreis mitteilt, sondern sie auch im Internet veröffentlicht (beispielsweise im eigenen → *Weblog*, beim Kurznachrichtendienst → *Twitter* oder auf *Facebook*). Auch die freudige Nachricht des sich ankündigenden Nachwuchses verkündete ich selbstverständlich nicht in einer Rundmail, in Briefen oder in stundenlangen Telefonaten – nur für einen ausgewählten Kreis – sondern in meinem *Weblog*. Manche nennen das Selbstentblößung, für mich ist es ein selbstverständlicher Teil meiner Kommunikation geworden. Bisher hat es mir nicht geschadet.

Produktempfehlungen und neue Bekanntschaften

Nun kann man mir natürlich einen ausgeprägten Hang zur Selbstdarstellung unterstellen. Das ist sicherlich nicht komplett von der Hand zu weisen. Und natürlich fragen sich viele: Warum macht sie das eigentlich? Die Antwort darauf ist einfach: Weil ich davon profitiere. Welcher Kinderwagen für mich (und mein Auto) der richtige ist, fand ich durch mein Blog (und mit Hilfe des Internets) heraus. Gute Filme, Bücher oder Musik werden mir empfohlen, weil ich meinen Geschmack preisgebe. Ausgehtipps gibt es ebenfalls inklusive – die Leute wissen, was ich mag. Über → *Twitter* und *Facebook* empfehlen mir Freunde, Bekannte, Kollegen und Fremde gute Texte, Videos, Ideen und Hintergründe, von denen ich ohne das Internet niemals erfahren hätte. Und noch viel besser: Durch diese virtuellen Aktivitäten sind über die Jahre Freundschaften entstanden, der Bekanntenkreis hat sich erweitert, aber auch berufliche Kontakte haben sich ergeben und ausgezahlt.

Ich bin damit nicht allein. Dem US-Journalisten Jeff Jarvis wurde beispielsweise auf diesem Weg durch die schwere Zeit seiner Krebserkrankung geholfen. Wie das funktionierte, hat er nicht nur in seinem Blog *www.buzzmachine.com* notiert, sondern im Herbst 2011 auch in einem Buch[1] veröffentlicht.

Mit Hilfe sozialer Medien werden auch politische Proteste organisiert (siehe auch den Beitrag von Beckedahl in diesem Band, S. 48 ff.). Das geschieht zunehmend auch in Deutschland, aber besonders in Ländern, in denen die öffentliche Meinung nicht so geschätzt wird. Die Revolutionen in der arabischen Welt im Jahr 2011 wären ohne den Einsatz sozialer Medien sicherlich nicht so effizient verlaufen.

2 Die Angst vor dem Verlust der Privatsphäre

Nun wäre es falsch, diesen von mir und ein paar Millionen Internetbegeisterten weltweit gewählten Weg auf andere zu übertragen und ihn als den einzig richtigen darzustellen. Ich kann Menschen, die dem Internet skeptisch gegenüber eingestellt sind, durchaus verstehen: Diejenigen, die mit Schrecken die Zahl der Ergebnisse beäugen, die die Eingabe ihres Namens in den Suchschlitz bei *Google* ergibt, obwohl sie selbst noch nicht einmal über eine eigene Webseite nachgedacht haben; diejeni-

gen, denen angst und bange wird, wenn sie bei *Google Earth*[2] nach ihrer Adresse suchen und sehen, dass dort der erst kürzlich im Garten eingerichtete Sandkasten bereits zu betrachten ist; diejenigen, die sich seit Jahren dem Netz und seinen Diensten verweigern, dort aber sehr wohl auffindbar sind. Ihre E-Mail-Adressen sind möglicherweise schon dem US-Amerikaner Mark Zuckerberg in die Hände gefallen, obwohl sie selbst noch nie einen Blick in *Facebook* geworfen haben. Ihre → WLAN-Daten, E-Mail-Adressen und Passwörter haben es in die Datenbanken des Internetgiganten *Google* geschafft, obwohl *Google* für seinen Straßenatlas → *Street View* nur ein paar Fotos der Häuserfassaden machen wollte.

All das macht Angst. Angst, dass Internetunternehmen bald nicht mehr nur über das Außenleben des privaten Heims Bescheid wissen, sondern auch detaillierte Informationen über dessen Innenleben haben. Oder sie wissen, was einen interessiert und können deswegen vorhersagen, was man als nächstes vorhat. Äußerungen wie die des ehemaligen *Google*-Chefs Eric Schmidt (»Wenn es etwas gibt, von dem Sie nicht wollen, dass es irgendjemand erfährt, sollten Sie es vielleicht ohnehin nicht tun«) oder die des *Facebook*-Gründers Mark Zuckerberg, der bereits die Privatsphäre für »überholt« erklärte, befeuern diese Angst zusätzlich.

3 Eine neue Einstellung zur Privatsphäre

Keine Frage: Mit dem Internet und seinen unzähligen Kommunikationswegen hat sich bei einer nicht unerheblichen Zahl der Deutschen die Einstellung zur Privatsphäre verändert. Immerhin mehr als 23 Millionen *Facebook-User* sehen hierzulande offenbar die soziale Komponente des Netzwerks so sehr im Vorteil, dass sie den laxen Umgang des Unternehmens mit ihren Daten zumindest hinnehmen.

Fakt ist: Das soziale Netz senkt Hürden. Nie war es einfacher, sich mit Hilfe sozialer Internetdienste eine eigene, virtuelle Identität aufzubauen, indem man ein paar Dinge aus seinem Leben preisgibt, Meinungen äußert oder Kompetenzen zeigt. Nie war es einfacher, mit Fremden Kontakt aufzunehmen, diesen zu pflegen oder eingeschlafene Freundschaften wiederzubeleben. Es war auch nie einfacher, an Informationen zu gelangen, weil sich innerhalb der Netzwerke sogenannte Subnetzwerke (oder Gruppen) bilden. Diese sind meist sehr spezialisiert und behandeln die abseitigsten Themen, die man sich vorstellen kann. Beispielsweise hatte die *Facebook*-Gruppe »Als ich in Deinem Alter war, war Pluto ein Planet« im Juli 2010 über eine Millionen Mitglieder.[3]

Online wird mehr über sich preisgegeben

Große Teile derjenigen, die sich bei *Facebook* und Co. tummeln, machen sich keine Gedanken darüber, was sie über sich selbst im Internet preisgeben. → *Twitter, Facebook* und andere soziale Netzwerke verleiten sie dazu, viel mehr über sich preiszugeben, als sie es normalerweise tun würden. Wer zu einem Vorstellungsgespräch geht, gibt sich in der Regel nicht nur durch ein gepflegtes Äußeres Mühe, einen möglichst guten Eindruck zu hinterlassen. Niemand präsentiert sich Partylieder grölend und mit Bierflasche in der Hand bei einem potenziellen neuen Arbeitgeber – in den sozialen Netzwerken allerdings schon. Fotos und Suffgeschichten sind dort auf ewig auffindbar, sorglos werden Kollegen oder Chefs als sogenannte Freunde hinzugefügt. Über die Konsequenzen sind sich die meisten jedoch nicht im Klaren. Nur die wenigsten nutzen die Einstellungen zur Privatsphäre und entscheiden, für wen welche Profilinformationen, Fotos und Videos einsehbar sind. Eine Antwort auf die Frage, ob sie dies aus Sorglosigkeit, Unachtsamkeit oder eventuell sogar wohlüberlegt tun (nach dem Motto: »Bringt ja eh nix«), kann ich nicht geben. Die Antwort würde mich auch interessieren (siehe hierzu auch den Beitrag von Wagner/Gebel/Brüggen in diesem Band, S. 226 ff.).

Ist der Protest gegen Datenerhebungen abgeflaut?

Wie passt das mit einer Gesellschaft zusammen, die noch in den 1980er Jahren gegen eine geplante Volkszählung auf die Straße ging und vor Gericht zog, weil die zu beantwortenden Fragebögen Rückschlüsse auf ihre Identität zuließen? Mittlerweile scheint es so, als ob die Diskussionen über den »gläsernen Bürger«, den Überwachungsstaat und die Datenskandale der vergangenen Jahre zu einer gewissen Abstumpfung geführt haben. In den zwanzig größten deutschen Städten erhoben lediglich 245 000 Menschen[4] Einspruch gegen die Abbildung ihres Hauses oder ihrer Wohnung bei *Googles* Straßenatlas *Street View*, obwohl die Medienmaschinerie das Thema wochenlang durchs Sommerloch prügelte.

Gibt man das Wort »Datenskandal« bei *Google* ein, so erscheinen über 220 000 Treffer, und auch die Vorschlagliste der Wörter, nach denen im Zusammenhang mit dem Begriff gesucht wird, ist lang und vielfältig: Große *Old-Economy*-Unternehmen sind darunter, ebenso wie internationale und nationale Internetkonzerne. Diese Fälle sorgten zwar jeweils für einen medialen Aufschrei, doch dabei blieb es meistens auch. Die Zahl derer, die das Internet mit seinen sozialen Komponenten nutzen, wurde dadurch nicht geringer, eher größer.

Natürlich gibt es auch die andere Seite, denn das dürfen wir nicht vergessen: Trotz aller Abstumpfung sind es eben »nur« rund 23 Millionen *Facebook-User* in Deutschland, also im Umkehrschluss rund 60 Millionen, die sich dieser Entwicklung bisher noch verweigern. Einige von ihnen können zwar mittlerweile mit Begriffen wie → *Weblogs*, *Twitter* oder *Youtube* etwas anfangen, für sie stellt aber eine per Handy verschickte SMS oftmals die höchstmögliche Form der digitalen Kommunikation dar. Ein paar von ihnen haben sich vielleicht schon einmal bei *Facebook* angemeldet, allerdings sofort wieder den Abmelde-Button betätigt. Sie waren vielleicht geschockt, weil das US-amerikanische Unternehmen gleich die eigenen Kinder, verloren geglaubte Schulfreunde oder die verhasste Ex-Freundin des Ehemanns als neue Kontakte empfahl. Sie haben Angst davor, durchsuchbar zu sein.

Dennoch stellt sich die Frage, ob die digitale Entwicklung mittlerweile so weit fortgeschritten ist, dass eben auch die Privatsphäre der »digitalen Besucher«[5] soweit verfügbar ist, dass eine komplette Verweigerung nichts mehr bringt, weil unsere digitale Durchsuchbarkeit nur noch eine Frage der Zeit ist.

4 Plädoyer für Aufklärung und Offenheit

Natürlich lauern in dieser Entwicklung auch Gefahren. Nie war es leichter, Identitäten zu missbrauchen. Wie einfach es geht, sich als eine fremde Person auszugeben, zeigt der Kurznachrichtendienst *Twitter.* Immer wieder machen sich Nutzende den Spaß und geben sich als jemand anderes aus. Das kann unterhaltsam sein, beispielsweise wenn plötzlich längst verstorbene Prominente wieder auferstehen und die aktuelle Weltlage auf ihre Weise interpretieren. Aber es kann auch nach hinten losgehen, wenn unter dem geklauten Namen plötzlich beleidigt, denunziert oder Falschinformationen verbreitet werden.

Hinzu kommt: Schon jetzt werden immer häufiger Daten von Privatpersonen für kriminelle Zwecke genutzt. Identitätsdiebstahl nennt sich dieses Delikt, das sich besonders in hoch technisierten Ländern verbreitet. Plötzlich flattern Rechnungen und Mahnungen ins Haus für Einkäufe, die man nie getätigt hat, und man stellt fest, dass die eigene Identität missbraucht wurde. Dabei kann es »nur« um einen kleinen Einkauf beim *Online*händler, aber auch um den Kauf eines Hauses oder die Aufnahme eines hoch verzinsten Kredits gehen. Betroffene müssen dann beweisen,

dass ihre Identität missbraucht wurde. Sie müssen in diesen Fällen Anzeige erstatten sowie Banken und Unternehmen informieren (siehe dazu auch den Beitrag von Schallbruch in diesem Band, S. 379 f.). Die Warnung der Polizei, sorgsam mit persönlichen Daten umzugehen, hilft nur zum Teil – ist es doch schwierig, zu kontrollieren, welche der Daten von Anderen entwendet oder veröffentlicht werden.

Fakt ist: Die Vorstellungen von Privatsphäre haben sich in den vergangenen Jahren verändert. Ich bin der festen Überzeugung, dass auch das sozialer werdende Internet diese Entwicklung unterstützt hat, obwohl der größere Teil der Deutschen nicht aktiv dazu beiträgt. Und ich werde keinen Versuch unternehmen, eine Art »besten Umgang« mit dem sozialen Netz zu propagieren, Tipps und Tricks für die digitale Kommunikation zu geben oder gar eine Art Regelkatalog aufzustellen über die »Dos und Don'ts« im Netz und wie man seine Privatsphäre am besten schützt. Ich plädiere für einen aufgeklärten und offenen Umgang auf beiden Seiten der Gesellschaft. Solange die Vorteile aus dem offenen Umgang mit den eigenen (und fremden) Daten die Nachteile überwiegen, wird die Zahl der Teilnehmer und Teilnehmerinnen an der digitalen Kommunikation weiter zunehmen, mit allen Konsequenzen.

Anmerkungen

1 Jeff Jarvis, Public Parts: How Sharing in the Digital Age Improves the Way We Work and Live, New York/London 2011.
2 *Google Earth* ist eine Software, die es den Nutzenden ermöglicht, die Erde aus einer Vogelperspektive zu betrachten.
3 Panagiotis Kolokythas, Lustige Facebook-Gruppen, in: PC Welt vom 30.7.2010, im Internet unter http://www.pcwelt.de/ratgeber/Ich-werde-Prinzessin-witzige-Gruppen-auf-Facebook-988720.html.
4 Jürgen Kuri, Google Street View: 244.237 Widersprüche, in: Heise Online vom 21.10.2010, http://heise.de/-1122375.
5 Peter Kruse, siehe: https://blog.whatsnext.de/.

Michael Seemann

Lasst die Daten, schützt die Menschen!

1 Informationelle Selbstbestimmung und *Social Media*

Als ich des Nachts mit einem Freund in Berlin unterwegs war und meinen Aufenthaltsort mit dem Kurznachrichtendienst → *Twitter* ins Internet posaunte, bat mich mein Freund, das doch zu lassen. Ich war leicht perplex. Wir kannten uns schon lange und ich weiß, dass auch er gerne twittert, wenn auch nicht ganz so viel wie ich. Er begründete seine Bitte damit, dass er seinerseits kurz zuvor getwittert habe, er sei im Begriff, mich zu treffen. Damit wäre ja nun bei all meinen → *Tweets* nicht nur öffentlich, was ich, sondern auch, was er mache – ohne, dass er es kontrollieren könne.

Informationelle Selbstbestimmung und → *Social Media* habe ich lange versucht, zusammen zu denken. Klar, man gibt Dinge über sich preis, man erweitert das Private in das Öffentliche und das wird einem oft genug vorgehalten, wenn man gleichzeitig an anderer Stelle Datenschutz anmahnt. Aber die informationelle Selbstbestimmung, wie sie das Bundesverfassungsgericht als Grundrecht definiert hat, sagt ja eben nicht, dass ich die Pflicht habe, mich zu verstecken, sondern nur, dass ich selbst entscheiden können soll, was jemand über mich weiß. Im Grunde gehört zum Recht der informationellen Selbstbestimmung eben auch, dass ich das Recht habe, alles, was ich will, über mich zu veröffentlichen, sei es auch noch so privat.

Ich habe daraufhin mein Handy ausgemacht und an diesem Abend nicht mehr getwittert. Das hat das »Problem« zwischen mir und meinem Freund gelöst. Aber das Grundproblem bleibt.

2 Von *Flickr* bis zur automatischen Gesichtserkennung

Das erste Mal, dass ich in einen solchen Interessenkonflikt geriet, war um das Jahr 2005 herum. In gewissen Kreisen war es gerade Mode geworden, seine digital geschossenen Fotos auf *Flickr* hochzuladen. Das ist ein mittlerweile fast historisch zu nennender Fotodienst im Internet. Menschen fühlten sich entblößt, weil Bilder von ihnen ohne ihre Genehmigung ver-

öffentlicht wurden. Fotos zu internetnahen Veranstaltungen landen nach wie vor dort zuhauf. Um *Flickr* werden bis heute erbitterte Diskussionen über Privatsphäre und das Recht am eigenen Bild geführt.

Ein anderes Beispiel: Im Sommer 2010 stand die Gesellschaft fassungslos vor dem → *Google Street View*-Auto, das in ihrer Straße entlang fuhr, um mit einer Kamera Aufnahmen der Häuserfronten für den digitalen Straßenatlas zu erstellen. Obwohl *Google* sich verpflichtet hatte, alle personenbezogenen Daten wie Gesichter oder Nummernschilder zu verpixeln, erschreckten viele angesichts dieser »Übernahme« des analogen Raumes durch die digitale Sphäre. Die zunehmende Gewissheit, dass die weißen Flecken im allwissenden Internet nach und nach getilgt werden, ist sicherlich einer der Gründe für die emotional geführte Debatte über den Straßenbilderdienst. Es scheint, als manifestiere sich die ganze Angst vor dem drohenden Kontrollverlust in diesem mit Kameras bestückten Wagen, der wie ein Besucher aus einer anderen Welt das Analoge in das Digitale verwandelt. Und das ungefragt.

Was viele nicht ahnen: Die Nachfolger von *Street View* sind gar nicht so auffällig wie das *Google*-Auto. Schon in den 1990er Jahren hat Steve Mann am *Massachusetts Institute of Technology* in Cambridge die ersten Experimente mit tragbaren, allgegenwärtigen Kameras gemacht. Vor wenigen Jahren dann wurde Justin Kan in den USA bekannt, der nicht nur sein Leben mehrere Monate lang 24 Stunden am Tag dokumentierte, sondern es ungefiltert direkt und in Echtzeit ins Internet stellte: *Justin.tv*. Damals musste er noch einen Rucksack mit Akkus und Festplatten mit sich herumschleppen. Heute sind entsprechende Gerätschaften in der Größe eines Hörgeräts zu haben. Der Akku ist hinten, die Kamera vorn, dazwischen ein Bügel zum »Hinters-Ohr-klemmen«. Damit kann die Kamera die Welt aus der Perspektive der Nutzenden erfassen und alles mitfilmen, was jene erleben, ohne dass sie selbst noch aktiv werden müssen. Kommt jetzt die komplett dokumentierte Welt, und alle machen mit?

Dabei haben wir aus dem Blick verloren, dass Kameras schon heute längst allgegenwärtig sind. Überall fotografieren die Menschen ihre Umwelt, vor allem mit dem Handy. Von dort bedarf es meist nur eines Knopfdruckes, um das Foto im Internet zu veröffentlichen. Die Frage, wie viele Bilder von jedem durchschnittlichen Deutschen bereits im Internet abrufbar sind, ohne dass er oder sie von ihnen wüsste, lässt sich schwer bis gar nicht beantworten. Fotografiert zu werden bemerkt man kaum noch – auf Partys, auf der Straße, bei Demonstrationen, vor Sehenswürdigkeiten oder nur mal so. Die Gelegenheiten sind vielfältig, niemand hat da mehr den Überblick. Aber das muss ja nicht so bleiben.

Gesichtserkennung in sozialen Netzwerken

Der neueste Trend ist es, die biometrische Gesichtserkennung – jahrelang nur von Polizei und Geheimdiensten eingesetzt – in Software für den Massenmarkt einzubauen (siehe zu Biometrie auch den Beitrag von Hansen, S. 78 ff.). Bei dem *Apple*-Dienst *iPhoto* und *Googles* Fotoverwaltung *Picasa* sind diese bereits Teil des Produktes. Lädt man bei *Facebook* ein Bild von Personen hoch, schlägt der *friend finder* einem automatisch vor, mit welchem Namen man das Bild »taggen«, das heißt markieren könnte. Es ist natürlich praktisch, wenn das Fotoprogramm meine Freunde automatisch anhand ihres Gesichtes erkennt und richtig einsortiert. Auch auf *Facebook* erleichtert die Gesichtserkennung das Versehen von Fotos mit Namen ungemein und fördert die Kommunikation und Vernetzung. Ob die »getaggte« Person damit allerdings einverstanden ist, stellt sich oft erst im Nachhinein heraus. *Apple* hat für viel Geld die Firma *Polar Rose* aus diesem Bereich akquiriert. *Google* forscht ebenfalls intensiv an besseren Algorithmen zur Gesichtserkennung. So wird es nicht lange dauern, bis alle diese Bilder von uns, von denen wir bislang nichts wussten, durch eine entsprechende Suchanfrage bei *Google* zutage gefördert werden.

Verknüpfungsmöglichkeiten bestehender Datensätze

Egal ob Bilderfassung und -auswertung oder *Twitter*-Verknüpfung – diese Verfahren haben eines gemeinsam: Sie basieren darauf, dass mit der digitalen Technik heute in Echtzeit Analysen und Verknüpfungen zwischen Daten generiert werden können, die unsere bisherigen Vorstellungen übertreffen. Der einzelne Datensatz liegt eben nicht mehr tot an seinem Speicherplatz, sondern wird durch immer neue Verknüpfungsmethoden »angereichert«. Im professionellen Umfeld nennt man das → *Datamining*, → *Targeting* oder → *Monitoring*. Im privaten Nutzungsumfeld gibt es andere Namen dafür: »Adressbuchsynchronisation«, »Bilderverwaltung« oder schlicht »*Google*-Suche«. Die ordnenden und verknüpfenden Algorithmen, die hier zum Einsatz kommen, erreichen schon heute eine ungeahnte Tiefe und Komplexität.

Vorhandene Datensammlungen sind nicht mehr überschaubar

Was gestern ein Text war, ist heute ein Fingerabdruck. Was gestern ein Bild war, ist morgen eine Datenbank. Was heute eine Statusnachricht ist, die nur aus meinem Leben berichtet, findet bereits jetzt Eingang in ein Gewebe von Hinweisen, Verknüpfungen und Relationen, die ich – und schlimmer noch: mein Umfeld – nicht mehr überschauen kann. Zusammen bilden sie ein undurchschaubares, engmaschiges Netz, dessen Lücken durch geschicktes Verknüpfen und algorithmisches Kombinieren mehr und mehr geschlossen werden. Wir leben in beschleunigten Zeiten. Wir leben an der Grenze zur »Echtzeitarchäologie«, in der unsere eigene unmittelbare Vergangenheit mit neuen Analysemethoden in einer ungeahnten Transparenz aufgeht. Seien wir ehrlich: Wir wissen so wenig über das, was unsere Daten in fünf Jahren aussagen werden, wie die ägyptischen Pharaonen die Radiokohlenstoffanalyse erahnen konnten.

3 Toleranz statt Datenschutz

Ich gebe es zu: Ich habe die Kontrolle verloren und – noch viel entscheidender – alle anderen mit mir. Nicht nur die intensiven Nutzer und Nutzerinnen des Internets und der digitalen Medien, sondern vor allem auch alle anderen, die mit uns zusammenleben, können sich ihrer Daten nicht mehr sicher sein. → *Blogger* sind wie Glühbirnen. Indem sie über ihr Leben

berichten, beleuchten sie nicht nur sich selbst, sondern bringen alles um sich herum ans Licht.

Es wird Zeit, dass sich die Gesellschaft fragt, wie sie mit den veränderten Bedingungen umgehen will. Und dies nicht erst morgen, denn Transparenz ist bereits jetzt ein Massentrend. Die Toleranz im Umgang mit den eigenen Daten hat sich in den letzten Jahren rapide verändert. Mehr als ein Zehntel der Menschen weltweit ist mittlerweile auf *Facebook*[1] und teilt Bilder, Statusupdates, Texte, Meinungen und seit neuestem auch Aufenthaltsorte miteinander. Auf dem Rest der Menschheit lastet ein riesiger Gruppenzwang. Wer Teil der Welt ist, wird entweder auch Teil des Internets sein oder als Eremit sein Leben fristen. Die Transparenz der Welt wird derweil weiter steigen und sicherlich noch das eine oder andere Chaos stiften.

Datenschutz ist kein angemessenes Instrument

Ich will die Gefahren nicht kleinreden. Nur weil einige unbesorgt ihre Welt in ein Diorama verwandeln, heißt das nicht, dass es keine Menschen gibt, die ein existentielles Interesse am Schutz ihrer Privatsphäre haben. Der schwule Krankenpfleger in der katholischen Einrichtung in Bayern hat mit Sicherheit ein höheres Bedürfnis nach Datenschutz als ein freier Publizist in Berlin. Wir müssen aber aufhören, so zu tun, als sei für diese Art von Problemen der gesellschaftliche Schutzraum namens Datenschutz langfristig ein probates Mittel. Er ist es heute nur unzureichend, und wird es in Zukunft immer mehr sein.

Datenschutz kann zwar noch die Symptome lindern, indem er spezielle Eigenschaften des Einzelnen für die intolerante Gesellschaft versteckt. Solche Maßnahmen bleiben allerdings ein Rückzugsgefecht und keine wirkungsvolle – nicht einmal eine wünschenswerte – Option für die Zukunft. Auf dem Weg in die transparente Gesellschaft ist es höchste Zeit, die gesellschaftlich-kulturellen Rahmenbedingungen zu verändern.

Das Netz macht die Gesellschaft sich selbst gegenüber transparent. Mit anderen Worten, es hält ihr den Spiegel vor. Dabei merken wir, wie rückständig wir immer noch sind und wie wir nach wie vor an unseren eigenen, ach so fortschrittlichen Ansprüchen scheitern. Darin steckt auch eine Chance. Eine Chance für einen echten kulturellen Wandel, der nicht nur eine fortschrittliche und tolerante Fassade vor die Mauer des Privaten nagelt. Die Mauer der Verschwiegenheit schützt nicht nur die Anderen vor der Intoleranz, sondern vor allem auch die Intoleranz selbst.

Gesellschaftliche Vorteile geteilter Informationen

Anstatt sich also in Panik an alte Gewissheiten und nicht durchsetzbare Rechte zu klammern, die in der alten Welt der Mauern und Entfernungen gegolten haben, sollten wir lieber neue Freiheiten aus den mannigfaltigen Möglichkeiten schöpfen, die als Potenzial in den neuen Informationsmedien schlummern. Und das passiert bereits. All jene, die den Mehrwert geteilter Informationen am eigenen Leib erfahren haben, verlieren die Scheu davor, ihre Daten freizugeben. Gerade der Andersartige findet im Internet Gemeinschaft. Nirgendwo sonst lassen sich schneller Vorurteile überwinden und Verständnis schaffen – und zwar durch Transparenz. Die Daten kommen auch ohne unseren Schutz aus. Angreifbar bleibt das Individuum. Der beste Schutz für den Menschen aber besteht in einer freien, offenen und toleranten Gesellschaft.

Anmerkung

1 Quelle: http://www.facebook.com.

Frank Spaeing / Thomas Spaeing

Datenschutz geht zur Schule

1 Die Initiative »Datenschutz geht zur Schule«

Datenschutzbeauftragte werden bei der Ausübung ihres Berufes regelmäßig damit konfrontiert, dass viele Menschen den digitalen Medien überaus hilflos gegenüberstehen. Aufgrund der positiven Resonanz auf erste Workshops in Schulen, sowohl von Seiten der Medien als auch von Schülerinnen und Schülern, wurde daher 2008 die Initiative »Datenschutz geht zur Schule« im Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.[1] gegründet. Der BvD verfolgte damit mehrere Ziele:

- Ein möglichst bundesweites Angebot für Schulen zu schaffen, um Jugendlichen das notwendige Rüstzeug für die digitale Welt zu geben.
- Mit Hilfe der Bekanntheit und der Möglichkeiten des BvD eine breitere Öffentlichkeit zu erzeugen, um auf das Defizit in der Schulausbildung hinzuweisen.
- Langfristig auf eine nachhaltige Lösung zur Beseitigung des Aufklärungsdefizits hinzuwirken, die nur unter Beteiligung der zuständigen öffentlichen Stellen erreicht werden kann.

2 Datenschutz und *Digital Natives*

Gerade bei zahlreichen Gesprächen mit Politikerinnen und Politikern mussten die Aktiven des BvD immer wieder feststellen, dass ein vollkommen falsches Bild von den Kenntnissen der Jugendlichen herrscht. Da wurde von → *Digital Natives* gesprochen, die besser als alle anderen wüssten, was sie im Netz tun. Teilweise wurde sogar nach dem Sinn von Datenschutzgesetzen gefragt, wo doch heute nahezu jede Person im Internet zuhause sei. Dem stehen Untersuchungen[2] entgegen, die zeigen, dass es in jeder Generation *Digital Natives* gibt, die neue Medien intensiv nutzen – aber die Risiken eben oft nicht richtig einschätzen können. Eine Vielzahl der Jugendlichen und jungen Menschen, die gerne dieser neuen Spezies zugerechnet werden möchten, nutzt die digitalen Medien wie ihre Eltern den Fernseher oder das Telefon. Sie haben aber keine ausreichende Erfahrung, um mögliche Gefahren zu erkennen. Tatsächlich hat sich in

den durchgeführten Workshops ein eklatanter Aufklärungsbedarf gezeigt, wie die folgenden Beispiele zeigen:

- Zahlreiche Jugendliche haben bereits Erfahrungen mit der Staatsanwaltschaft aufgrund von illegalen Downloads gemacht. Keiner war sich der rechtlichen Zusammenhänge bewusst und alle sahen Downloads eher als Sport.
- Noch mehr Jugendliche sind bereits »Internetabzockern« zum Opfer gefallen und haben unnötig Beträge gezahlt, um sich von den falschen Anschuldigungen zu befreien.
- Viele Schülerinnen und Schüler sind bereits in Chatrooms von dubiosen Teilnehmern angesprochen worden und sollten zu Treffen verleitet werden.
- Häufig geben die Jugendlichen bereitwillig all ihre Daten und oft auch die der Eltern an, vor allem wenn Gewinnchancen und Vorteile versprochen werden, die es oft nicht gibt.
- Ein Hacker, der sich gezielt in die Computer von Schülerinnen eingeschlichen hatte, um mit deren *Webcam* das Kinderzimmer permanent zu filmen, wurde bei einer Veranstaltung entdeckt. Die Ermittlungen gegen diesen »*Webcam*-Spanner« hat dann die Staatsanwaltschaft übernommen.
- Viren, Würmer und → Trojaner finden in dieser Zielgruppe leicht Opfer, da kaum an Schutzmaßnahmen gedacht wird.

Der Bedarf an Aufklärung und Wissensvermittlung in diesem Bereich ist gewaltig. Die Initiative »Datenschutz geht zur Schule« erhält erheblichen Zulauf, sowohl von Datenschützern als auch von Schulen. Zudem nimmt die Politik das Thema Datenschutz deutlicher wahr und es melden sich immer neue Unternehmen, die das Projekt – meist regional – unterstützen möchten.

Trotzdem stellen die Aktivitäten nur einen Tropfen auf den berühmten heißen Stein dar, denn schon längst übersteigen die Anfragen von Schulen die Möglichkeiten der ehrenamtlich tätigen Datenschützer bei weitem. Es gilt also, die Erfahrungen und Kapazitäten in ein umfassenderes Projekt zu überführen, um diese Aufgabe mit dem gebotenen Ernst als eine öffentliche wahrzunehmen.

3 Wie arbeitet die Initiative »Datenschutz geht zur Schule«?

Die Initiative erarbeitet und pflegt die Schulungsunterlagen, kümmert sich um die begleitenden Dokumente (beispielsweise zur Qualitätsmessung) und legt in Abstimmung mit dem BvD-Vorstand die Regeln für die Arbeitsweise der Initiative fest. Hier werden die Kriterien für Dozenten und Dozentinnen sowie Mentoren und Mentorinnen definiert und deren Einhaltung überwacht.

Alle Veranstaltungen sind für die Jugendlichen (und damit auch für die Schulen) kostenfrei. Auf Wunsch einer Schule können auch, gegen ein geringes Entgelt, Veranstaltungen für das Lehrpersonal und/oder Eltern durchgeführt werden. Da die Schülerveranstaltungen kostenfrei sind (und dies auch bleiben sollen), für die Dozenten und Dozentinnen aber mitunter durchaus hohe Aufwendungen entstehen, werden eventuelle Anfahrts- und Übernachtungskosten bis zu einer festgelegten Höhe aus den eingenommenen Sponsorengeldern gezahlt.

4 Vorbereitung und Ablauf einer Schulung

Wenn eine Schule von der Initiative erfahren hat und daran teilnehmen möchte, meldet sie sich bei der Geschäftsstelle des BvD. Hier werden die Anfrage aufgenommen und der für die Region zuständige Dozent oder die Dozentin benachrichtigt. Es wird dann ein Erst-Termin vor Ort in der Schule vereinbart. Dabei werden die wesentlichen Projektparameter besprochen: ehrenamtliche Tätigkeit, Zeitumfang (90 Minuten je Gruppe), Gruppenstärke (maximal 60 Schülerinnen und Schüler), Anzahl der Veranstaltungen pro Tag (drei bis vier, je nach Stundenplan und Ausdauer des Dozierenden), benötigte technische Voraussetzungen sowie eventuell schon konkrete Termine. Dabei wird ein »Vor-Ort-Treffen« angestrebt, so dass die Schule weiß, wer mit den Jugendlichen arbeitet und auch geprüft werden kann, ob »die Chemie stimmt«.

Vorbereitende Recherche

Kurz vor dem konkreten Veranstaltungstermin recherchiert der Dozent oder die Dozentin üblicherweise in den einschlägigen sozialen Netzwerken, um gegebenenfalls konkrete Informationen über die Kinder und Jugendlichen herauszufinden. In manchen Klassen, in denen es schon Fälle von *Cyber-Mobbing*[3] gab, lässt er oder sie sich über diese ins Bild setzen, um

keine weiteren unerwünschten Eskalationen während des Vortrags zu provozieren. Die Vorträge sind entweder für die 5. bis 9. Klasse oder für die 10. bis 13. Klasse ausgelegt.

Die Präsentationsunterlagen für die 10. bis 13. Klasse enthalten neben Pressemeldungen zu allgemeinen Datenschutzthemen auch Informationen zu Gesetzen und altersgerechten Themen, die üblicherweise erst Jugendliche dieser Altersklassen interessieren (beispielsweise über Versicherungen, Banken, → Auskunfteien, Kartensysteme, Einwohnermeldeämter, Finanzämter). Hier sind manche Videos anspruchsvoller und die Folien stellen komplexere Sachverhalte dar (beispielsweise Recherche nach einer Person anhand eines Nicknamens im Internet). Ansonsten gleicht die Präsentation derjenigen, die für die 5. bis 9. Klasse genutzt wird.

Ablauf einer typischen Veranstaltung in der Schule

Die Veranstaltung beginnt mit einer knappen Vorstellung der Initiative und des Dozenten oder der Dozentin. Dabei werden die Jugendlichen ermuntert, während des Vortrages jederzeit Zwischenfragen zu stellen. Diese Möglichkeit nutzen die meisten Gruppen reichlich. Nach einem Einstieg in die Thematik über den arg strapazierten Begriff der »Freunde« in sozialen Netzwerken wird mit einem kurzen Film aufgezeigt, was heutzutage technisch alles realisierbar ist und es wird mit den Jugendlichen diskutiert, ob und inwieweit diese Möglichkeiten auch tatsächlich genutzt werden.

Nach dieser ersten meist angeregten Diskussion mit den Jugendlichen wird nach der Vorstellung der Agenda der Veranstaltung der Begriff des Datenschutzes erläutert. Altersgemäß wird hier nicht auf Gesetze eingegangen, sondern der Begriff wird den Jugendlichen in anschaulichen Beispielen (etwa durch Gleichsetzung mit einem Geheimnis) verdeutlicht und durch Filme unterlegt.

Nach der Darstellung, was persönliche Daten (entsprechend dem im Gesetz genutzten Begriff der personenbezogenen Daten) alles sein können (über Name, Telefonnummer und Schulnoten bis hin zu den Informationen über die realen Freunde), wird den Jugendlichen gezeigt, wer alles ein berechtigtes Interesse an der Nutzung der persönlichen Daten hat (etwa der Staat oder die Schule), wem sie ihre Daten gerne auch freiwillig geben (zum Beispiel Vereinen) und wer die Daten sonst noch haben möchte und auch vor illegalen Praktiken nicht zurückschreckt, um an sie zu kommen (wie etwa Betrüger).

Der etwa einstündige zentrale Teil der Veranstaltung umfasst insgesamt neun Themenkomplexe, die im Vortrag, der durch Folien und Filme angereichert wird, ausführlich behandelt und diskutiert werden:

Soziale Netzwerke

Der erste Bereich beschäftigt sich mit dem →Web 2.0. Hier wird im Wesentlichen versucht, die Jugendlichen davon zu überzeugen, dass sie in Zukunft vor dem Einstellen irgendwelcher intimen oder persönlichen Informationen in →sozialen Netzwerken wie beispielsweise *Facebook* oder SchülerVZ über die Folgen dieser Veröffentlichung nachdenken. Sie werden darüber informiert, dass zum einen die Personalverantwortlichen in den Unternehmen (unabhängig von der geltenden Gesetzeslage) natürlich im Vorfeld einer Beschäftigung versuchen werden, sich durch Internetrecherchen ein Bild von zukünftigen Beschäftigten zu machen. Zum anderen lassen sich aber auch potentielle Straftäter nicht durch freiwillige Zugangsbeschränkungen (beispielsweise Altersverifikation bei sozialen Netzwerken für Jugendliche) davon abhalten, diese Plattformen zu nutzen, um Informationen über mögliche Opfer einzuholen.

Videochats

Über einen anschaulichen Film zum Thema Videochat wird dann der Bogen zur Problematik von *Webcams* geschlagen und der Fall des »*Webcam*-Spanners« ausführlich beschrieben, damit die Jugendlichen auch hier sensibilisiert sind und wissen, wie sie sich vor solchen Missbrauchsversuchen schützen können. Dieser Fall ist – wie die meisten Beispiele – erst im Zusammenhang mit der Initiative »Datenschutz geht zur Schule« publik geworden. Solche Beispiele werden immer wieder herangezogen, weil sie authentisch und nicht konstruiert sind.

Handy

Den Jugendlichen wird zum Thema Handy gezeigt, wie schnell sie mit ihren Geräten zu orten sind. In jeder Gruppe hat mindestens eine Person ein Handy eingeschaltet, →*Bluetooth* aktiviert und auf sichtbar geschaltet. Meist macht sich Betroffenheit breit, wenn beschrieben wird, wozu diese Sichtbarkeit alles genutzt werden kann. Die Themen →*Tracking* und Schutz der auf dem Mobiltelefon enthaltenen Daten werden ausführlich behandelt.

Abzockfallen

Nach einer kurzen Darstellung des unsicheren Mediums E-Mail werden die »Abzockfallen« im Internet vorgestellt. Die Jugendlichen werden über die wichtigsten Betrugsmethoden informiert und es wird dargestellt, wie sie sich in einem solchen Fall verhalten sollten.

Urheberrechte

Beim nächsten Themengebiet – Urheberrechte im Internet – wird umfassend dargestellt, woran illegale Downloads von Video- und Audiodateien zu erkennen sind. Dieses Thema wird nicht als reines Verbot dargestellt, vielmehr werden auch legale Alternativen gezeigt – etwa das Mitschneiden von Internetradiosendungen. Da die für illegale Downloads zu erwartenden Strafen und Abmahngebühren benannt werden, ist dieser Teil der Veranstaltung für viele Jugendliche mehr als ernüchternd.

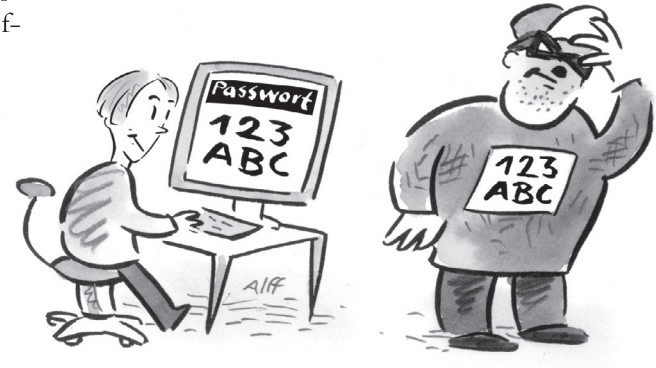
Internet

Um einen Wiederholungseffekt zu erzielen, wird im nächsten Themenkomplex allgemeiner auf das Internet eingegangen. Hier wird zusammen mit den Jugendlichen erarbeitet, dass das Internet zwar eine quasi allumfassende Informationsquelle ist, aber auch nichts vergisst. Fast niemand ist beispielsweise vor der Gruppe bereit, zu sagen, dass er einmal Fan der Band Tokio Hotel war oder es immer noch ist. Anhand dieses einfachen Beispiels und eines inhaltlich zum Thema passenden Films wird den Jugendlichen klar, dass einmal veröffentlichte Informationen (beispielsweise das Posting »Super Konzert von Tokio Hotel!!!«) nur noch sehr schwer (wenn überhaupt) aus dem Medium Internet wieder entfernt werden können.

Sichere Passwörter

Als wichtige Schutzmaßnahme wird das Thema Passworte mit den Jugendlichen behandelt. Es werden anhand passender Übereinstimmungen Regeln für Passworte verdeutlicht und dann mit entsprechenden Tabellen aufgezeigt, wie schnell Passworte per *Brute-Force*-Attacke [4] »geknackt« werden können. Es wird den Jugendlichen aufgezeigt,

- wie gute, sichere Passworte prinzipiell aufgebaut sein müssen,
- dass es sinnvoll ist, für verschiedene Webseiten verschiedene Passworte zu haben,
- wie einfach zu merkende und trotzdem starke Passworte erzeugt werden können.



Dieses Thema der Veranstaltung hat unserer Erfahrung nach die direktesten Konsequenzen. Wir erhalten oft die Rückmeldung, dass die Mehrzahl der Jugendlichen (und auch des Lehrpersonals) im Anschluss an die Veranstaltung ihre Kennworte ändert.

PC-Sicherheit

Der PC-Sicherheit ist eine eigene Folie gewidmet, die auf Schutzmechanismen wie Virenscanner, → *Firewalls*, *Updates*, → WLAN-Verschlüsselung und Datensicherung eingeht. Speziell die Datensicherung ist für Jugendliche ein Thema, bei dem sie unruhig werden, da sie sich über die »Sterblichkeit« ihrer Technik bisher meist keine Gedanken gemacht haben.

Cyber-Mobbing

Das Thema *Cyber-Mobbing*[5] schließlich ist an vielen Schulen schon präsent. Hier informieren wir die Jugendlichen über die technischen Möglichkeiten, mit denen »Mobber« dingfest gemacht werden können, sowie über die geltenden Gesetze. Wir möchten den Schülerinnen und Schülern damit klarmachen, dass Betroffene durchaus Chancen haben, sich zu schützen.

Abschließende Verhaltensregeln

Wenn die letzten Diskussionen beendet sind, kommt die abschließende Folie, auf der wir den Jugendlichen sieben Verhaltenstipps mit auf den Weg geben:

- Schütze dich und deine Daten.
- Sei misstrauisch, glaube nicht alles.
- Halte dein Passwort geheim.
- Keine illegalen Downloads.
- Vorsicht bei Treffen mit *Cyber*-»Freunden«.
- Sei auch im Netz immer fair.
- Bist du unsicher, frage nach.

Hier werden den Jugendlichen die wesentlichen Punkte erneut kurz ins Gedächtnis gerufen. Die letzte Folie bietet noch einmal die Gelegenheit, Fragen innerhalb der Gruppe zu stellen. Meistens aber haben die Jugendlichen Fragen, die sie individuell klären möchten. Regelmäßig gibt es euphorische Verabschiedungen durch die Jugendlichen, was uns bestätigt, dass die Schülerinnen und Schüler diese Veranstaltung für sich als Gewinn erlebt haben.

Anmerkungen

1 Der Berufsverband der Datenschutzbeauftragten Deutschland (BvD) e. V. wurde 1989 mit dem Ziel gegründet, die beruflichen Interessen der betrieblichen und behördlichen Datenschutzbeauftragten zu unterstützen, im Internet unter https://www.bvdnet.de

2 Siehe zu allgemeinen Informationen über das Nutzungsverhalten in bestimmten Altersgruppen die jährliche Studie »(N)Onliner, die von der Initiative D21 durchgeführt wird, im Internet unter http://www.intiative21.de (Anm. d. Red.)

3 *Cyber-Mobbing* (*Mobbing* bedeutet schikanieren, pöbeln) bezeichnet ein Verhalten, bei dem eine andere Person etwa in sozialen Netzwerken oder über andere internetbasierte Anwendungen beleidigt, herabgesetzt oder bloßgestellt wird.

4 Bei der *Brute-Force*-Methode werden alle möglichen Zeichenkombinationen der Reihe nach ausprobiert, um eine Passwort- oder Zugangssperre zu überwinden. Üblicherweise beginnt ein solcher Angriff und die Suche nach dem richtigen Passwort mit dem Test der gebräuchlichsten Passworte. Bei der heutigen Rechengeschwindigkeit von Computern lassen sich so zahlreiche Passwortkombinationen innerhalb kurzer Zeit prüfen.

5 Siehe Anm. 3.

»Wenn du dich nicht als die Person präsentieren willst, die du bist, solltest du nicht unseren Dienst nutzen«

Richard Allen, Director of European Public Policy bei Facebook, arbeitet als oberster Datenschützer des Unternehmens in Europa mit den Regulierungsbehörden und Politikverantwortlichen der Europäischen Union zusammen.

Das Gespräch führte Lars Reppesgaard Ende Dezember 2010.

Richard Allen, womit beschäftigen Sie sich als *Director of European Public Policy*?

Unser Team und ich sind vor allem Ansprechpartner für Politiker, Regierungen, Verbände und Organisationen und helfen dabei, *Facebook* zu verstehen und einzusetzen. Außerdem habe ich die Aufgabe, mich mit allen politischen Fragen zu beschäftigen, die für *Facebook* relevant sind. Fragen des Datenschutzes und der Privatsphäre gehören hier natürlich zu den wesentlichen Themen, mit denen ich mich beschäftige. Sie machen etwa ein Drittel des Zeitbudgets aus. Wichtig ist bei meiner Arbeit auch ein Thema wie Datensicherheit, aber auch die Redefreiheit. Wo gilt sie noch, wo endet sie? Welche Regeln müssen wir für sie auf unserer Plattform aufstellen? Hier gibt es von Land zu Land oft unterschiedliche Auffassungen.

***Facebook* ist ein amerikanisches Unternehmen, das international agiert. Welches Datenschutzrecht gilt eigentlich für so ein globales Internetunternehmen? An wen wende ich mich als *Facebook*-Nutzer oder als Datenschützer in Deutschland?**

Wir sind tatsächlich ein globales Unternehmen. Wir versuchen also, Dienste für eine globale Nutzerbasis anzubieten und ihre Ansprüche zu erfüllen.

Deutsche *Facebook*-Nutzerinnen und -Nutzer haben formell einen Vertrag mit *Facebook* Irland, dort ist unsere Europazentrale. Dort gibt es Ansprechpartner wie mich, dort können *Facebook*-Mitarbeiterinnen

und -Mitarbeiter Nutzerdaten kontrollieren. Wir haben die → *Safe Harbour*-Vereinbarungen der Europäischen Union unterzeichnet. Es ist unser Anspruch, dass die Daten, auch wenn sie in den Vereinigten Staaten gespeichert werden, auf ähnliche Weise geschützt werden wie bei einem europäischen Unternehmen.

Es gibt also drei Schichten bei den Regeln, die für uns gelten: die US-Gesetzgebung, denn die Daten liegen physisch in den Vereinigten Staaten; dann die EU-Regeln, und zuletzt auch spezifische Regeln in den lokalen Märkten. Auch die sind wichtig. Wir sagen nicht: »Okay, das hat nichts mit uns zu tun, denn die Daten sind ja in den USA.«

Wie würden Sie das Verhältnis zu den Datenschutzbeauftragten in Deutschland beschreiben?

Wir stehen häufig in Kontakt mit vielen Datenschutz-Beauftragten aus Ländern wie etwa Spanien, Frankreich, Italien, Irland, aber natürlich auch Deutschland. Wir arbeiten vor allem mit ihnen zusammen, um strittige Fragen zu lösen. Meist ist dieses Zusammenspiel sehr positiv. Die Behörden sprechen Punkte an, die für Beunruhigung sorgen, so dass wir Verbesserungen für die Nutzenden entwickeln können. Mitunter gibt es aber auch Themen, die eine größere Herausforderung darstellen, etwa wenn es um Dinge geht, die für unser Geschäftsmodell von fundamentaler Bedeutung sind.

Was sind das für Streitpunkte?

Das sind etwa Fragen, die sich darum drehen, dass man auf *Facebook* nicht anonym sein oder sich mit einer Scheinidentität anmelden kann. Wir sprechen uns sehr für diese Bestimmung aus, was nicht jeder für richtig hält. Von dieser Bestimmung abzurücken, würde aber absolut unserem Geschäftsmodell widersprechen, so dass wir von ihr nicht einfach abrücken können, um Bedenken auszuräumen. Wir sagen: »Wenn Du Dich nicht als die Person präsentieren willst, die Du bist, solltest Du nicht unseren Dienst nutzen, sondern einen anderen, wo man sich vielleicht ›Mickymaus123‹ nennen kann.« Die Wahl hat man. Man kann aber nicht unseren Dienst nutzen und dann verlangen, dass wir etwas ganz anderes daraus machen.

Dass *Facebook* keine anonymen *Online*profile erlaubt, ist sicher ein grundsätzlicher Streitpunkt, wenn es um das Thema Datenschutz geht. In vielen Auseinandersetzungen mit den deutschen Daten-

schützern geht es aber auch um bestimmte Teile ihres Dienstes, zum Beispiel den *Friend Finder*, bei dem Nutzende ihre E-Mail-Adressbücher hochladen können. Die Anwendung nutzt Kontaktdaten auch von Menschen, die *Facebook* nicht nutzen. Das mag die Suche nach Freunden auf *Facebook* erleichtern, ist aber etwas, was Deutschlands Datenschützer im Jahr 2010 inakzeptabel fanden. Geht *Facebook* auf solche Einwände ein?

Das ist zum Beispiel ein Punkt, an dem wir bereit waren, uns mit den deutschen Datenschützern zu einigen. Nach ihren Einwänden haben wir einiges an dem Dienst verändert. Bei solchen Dingen können wir Veränderungen anbieten.

Was ist mit dem »Gefällt mir«-*Button*, mit dem *Facebook*-Nutzende Webseiten, Artikel, Fotos oder Videos anderen *Facebook*-Nutzenden empfehlen können? Er ist in hunderttausenden deutschen Webseiten integriert. *Facebook* kann darüber das Verhalten von Nutzerinnen und Nutzern auf den Webseiten, auf denen der Knopf angebracht ist, verfolgen. Auch das hielten deutsche Datenschützer 2010 für problematisch.

Hier ist die Frage, ob jemand *Facebook* nutzt oder nicht. Ist jemand *Facebook*-Nutzer, so ist in den Nutzungsbedingungen festgelegt, welche Informationen auch auf diese Weise gesammelt werden dürfen. Problematisch wird es, wenn diejenigen, die keine *Facebook*-Nutzenden sind, von der Datenübertragung betroffen sind. Der strittige Punkt ist, ob auch ihre Daten an *Facebook* geschickt werden dürfen. Wir lösen das so: Auf deutschen Webseiten, auf denen der »Gefällt mir«-*Button* integriert ist, speichern wir nicht die genaue Webadresse der Nutzenden, sondern nur die generell deutsche →IP-Adresse.

In Detailfragen geht *Facebook* also auf Anregungen von behördlichen Datenschützern ein. Wie würden Sie das Verhältnis des Unternehmens zu Verbraucherschutzorganisationen charakterisieren, die ja in Deutschland auch in der öffentlichen Diskussion um den Datenschutz ein gewichtiges Wort mitreden? Der Verbraucherzentrale Bundesverband hat immer wieder an *Facebook* Kritik geübt und geht mitunter auch mit juristischen Mitteln vor, weil *Facebook* fortlaufend gegen deutsche Datenschutzstandards verstoßen soll …

Ich denke, solche Probleme anzusprechen, gehört nicht zu ihrem Aufgabenbereich. Uns hilft es nicht weiter, dass auch diese Institutionen beginnen, über Datenschutzfragen zu sprechen. Natürlich gibt es Verbraucherschutzregelungen, und denen versuchen wir natürlich gerecht zu werden. Aber es gibt behördliche Institutionen, die in Deutschland für den Bereich des Datenschutzes zuständig sind. Wir hoffen, dass wir nicht mit lauter unterschiedlichen Organisationen in einem Land sprechen müssen, wenn es um Datenschutz geht. Wir versuchen, wenn es geht, mit global einheitlichen Unternehmensregeln zu arbeiten. Wenn wir 150 kleine Ausnahmen definieren müssten, wären sie sehr komplex. Wenn eine Änderung rechtlich zwingend erforderlich ist, verändern wir etwas. Aber unser erstes Bestreben ist es, die Dinge nicht zu variieren.

In anderen Netzwerken ist ja die Möglichkeit, Pseudonyme zu nutzen und in andere Identitäten zu schlüpfen, auch eine Methode, um das Netz nutzen zu können, ohne allzu viel Persönliches preiszugeben. Würden Sie mir zustimmen, dass *Facebook* mit seinem Wunsch nach absoluter Authentizität der Nutzenden eine besonders große Verantwortung für die Daten trägt, die man dem Unternehmen anvertraut?

Ja, deswegen stecken wir viel Arbeit in das System, um die Daten sicher aufzubewahren und den Nutzenden die Kontrolle darüber zu geben, wie ihre Daten bei *Facebook* genutzt werden. Wir sagen, die Daten gehören ihnen, und wir wollen sie so mit anderen teilen, wie sie es uns sagen.

In der Vergangenheit gab es viele Irritationen, weil Nutzerinnen und Nutzer die Möglichkeiten, die Verbreitung der von ihnen hinterlegten Informationen zu managen, extrem verwirrend fanden. Zudem hat *Facebook* ja die Regeln, nach denen Informationen publik gemacht werden, mehrfach geändert, wodurch sich einige Nutzende überrumpelt fühlten.

Ich denke, oft werden unsere Änderungen auch missverstanden. Wir haben beispielsweise definiert, dass ein Profilfoto im Gegensatz etwa zu privaten Fotos grundsätzlich öffentlich einsehbar ist. Das wurde kritisiert. Aber ein Profilfoto wird an so vielen Stellen im Netz automatisch abgebildet, dass man es tatsächlich nicht kontrollieren kann, wo es zu sehen ist und wer es sieht. Da sehen wir es als ehrlich an, so etwas deutlich zu machen. Bei privaten Fotos ist das natürlich etwas anderes, die soll und kann nicht jeder sehen.

Kann man die ständigen Auseinandersetzungen um *Facebook*-Dienste damit erklären, dass *Facebook* so jung ist? Dass man noch ständig experimentiert und auf der Suche ist? Der amerikanische Technologie-Experte Tim O'Reilly hat einmal gesagt, er erwarte von Unternehmern wie dem *Facebook*-Gründer Mark Zuckerberg, dass sie Dinge entdecken, von denen die Nutzenden noch gar nicht wissen, dass sie sie wollen. Und dass es dabei natürlich passieren kann, dass man bei der Suche nach diesen Entdeckungen mitunter auch zu weit geht …

Eigentlich nicht. Mark Zuckerberg, der Gründer von *Facebook*, hat eine klare Produktvision. Er hat viele Ideen und ein gutes Gespür dafür, welche Dienste die Leute in Zukunft wollen. Manchmal gibt es bei Änderungen zuerst Protest. Es gab Fälle, bei denen Millionen von Nutzenden nach Veränderungen gesagt haben: »Bitte nehmt es zurück.« Aber wir sehen, dass nach einiger Zeit die meisten dann doch sagen: »So ist es besser.«

Der Computersicherheitsexperte Bruce Schneier geht davon aus, dass es in Zukunft spektakuläre »Datenlecks« geben wird, bei denen in großem Maße Daten verloren gehen oder entwendet werden. Diese Pannen vergleicht er in ihrer Wirkung mit den Ölkatastrophen von heute. Sind Sie in einer Risikoindustrie tätig?

Wir sind nicht im Datengeschäft, sondern betreiben einen Internetdienst. Wir fügen zu allem, was du in der Internetwelt tust, ein soziales Element hinzu. Unser Erfolg ist dadurch entstanden, dass die Leute sehen, dass durch *Facebook* Dinge wie Fotos oder Videos für sie an Wert gewinnen. Dinge, die alltäglich erscheinen, bekommen eine Bedeutung, weil Menschen sie miteinander teilen.

Dazu bauen wir mit unserem System etwas, was wir den »sozialen Graphen«[1] nennen. Das ist die Summe aller Beziehungen der Menschen, die bei *Facebook* sind. Die Verbindungen sind wichtiger als die Daten selbst. Auch wenn wir verstehen, dass Leute besorgt sind, dass es Datenhändler gibt: Wir sind nicht im Geschäft, um Daten zu sammeln und zu verkaufen.

Trotzdem entstehen ja riesige Informationsmengen. Auch der soziale Graph besteht aus Daten. Und andere Unternehmen können sie nutzen. *Facebook* stellt sie Partnerfirmen zur Verfügung, die reichen sie dann weiter. Mitunter wird dabei auch die sogenannte *User-ID* weitergegeben, eine Nummer, die für jedes *Face-*

***book*-Profil einmalig vergeben wird. Verkauft *Facebook* also die persönlichen Daten seiner Nutzerinnen und Nutzer?**

Nein. Die Weitergabe von *User-IDs* hat das *Wall Street Journal* in der Tat 2010 öffentlich gemacht. Aber dabei sind Daten in einer Art und Weise von Firmen genutzt worden, die wir nicht erlaubt haben. Unternehmen, die mit *Facebook* zusammen arbeiteten, haben hier nicht korrekt gehandelt. Wir haben daraufhin unsere Regeln überarbeitet, um zu verhindern, dass sich so etwas wiederholt. Wir versuchen, mit technischen Maßnahmen zu verhindern, dass Dritte öffentliche Daten abgreifen, und wir verklagen auch Leute, die versuchen, Daten auf unerlaubte Weise zu nutzen.

Einige Neuerungen bei *Facebook* tragen dazu bei, dass auch Menschen, die kein *Facebook*-Profil haben, in dem Netzwerk mit ihrem vollen Namen und anderen Hinweisen gespeichert werden. Wenn Bilder bei *Facebook* gespeichert werden, können Nutzende eintragen, wer dort zu sehen ist – egal ob sie oder er *Facebook*-Mitglied ist oder nicht. Sie helfen den Nutzenden sogar beim Eintragen durch eine automatische Gesichtserkennungsfunktion. Haben Leute, die nicht bei *Facebook* sind, nicht ein Recht darauf, dass sie nicht mit Namen und Bild im Netz gespeichert werden?

Sie sprechen hier eine Funktion an, die Freunden hilft, ihre Freunde zu identifizieren. Die Vorschläge, die die Software macht, funktionieren in erster Linie bei Menschen, die auch *Facebook* benutzen. Was man aber nicht tun kann, ist zu verhindern, dass *Facebook*-Nutzende auf Fotos Menschen kennzeichnen, die nicht auf dem Service sind. Dass kann man, wenn man mehrere Millionen Nutzende hat, nicht verhindern. Und man kann ebenso wenig verhindern, dass *Facebook*-Nutzende sich über Menschen äußern, die nicht bei *Facebook* sind.

Wir haben Kontrollen in den Dienst eingebaut, bei denen uns Nichtnutzende mitteilen können, dass sie zum Beispiel keine Einladungsmail bekommen möchten. Auch die Kontaktadressen auf unseren Hilfe-Seiten sind für Nichtnutzende da. Sie kann man nutzen, wenn man Inhalte gelöscht haben möchte. Das ist, was wir tun können. Es ist aber nicht realistisch zu sagen, dass man verhindern kann, dass Leute über einen reden oder Inhalte ins Netz stellen, die sich auf einen beziehen. Immerhin erscheinen diese Inhalte bei uns in einem kontrollierten Umfeld. Wenn ein Foto von Ihnen etwa in einem anonymen →Blog veröffentlicht wird, haben Sie sehr viel weniger Möglichkeiten, dagegen Einspruch zu erheben.

Anmerkung

1 Anm. d. Red.: Mark Zuckerberg und seine Firma beziehen sich seit 2007 auf den Begriff des sozialen Graphen, um den Mehrwert ihres Netzwerkes zu charakterisieren. Der soziale Graph ist ein Begriff aus der Soziometrie, die Beziehungen zwischen Menschen mithilfe mathematischer Modelle (hier der Graphentheorie) beschreiben will. Die Graphentheorie dient zur analytischen Beschreibung komplexer Mengen (die aus vielen Elementen bestehen); sie eignet sich besonders zur Behandlung algorithmischer Probleme und der Beschreibung von Netzwerken. In *Facebook* steht der soziale Graph für alle Arten von Verbindungen und Gemeinsamkeiten, die zwischen den Nutzerinnen und Nutzern feststellbar sind, zum Beispiel »Freundschaften«, Nachrichtenabonnements, gegenseitige Kommentierungen, gemeinsame Gruppenmitgliedschaften, geteilte Fotos etc. Weiterführende Informationen siehe: Alex Iskold, Social Graph: Concepts and Issues, ReadWriteWeb vom 11.9.2007, im Internet unter http://www.readwriteweb.com/archives/social_graph_concepts_and_issues.php.

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.

Dirk Heckmann

Grundprinzipien des Datenschutzrechts

Datenschutzrechtliche Fragestellungen haben heute – fast 30 Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts – an Aktualität und Bedeutung gewonnen (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.). Die Gründe dafür sind vielfältig: der ausufernde, auf prekäre Gefährdungslagen durch Terrorismus, Extremismus und organisierte Kriminalität reagierende staatliche Kontrollanspruch, aber auch private Datenverarbeitung zu Lasten Dritter im →Web 2.0 sowie die von ungeahnten Vernetzungsmöglichkeiten begleitete globale IT-Entwicklung hin zu einem →*Ubiquitous Computing*. In einem *Smart Life* werden die informationelle Selbstbestimmung und der Persönlichkeitsschutz scheinbar zu einem Rudiment aus vergangener Zeit.

Angesichts eines aus Sicht der Nutzenden eher sorglosen, aus Sicht mancher Anbieter durchaus gewinnorientierten Umgangs mit persönlichen Daten im Internet steht der Ordnungsanspruch des Staates vor Herausforderungen, denen nicht alleine mit der Schaffung oder Änderung von Gesetzen begegnet werden kann. Oft kann eine »datenschutzfreundliche Modellierung« entsprechender Software mehr leisten als Gesetze und damit verbundene Rechtsdurchsetzungsverfahren (siehe auch den Beitrag von Schaar in diesem Band, S. 363 ff.). Dies setzt voraus, dass sich die Gestaltung der Software an den wesentlichen Grundsätzen des Datenschutzrechts orientiert.

Allein das genügt aber auch nicht. Neben die rechtliche und technische Steuerung tritt die Eigenverantwortung der Einzelnen und somit auch ein Mindestmaß an Selbstschutz. Dazu müssen die Nutzerinnen und Nutzer jedoch befähigt werden, verantwortungsbewusst mit den Chancen und Risiken informationellen Handelns umzugehen. Dies umfasst insbesondere die verantwortungsbewusste Nutzung elektronischer Medien. Datenschutzpolitik erfordert deshalb auch einen Paradigmenwechsel in der Bildungspolitik, die sich stärker als bisher der sozialen Realität extensiver Mediennutzung stellen sollte (siehe auch den Beitrag von Wagner in diesem Band, S. 88 ff.).

1 Rechtsquellen und Zielsetzung des Datenschutzrechts

Die Datenschutzbestimmungen sollen den Einzelnen davor schützen, dass er – wie es das Bundesdatenschutzgesetz (BDSG) zum Ausdruck bringt – durch den Umgang mit seinen personenbezogenen Daten in seinem allgemeinen Persönlichkeitsrecht beeinträchtigt wird.[1] Zu diesem Zweck hat der Gesetzgeber einen Rechtsrahmen geschaffen, der sowohl im öffentlichen als auch im nicht-öffentlichen Bereich die den natürlichen Personen zurechenbaren Informationen unter Schutz stellt. Keine Anwendung findet das Datenschutzrecht hingegen, wenn auf sachbezogene Daten oder auf Daten juristischer Personen (beispielsweise Unternehmen, Vereine, Gemeinden, Landkreise) zugegriffen werden soll.

Es ist nicht einfach, den Überblick über die Vielzahl an datenschutzrechtlichen Regelungen zu behalten, da diese in den unterschiedlichsten Regelwerken verortet werden können. Insoweit gilt der Grundsatz, dass spezielle Rechtsvorschriften, die einen konkreten Sachverhalt betreffen, den allgemeinen Regelungen des BDSG vorgehen.

Anwendungsbereich der jeweiligen Datenschutzvorschriften

Das BDSG findet zunächst Anwendung auf die Verarbeitung personenbezogener Daten durch öffentliche Einrichtungen des Bundes[2] (zum Beispiel den Bundesrechnungshof oder die Bundesministerien). Darüber hinaus gilt es für die Datenverarbeitung durch private oder – mit den Worten des BDSG – nicht-öffentliche Stellen (beispielsweise Unternehmen oder Vereine).[3] Praktisch betrachtet greift das BDSG somit wohl hauptsächlich in Fällen, in denen nicht-öffentliche Stellen Daten erheben oder nutzen, denn dort werden wohl insgesamt mehr Daten verarbeitet als bei den Einrichtungen des Bundes.

Neben dem BDSG muss auch die Einhaltung des bereichsspezifischen Datenschutzes gemäß dem Telekommunikationsgesetz (TKG) und dem Telemediengesetz (TMG) gewährleistet werden. Das TKG regelt vor allem die rechtlichen Rahmenbedingungen der Telekommunikation, während das TMG den Bereich der Telemedien, das heißt die elektronischen Informations- und Kommunikationsdienste (darunter fallen regelmäßig Angebote im Internet wie zum Beispiel →soziale Netzwerke), abdeckt.

Um eine rechtskonforme Datenverarbeitung im gesamten öffentlichen Bereich zu gewährleisten, bedarf es neben dem BDSG der Beachtung des jeweils einschlägigen Landesdatenschutzgesetzes. Diese Regelungen auf Landesebene gelten für die Verarbeitung personenbezogener Daten durch

öffentliche Einrichtungen der einzelnen Bundesländer (beispielsweise Landesministerien oder Landesbanken). Darüber hinaus gelten sogenannte bereichsspezifische Regelungen im öffentlichen Bereich. Diese sind unter anderem in den folgenden Gesetzen zu finden:

- Polizeigesetze (siehe auch den Beitrag von Petri in diesem Band, S. 115 ff.)
- Strafprozessordnung (siehe ebenda)
- Melde- und Steuergesetze (siehe auch den Beitrag von Polenz in diesem Band, S. 145 ff.).

2 Maßstäbe für die Rechtmäßigkeit der Datenverarbeitung

Die Regelungen des Datenschutzrechts werden in Umsetzung der ständigen Rechtsprechung des Bundesverfassungsgerichts durch einige Grundprinzipien geprägt, die zu unabdingbaren Voraussetzungen einer rechtskonformen Datenverarbeitung geworden sind. Maßgeblich war insoweit vor allem das Volkszählungsurteil vom 15. Dezember 1983, in dem der Datenschutz als »Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen«, definiert wurde (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.). Die Gewährleistung der verfassungsrechtlich verankerten individuellen »informationellen Selbstbestimmung« setzt gerade unter den Bedingungen moderner Informationsverarbeitungstechnologien voraus, dass dem Einzelnen hinreichend bekannt ist, wer über ihn betreffende Informationen verfügt. Nur wer sich des in seinem sozialen Umfeld vorherrschenden Informationsstands bewusst ist und somit die Reaktion seiner Kommunikationspartner in ihren Grundzügen vorhersehen kann, ist zu selbstbestimmtem Planen und Handeln fähig. Die Frage der Rechtmäßigkeit der meisten datenschutzrechtlich relevanten Vorgänge lässt sich in Anwendung der nachfolgend näher erläuterten Grundprinzipien bereits überschlägig beurteilen.

Verboten ist, was nicht ausdrücklich erlaubt ist

Maßgeblich für das Datenschutzrecht ist zunächst das in § 4 Absatz 1 BDSG verankerte Verbot mit Erlaubnisvorbehalt. Es lässt eine Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur dann zu, wenn eine Rechtsvorschrift dies gestattet oder der Betroffene eingewilligt hat. Der Umgang mit personenbezogenen Daten ist demnach nicht grundsätzlich erlaubt, sondern bedarf einer ausdrücklichen Ermächtigung (siehe dazu auch den Beitrag von Hartge in diesem Band, S. 280 ff.). Die Erlaub-

nis zu Erhebung, Verarbeitung oder Nutzung personenbezogener Daten kann sowohl mittels des BDSG, landesrechtlicher Datenschutzvorschriften als auch über bereichsspezifische Datenschutzvorschriften erteilt werden. Dabei ist zu beachten, dass jede datenschutzrechtlich relevante Handlung eigenständige Grundrechtsrelevanz aufweist. Das heißt, jede einzelne Phase einer angestrebten Datenerhebung, -verarbeitung und -nutzung stellt eine Beeinträchtigung des Rechts auf informationelle Selbstbestimmung dar und muss auf ihre datenschutzrechtliche Zulässigkeit hin überprüft werden.

Datenverarbeitung aufgrund einer informierten Einwilligung

Besteht keine gesetzliche Erlaubnis, kommt eine Verarbeitung oder Nutzung personenbezogener Daten erst dann in Betracht, wenn die/der Betroffene eingewilligt hat (vgl. zur Erlaubnis durch Einwilligung auch den Beitrag von Hartge in diesem Band, S. 281 f.). Eine solche Einwilligung ist wiederum nur wirksam, wenn sie auf einer freien Entscheidung der Betroffenen beruht. Dies setzt voraus, dass der Einzelne ausreichende Kenntnis über die Umstände der Datenverarbeitung hat (Grundsatz der informierten Einwilligung). Die datenverarbeitende Stelle muss den Betroffenen in transparenter Weise darlegen, welche Daten zu welchem Zweck von wem verarbeitet werden. Fehlen entsprechende Angaben, erfolgt die Einwilligung »ins Blaue hinein« und ist im Regelfall unwirksam.

Gerade im Internet besteht insoweit ein Dilemma: Viele Einwilligungserklärungen und diesbezügliche Informationen der Diensteanbieter sind »formaljuristisch korrekt«, für die Nutzenden als juristische Laien unterdessen kaum verständlich. So mag dem Datenschutzrecht auf den ersten Blick Rechnung getragen sein; das eigentliche Ziel, eine selbstbewusste und selbstbestimmte Entscheidung über die Datenverarbeitung zu treffen, wird jedoch verfehlt. Einwilligungsmodi in Internetdiensten sollten deshalb (zum Beispiel mit mediendidaktischen Mitteln) für eine bessere Verständlichkeit sorgen, damit die Nutzerinnen und Nutzer tatsächlich erkennen können, was mit ihren Daten geschieht.

Personenbezogene Daten müssen grundsätzlich bei den Betroffenen erhoben werden

Der sogenannte Grundsatz der Direkterhebung der Daten ist im § 4 Absatz 2 BDSG geregelt. Die Vorschrift besagt, dass personenbezogene Daten bei den Betroffenen selbst zu erheben sind. Dieses Gebot gewähr-

leistet vor allen Dingen die informationelle Selbstbestimmung. Eine Person soll gegen die unbegrenzte Erhebung, Verarbeitung, Nutzung und Weitergabe ihrer persönlichen Daten, die durch die modernen Technologien immer leichter werden, geschützt werden. Eine Erhebung von Daten ist grundsätzlich dann gegeben, wenn Daten über eine bestimmte Person beschafft werden. Werden diese Daten geändert, gespeichert, an Dritte übermittelt, gesperrt oder gelöscht oder in einer sonstigen Form verwendet, spricht man von der Nutzung beziehungsweise von der Verarbeitung von Daten.

Möchte eine Stelle Daten erheben, hat sie also zuerst bei der betroffenen Person nachzufragen, ob sie ihre Daten erheben darf und mitzuteilen, wieso sie diese Daten benötigt. Die betroffene Person kann dann, wenn sie mit der Erhebung ihrer Daten einverstanden ist, einwilligen. Eine Erhebung von personenbezogenen Daten hinter dem Rücken der Betroffenen ist grundsätzlich unzulässig. Ausnahmen, in denen eine Datenerhebung auch ohne Mitwirkung der Betroffenen erfolgen kann, bedürfen einer gesetzlichen Regelung. Das Bundesverfassungsgericht fordert erhebliche Verfahrensvorkehrungen (etwa einen Richtervorbehalt[4], Informationspflichten und hohe Eingriffsschwellen[5]) für eine heimliche Datenerhebung wie etwa bei der *Online*-Durchsuchung (siehe auch den Beitrag von Petri in diesem Band, S. 115 ff.).

Unter Verstoß gegen den Grundsatz der Direkterhebung gewonnene Daten dürfen regelmäßig nicht verwendet werden und sind auf Verlangen der Betroffenen zu löschen.

Personenbezogene Daten dürfen nur zweckgebunden verarbeitet werden

Die Zulässigkeit einer Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist zudem grundsätzlich an einem bestimmten Zweck ausgerichtet. Nur zu dessen Erfüllung darf die auf gesetzlicher Grundlage oder mittels Einwilligung gestattete datenschutzrechtlich relevante Handlung erfolgen. Jede Zweckänderung bedarf als eigenständiger Eingriff in die informationelle Selbstbestimmung einer eigenen Ermächtigungsgrundlage (Gesetz oder Einwilligung). Der Grundsatz der Zweckbindung untersagt es, die bei verschiedenen Stellen vorhandenen Daten zusammenzuführen. Er wirkt somit der Erstellung von Persönlichkeitsprofilen (Gesamtbild der in den Daten verkörperten sozialen Beziehungen) entgegen. Die Zweckbindung ist besonders bei der Weitergabe personenbezogener Daten zu Werbezwecken zu beachten.

Hierzu ein Beispiel: Persönliche Daten, die Firmen von ihren Kunden zur Abwicklung eines Vertrages erhalten, dürfen von den Firmen nach dem Zweckbindungsgrundsatz nicht genutzt werden, um die Kunden später zu Werbezwecken zu kontaktieren.

Eine Ausnahme von diesem Grundsatz enthält das sogenannte →Listenprivileg, wonach bestimmte personenbezogene Daten, wenn sie listenmäßig oder sonst zusammengefasst sind, für Zwecke der Werbung oder der Markt- bzw. Meinungsforschung genutzt werden dürfen.[6] In dieser Liste können Informationen über folgende Merkmale enthalten sein:

- Zugehörigkeit des Betroffenen zu einer bestimmten Personengruppe (sogenanntes freies Merkmal),
- Berufs-, Branchen- oder Geschäftsbezeichnungen,
- Namen,
- Titel,
- akademische Grade,
- Anschrift,
- Geburtsjahr.

Diese Ausnahme gilt aber nur, wenn der Nutzung der Daten die schutzwürdigen Interessen der Verbraucher und Verbraucherinnen nicht entgegenstehen. Firmen müssen also abwägen, ob sie das Listenprivileg überhaupt nutzen dürfen.

Datenvermeidung und Datensparsamkeit

Das Prinzip der Datenvermeidung und Datensparsamkeit[7] ist ein weiterer Bestandteil des datenschutzrechtlichen Grundkonzeptes. Es besagt, dass nur diejenigen Daten gesammelt und verwendet werden dürfen, die zur Erfüllung des jeweils angestrebten Zwecks unbedingt benötigt werden. Die Notwendigkeit einer Datenerhebung oder -verarbeitung kann sich im nicht-öffentlichen Bereich etwa aus der Natur einer Dienstleistung ergeben. So sind beispielsweise für die Einrichtung eines Kontos bei einem *Online*-Buchhändler mehr Daten erforderlich als für das Betrachten von Nachrichten-Webseiten. Mit anderen Worten dürfen also so viele Daten wie nötig, aber gleichzeitig so wenig wie möglich gesammelt und verwendet werden.

Datensparsamkeit sollte mehr als eine Zielvorgabe sein

Das Prinzip von Datenvermeidung und Datensparsamkeit ist als Zielvorgabe ausgestaltet. Mit anderen Worten: das BDSG gibt lediglich das Ziel

vor, möglichst wenige Daten zu sammeln. Die technische Ausgestaltung der Datenverarbeitungsanlagen bleibt den verantwortlichen Stellen überlassen, ist aber an diesem Grundsatz auszurichten. Zudem versteht sich das Prinzip der Datenvermeidung und Datensparsamkeit als Mahnung an die Bürgerinnen und Bürger, keine Daten preiszugeben, soweit dies nicht unbedingt erforderlich ist. Der Selbstdatenschutz gewinnt zunehmend an Bedeutung. So ist beispielsweise die Angabe der Telefonnummer nicht erforderlich, wenn man sich bei einem sozialen Netzwerk registriert. Die Nutzenden sollen durch diese Vorschrift gemahnt werden, sorgsam auf die Preisgabe von Daten zu achten, vor allem sie nicht bedenkenlos jedweder Stelle mitzuteilen.

Da Verstöße gegen die Zielvorgabe der Datenvermeidung und Datensparsamkeit nicht geahndet werden können, halten sich viele Unternehmen nicht an diesen Grundsatz. Oftmals werden mehr Daten erhoben, als im Einzelfall erforderlich sind. Es wurde daher wiederholt gefordert, den Grundsatz der Datenvermeidung und Datensparsamkeit in einer verbindlichen Norm umzusetzen.[8]

Ein Personenbezug der Daten soll grundsätzlich vermieden werden

Konkretisiert wird der Grundsatz der Datenvermeidung und Datensparsamkeit durch das in § 3a Satz 2 BDSG niedergelegte Gebot, Daten des Betroffen grundsätzlich in →anonymisierter oder →pseudonymisierter Form zu erheben oder zu verarbeiten. Die Gewährleistung von →Anonymität oder zumindest →Pseudonymität leistet insbesondere im Internet angesichts der dort vorherrschenden Kombinations- und Verknüpfungsmöglichkeiten einen effektiven Beitrag zum präventiven Schutz der informationellen Selbstbestimmung.

Recht auf Anonymität

Ein vom Gebrauch neuer Medien unabhängiges »Recht auf Anonymität« soll sicherstellen, dass niemand gegen seinen Willen ins Rampenlicht gezogen wird. Die Gewährleistung eines anonymen oder pseudonymen Umgangs mit personenbezogenen Daten findet dort ihre Grenzen, wo sie dem Verwendungszweck widerspricht oder im Verhältnis zu dem angestrebten Schutzzweck einen unverhältnismäßigen Aufwand erfordern würde. Die Betroffenen können also nicht eine Pseudonymisierung oder Anonymisierung verlangen, wenn dies eine zweckgerechte Verwendung der Daten verhindern oder erhebliche wirtschaftliche Interessen der verantwortlichen Stelle unangemessen beeinträchtigen würde.

»Digitales Vermummungsverbot«

Ein allgemeines »digitales Vermummungsverbot«, wie gelegentlich von politischer Seite gefordert, wäre allerdings schon mit den Grundsätzen der Anonymisierung unvereinbar, überdies schlicht unverhältnismäßig und praktisch nicht umsetzbar. Umgekehrt widerspräche ein unbegrenztes Recht auf Anonymität dem Menschenbild des Grundgesetzes, das vom Prinzip des gemeinschaftsgebundenen Individuums ausgeht. Eine Rechtsordnung kann und muss deshalb vorsehen, dass eine Zurechnung von (Fehl-)Verhalten unter bestimmten, eng umgrenzten Voraussetzungen herstellbar ist. Dies kann im Internet etwa über die → IP-Adresse erfolgen. Der Streit um die → Vorratsdatenspeicherung zeigt die Schwierigkeit einer ausgewogenen Abgrenzung zwischen anonymer und zurechenbarer Nutzung des Internets (siehe auch die Beiträge von Sokol, S. 137 ff. und Ziercke, S. 129 ff. in diesem Band).

Verbot automatisierter Entscheidungen

Das Verbot automatisierter Entscheidungen ist in § 6a BDSG geregelt. Diese Vorschrift soll verhindern, dass Menschen komplizierten automatisierten Entscheidungen unterworfen werden, die für sie große Nachteile bringen könnten, ohne dass ein Mensch die unmittelbare Verantwortung für diese Nachteile übernehmen würde. Hier ist etwa an das sogenannte → *Scoring*-Verfahren zu denken (siehe auch die Beiträge von Lüke, S. 154 ff. und Hartge, S. 280 ff. in diesem Band).

Problematisch ist, dass Verstöße gegen das Verbot der automatisierten Einzelfallentscheidung häufig ohne Kenntnis der Betroffenen erfolgen. Diese können allenfalls von ihrem Auskunftsrecht Gebrauch machen, um sich hinsichtlich der über sie gespeicherten Daten und die sie betreffenden Entscheidungsprozesse informieren zu lassen. Zudem besteht die Möglichkeit, eine Gegendarstellung zu fordern, wenn die gespeicherten Daten falsch sind. Die Betroffenen haben schließlich das Recht, unzutreffende Daten korrigieren und gegebenenfalls die automatisiert gefällte Entscheidung rückgängig machen zu lassen.

Datenschutzrechtlicher Transparenzgrundsatz

Geprägt wird das Datenschutzrecht zudem vom Grundsatz der Transparenz.[9] Transparenz im datenschutzrechtlichen Kontext bedeutet: Betroffene sollen nachvollziehen können, was mit ihren Daten geschieht. Erst das Verständnis um die datenschutzrechtlich relevanten Vorgänge ermög-

licht eine effektive Ausübung des Rechts auf informationelle Selbstbestimmung. Zu diesem Zweck hat der Gesetzgeber zahlreiche Aufklärungs- und Hinweispflichten in das BDSG, das TMG und das TKG aufgenommen.

Hinweispflichten und Auskunftspflichten

Die Hinweispflicht in § 4 Absatz 3 Satz 1 BDSG, wonach Betroffene im Falle der Direkterhebung von personenbezogenen Daten über die Identität der verantwortlichen Stelle, die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und in dem gesetzlich geregelten Fall der Weitergabe auch über die Kategorien von Empfängern unterrichtet werden müssen, greift bereits vor der Datenerhebung. Hierdurch soll es den Betroffenen ermöglicht werden, die Risiken und Gefahren der Datenerhebung abzuschätzen, sich gegebenenfalls gegen die Datenerhebung zu wenden und aktiv von ihrem informationellen Selbstbestimmungsrecht Gebrauch zu machen.

Sofern personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben werden, die zur Auskunft verpflichtet, oder wenn die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen ist, ist die verantwortliche Stellen nach § 4 Absatz 3 Satz 2 BDSG zum Hinweis darauf verpflichtet. Existiert eine solche Rechtsvorschrift nicht, ist die betroffene Person auf die Freiwilligkeit ihrer Angaben hinzuweisen. Die Vorschrift richtet sich in erster Linie an öffentliche Stellen. Im privatwirtschaftlichen Bereich bedarf es jedoch regelmäßig keines Hinweises auf die Freiwilligkeit der Angaben, da sie hier selbstverständlich ist.

Schließlich sieht § 4 Absatz 3 Satz 3 BDSG eine Aufklärung über die Rechtsvorschrift und die Folgen der Verweigerung von Angaben vor, soweit dies nach den Umständen des Einzelfalles erforderlich ist oder die Betroffenen hierum gebeten haben. Auch diese Verpflichtung dient der effektiven Wahrnehmung von Rechten und soll den Betroffenen eine Meinungsbildung bezüglich der Datenfreigabe ermöglichen.

Anzumerken ist in diesem Zusammenhang, dass die Verpflichtung zur Transparenz gerade im Telemedienbereich oft nicht effizient umgesetzt wird. Neue undurchsichtige Geschäftsmodelle der sozialen Netzwerke oder Suchmaschinen vertragen sich grundsätzlich nicht mit Einzelinteressen. Die Nutzenden sind auf diesem Gebiet über das übliche Maß hinaus von den ihnen seitens der Betreiber zur Verfügung gestellten Informationen abhängig und zudem regelmäßig nicht in der Lage,

sich die komplexen Geschäftsmodelle in der für eine konsequente Rechtewahrnehmung erforderlichen Weise zu erschließen.

3 Datenschutz als unternehmerischer Selbstschutz

Datenschutz wurde in Unternehmen lange Zeit als Hemmnis und unsinnige Beschränkung der unternehmerischen Entfaltungsfreiheit verstanden. Die Datenschutzskandale der vergangenen Jahre haben eine Empörung bei Medien, Politik und Gesellschaft ausgelöst und zu einer Wahrnehmungsänderung geführt. Datenschutz bedeutet auch für Unternehmen Selbstschutz vor finanziellen Einbußen und Rufschädigungen. Zunehmend setzt sich ein Verständnis durch, wonach die Beachtung datenschutzrechtlicher Bestimmungen nicht nur lästig ist, sondern vielmehr auch einen Wettbewerbsvorteil bedeuten kann. Dies erweist sich ebenso für die Verbraucherseite als vorteilhaft.

Umstritten ist hingegen, ob die Regelungen des BDSG eine wettbewerbs- und verbraucherschützende Funktion im Sinne des § 1 Gesetz gegen den unlauteren Wettbewerb[10] aufweisen. Während das Datenschutzrecht in erster Linie dem Schutz der informationellen Selbstbestimmung dient, soll das Wettbewerbsrecht den lauteren und unverfälschten Wettbewerb gewährleisten. Die Beachtung datenschutzrechtlicher Bestimmungen ist demnach nur unter wettbewerbsrechtlichen Gesichtspunkten zu beurteilen, wenn diese einen hinreichenden Marktbezug aufweisen. Dies zu beurteilen bedarf regelmäßig einer Bewertung der jeweiligen datenschutzrechtlichen Bestimmungen hinsichtlich ihrer möglichen Beeinflussung des Marktverhaltens. Verstöße gegen das Wettbewerbsrecht können von den Verbraucherschutzverbänden sowie der am Markt agierenden Konkurrenz geahndet werden.

4 Datenschutz und Medienprivileg

Datenschutz wird nicht grenzenlos gewährleistet. Vielmehr weist das Datenschutzrecht dann Besonderheiten auf, wenn der Datenschutz in Konflikt mit anderen gleichbedeutenden Rechtspositionen gerät. Dies ist immer dann der Fall, wenn Daten erhoben oder verarbeitet werden sollen und hierdurch neben der informationellen Selbstbestimmung weitere grundrechtlich geschützte Rechtspositionen berührt werden. Die betroffenen Rechtsgüter sind dann in einen angemessenen Ausgleich zu bringen.

Ein praktischer Anwendungsfall ist die aus Artikel 5 Absatz 1 Satz 2 Grundgesetz folgende Pressefreiheit, die journalistische Unabhängigkeit und den für eine effektive Pressearbeit unerlässlichen Quellenschutz garantiert. Dieser Quellenschutz kann in Konflikt mit der informationellen Selbstbestimmung der in der Presseberichterstattung erwähnten Personen geraten. Die Pressevertreter sind im Interesse der öffentlichen Meinungsbildung tätig. Im Konfliktfall muss deshalb sorgsam abgewogen werden, welcher Rechtsposition aufgrund verfassungsrechtlicher Wertungen ein Vorrang eingeräumt werden soll. Gerade im Pressebereich kann demnach auch die Nutzung sensitiver Daten zulässig sein.

Dem Interessenausgleich zwischen informationeller Selbstbestimmung und Pressefreiheit dient zudem das in § 41 BDSG niedergelegte Medienprivileg. Die Regelung nimmt die Medien aus dem Anwendungsbereich des BDSG heraus, soweit Daten »ausschließlich« zu publizistischen Zwecken verarbeitet werden, und verpflichtet die Länder, für einen angemessenen Mindeststandard auf dem Gebiet des medienbezogenen Datenschutzes zu sorgen.

5 Grundprinzipien des Datenschutzes im Internetzeitalter

→ *Smartphones*, → *Smart Metering*, → *Smart Home Networks* – unsere Welt wird immer *smarter* (cleverer). So lässt sich mit Hilfe des *Smart Meterings* etwa der Stromverbrauch im Haus durch intelligente Systeme von außen messen und regulieren. *Smart Home Networks* gehen noch einen Schritt weiter und ermöglichen zum Beispiel die automatisierte Regulierung der Klimaanlage oder der Beleuchtung. Neue Medien und innovative Technologien erleichtern den Alltag, sind im beruflichen und gesellschaftlichen Leben nützlich und werden dankbar angenommen. Die damit verbundene Erosion der Privatsphäre wird allerdings nur teilweise erkannt und oftmals verdrängt.

Moderner Datenschutz setzt die Erkenntnis voraus, dass die Digitalisierung des Alltags mehr ist als die einfache Summe mehrfachen Einsatzes von Informations- und Kommunikationstechnologien. Es geht nicht nur darum, dass technische Geräte genutzt, einzelne Arbeitsschritte durch Softwarelösungen automatisiert oder notwendige Daten für nützliche Anwendungen erhoben und gespeichert werden. Die rapide Fortentwicklung der Informationstechnologien hin zu einem *Smart Life* ist über die technologische, ökonomische und gesellschaftliche Dimension hinausgehend eine Herausforderung in rechtlicher Hinsicht, weil eine tendenziell unbegrenzte Anzahl von Daten in unüberschaubaren Kontexten mit einer bislang nicht erfahrenen Nachhaltigkeit erhoben, gespeichert und genutzt werden.

Der Gesetzgeber darf sich angesichts der zunehmenden Gefahren für die informationelle Selbstbestimmung nicht damit abfinden, den rechtlichen Entwicklungen hinterherzuhinken. Vielmehr muss der Anlauf für eine grundlegende Überarbeitung und gegebenenfalls Neukonstruktion des Datenschutzrechts gewagt werden. Den Weg in diese Richtung weist das am 18. März 2010 seitens der Datenschutzbeauftragten des Bundes und der Länder vorgelegte Eckpunktepapier »Ein modernes Datenschutzrecht für das 21. Jahrhundert«[11], wonach unter anderem ausgehend von den Schutzzielen sanktionsbewährte Grundsatznormen geschaffen, die Eigenkontrolle der verantwortlichen Stellen befördert und der Datenschutz durch technische und organisatorische Vorkehrungen gestärkt werden soll.

Diese Gedanken werden aufgegriffen und weiterentwickelt in dem Konzept eines *Smart Privacy Management*, das die Arbeitsgruppe 5 des Nationalen IT-Gipfels der Bundesregierung am 7. Dezember 2010 in Dresden vorgelegt hat.[12] Es fordert mehr Transparenz und Vertrauensbildung in Datenverarbeitungsprozessen sowie die Möglichkeit, dass die Nutzenden über das Maß der Datenverarbeitung in smarten Technologien mitbestimmen können.

Anmerkungen

1 § 1 Abs. 1 BDSG.
2 § 1 Abs. 2 Nr. 1 BDSG.
3 § 1 Abs. 2 Nr. 3 BDSG.
4 Bei einem sogenannten Richtervorbehalt muss vor der Datenerhebung die Erlaubnis eines Gerichts eingeholt werden.
5 Als Eingriffsschwellen bezeichnet man die tatbestandlichen Voraussetzungen, die erfüllt sein müssen, damit eine Datenerhebung oder ein anderer Grundrechtseingriff rechtmäßig erfolgen kann.
6 § 28 Abs. 3 Nr. 3 BDSG.
7 § 3a S. 1 BDSG.
8 Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Ein modernes Datenschutzrecht für das 21. Jahrhundert (Eckpunktepapier), im Internet unter: http://www.bfdi.bund.de/cln_136/sid_315BB789466108187F7149CA215FD321/SharedDocs/Publikationen/Allgemein/79DSKEckpunktepapierBroschuere.html?nn=408908.
9 Siehe zum Grundsatz der Transparenz als Recht auf Zugang zu öffentlichen Dokumenten den Beitrag von Hustinx in diesem Band, S. 322 ff.

10 § 1 UWG besagt: »Dieses Gesetz dient dem Schutz der Mitbewerber, der Verbraucherinnen und Verbraucher sowie der sonstigen Marktteilnehmer vor unlauteren geschäftlichen Handlungen. Es schützt zugleich das Interesse der Allgemeinheit an einem unverfälschten Wettbewerb.«

11 Siehe Anm. 8.

12 Die Ergebnisse der Unterarbeitsgruppen sind im Internet abrufbar unter http://www.bmj.de/SharedDocs/Downloads/DE/pdfs/5_Nationaler_IT_Gipfel_Ergebnisband.pdf?__blob=publicationFile.

Dagmar Hartge

Erlaubnisse und Verbote im Datenschutzrecht

Alle Datenschutzgesetze gehen von dem Grundsatz aus, dass jede Verarbeitung personenbezogener Daten zunächst einmal verboten ist, es sei denn, das jeweilige Datenschutzgesetz oder eine andere spezialgesetzliche Regelung erlaubt die Verarbeitung bzw. die/der Betroffene hat in die Datenverarbeitung eingewilligt. Man spricht im Datenschutzrecht kurz von einem »Verbot mit Erlaubnisvorbehalt«.

Übersicht 1: Wichtige Erlaubnistatbestände im Bundesdatenschutzgesetz (Auswahl)

Die Verarbeitung personenbezogener Daten ist unter bestimmten Voraussetzungen zulässig

- bei Einwilligung des/der Betroffenen (§ 4, 4a BDSG),
- zur Durchführung eines Vertrages (§ 28 Absatz 1 Nummer 1 BDSG),
- bei berechtigten Interessen und Interessenabwägung (§ 28 Absatz 1 Nummer 2 BDSG),
- für allgemein zugängliche Daten (§ 28 Absatz 1 Satz 1 Nummer 3 BDSG),
- für Adresshandel und Werbung, insbesondere wenn es sich um listenmäßig erfasste Daten handelt (§ 28 Absatz 3 und 4 BDSG),
- für besonders sensible persönliche Daten (etwa Angaben über die ethnische Herkunft, politische Meinungen, religiöse Überzeugungen, Gesundheit oder Sexualleben) nur unter engen Voraussetzungen, beispielsweise wenn sie dem Schutz lebenswichtiger Interessen der betroffenen Person dient, zum Zweck der Gesundheitsvorsorge oder zur Abwehr von erheblichen Gefahren (§ 28 Absatz 6 bis 9 BDSG),
- für Auskunfteien, etwa für Schuldnerverzeichnisse (§ 28a BDSG),
- für → *Scoring*-Verfahren (§ 28b BDSG),
- für geschäftsmäßiges Erheben und Verarbeiten personenbezogener Daten (§ 29 BDSG),
- für die Markt- und Meinungsforschung (§§ 30, 30a BDSG),
- im Beschäftigtenverhältnis (§ 32 BDSG).

Mit dem grundsätzlichen Verbot der Verarbeitung unserer personenbezogenen Daten folgt das Datenschutzrecht dem vom Bundesverfassungsgericht im sogenannten Volkszählungsurteil herausgearbeiteten Recht auf informationelle Selbstbestimmung (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.). Bei näherer Prüfung wird allerdings schnell klar, dass dieses Selbstbestimmungsrecht über die Verarbeitung unserer Daten auch Grenzen haben muss. Unser Zusammenleben kann nicht funktionieren, wenn andere bestimmte Dinge über uns nicht wissen.

Der Gesetzgeber hat daher verschiedene *Erlaubnistatbestände* geschaffen (siehe Übersicht 1). Sie beschreiben die Umstände, wann eine Verarbeitung personenbezogener Daten zulässig ist.

In diesem Beitrag können aus Platzgründen nur die wichtigsten Erlaubnistatbestände des Bundesdatenschutzgesetzes (BDSG) und ihr Anwendungsbereich beschrieben werden.

1 Erlaubnis durch Einwilligung

Im Alltag werden ständig personenbezogene Daten verarbeitet. Ohne die Nutzung unserer personenbezogenen Daten wäre die Gestaltung eines sozialen Miteinanders nicht denkbar. Gesetzliche Regelungen können nicht alle Fälle der Datenverarbeitung abdecken. Eine andere wichtige Durchbrechung des Verbots ist die Einwilligung derjenigen, deren Daten verarbeitet werden sollen. Sie wird in § 4a BDSG geregelt, aber auch in den Datenschutzgesetzen der Länder finden sich entsprechende Vorschriften. Da die Einwilligung eine höchst persönliche Entscheidung ist, beschreiben die Datenschutzgesetze nicht nur die *Möglichkeit*, sondern auch die *Anforderungen* an eine wirksame Zustimmung der Betroffenen in die Datenverarbeitung.

Freiwilligkeit

Ein wesentliches Merkmal einer wirksamen Einwilligung ist die freie Entscheidung der Betroffenen. Eine solche setzt voraus, dass keinerlei Druck ausgeübt wird, also beispielsweise weder zeitlicher noch psychologischer Druck. Den Betroffenen dürfen auch keine Nachteile angedroht werden für den Fall, dass sie der Verarbeitung ihrer personenbezogenen Daten nicht zustimmen. Genau so wenig dürfen Vorteile verweigert werden, wenn die Einwilligung nicht erteilt wird. Freiwilligkeit setzt eine echte Wahlfreiheit voraus.

Widerruf

Die Einwilligung kann jederzeit widerrufen werden. Nach einem Widerruf ist die Verarbeitung der personenbezogenen Daten unzulässig, weil die Erlaubnis für die weitere Verarbeitung der personenbezogenen Daten entfällt. Der Widerruf bewirkt allerdings nicht, dass die bereits verarbeiteten Daten gelöscht werden müssen, er gilt vielmehr von jetzt an für die Zukunft.

Form

In der Regel bedarf die Einwilligung der Schriftform[1]. Das Schriftformerfordernis dient der Beweissicherung und hat zudem eine Warnfunktion für die Einwilligenden. Um die Bedeutung der freien Entscheidung hervorzuheben, ist die Erklärung im Text (etwa in einem Vertrag) besonders hervorzuheben, so dass sie sich von den anderen Inhalten abhebt. Dies soll verhindern, dass sie unbemerkt – also quasi nebenher – erteilt wird.

Nicht immer wird jedoch in Papierform miteinander kommuniziert. Deshalb ist es auch möglich, die Einwilligung elektronisch zu erteilen. Allerdings werden hier an die Beweisfunktion besondere Anforderungen gestellt. Eine elektronisch erteilte Zustimmung muss dem Betroffenen eindeutig zuzuordnen sein, sie muss unveränderbar sein und ist zu protokollieren. Die Erklärung muss jederzeit nachvollzogen werden können; der Betroffene muss sie jederzeit noch einmal anschauen können.

Erfolgt die Kommunikation zwischen den Parteien weder schriftlich noch elektronisch, so muss in diesen Sonderfällen die Einwilligung auch nicht in einer bestimmten Form erfolgen. Das gilt beispielsweise für telefonische Befragungen in der Markt- und Meinungsforschung. Allerdings gibt es nur wenige Umstände, bei denen eine mündliche Zustimmung erteilt werden darf. Kommt es in Fällen der alleinigen telefonischen Einigung zu Nachweisproblemen, gehen diese zu Lasten desjenigen, der die personenbezogenen Daten verarbeitet.

2 Erlaubnis zur Vertragsdurchführung

Im Alltag schließen wir ständig mündlich oder schriftlich Verträge ab (beispielsweise Mietverträge, Arbeitsverträge, Stromlieferungsverträge oder ärztliche Behandlungsverträge). Am häufigsten werden bei schriftlichen Verträgen die Adressdaten wie Name, Titel und Anschrift angegeben. Nicht selten wird auch nach einer Kontoverbindung im Vertrag gefragt.

Für diese alltäglichen Fälle ist § 28 Absatz 1 Nummer 1 BDSG die zentrale rechtliche Erlaubnisnorm für die Datenverarbeitung durch private Stellen. Diese Vorschrift erlaubt die Verarbeitung und Nutzung personenbezogener Daten als Mittel für die Erfüllung eigener Geschäftszwecke. Die Vermieterseite darf beispielsweise von Mietern und Mieterinnen nur die personenbezogenen Daten erheben, die sie für die Abwicklung des Mietverhältnisses tatsächlich benötigt. Welche Daten das sind, muss im Einzelfall geprüft werden.

Die wichtigste Frage im Hinblick auf die Verarbeitung personenbezogener Daten ist die Frage nach dem Zweck des Vertrages. Die Vielzahl möglicher Vertragsverhältnisse zeigt, dass ein Vertrag mit einem anderen Zweck ganz andere Daten beinhalten kann. Wer einen Kreditvertrag abschließt, muss beispielsweise Angaben zu seinen Einkommensverhältnissen machen; wer eine Versicherung abschließt, muss Angaben zu dem Versicherungsobjekt machen. In jedem einzelnen Fall ist also zu prüfen, welche personenbezogenen Daten jeweils verarbeitet werden dürfen.

Wichtig ist, dass keine personenbezogenen Daten erhoben werden, die über den Vertragszweck, das heißt die Vertragsabwicklung hinausgehen. Es gilt die Maßgabe: So viele personenbezogene Daten wie für den Vertrag in jedem Einzelfall erforderlich sind, und so wenig personenbezogene Daten wie möglich.

3 Erlaubnis durch Interessenabwägung

§ 28 Absatz 1 Nummer 2 BDSG beinhaltet eine weitere Durchbrechung des grundsätzlichen Verbotes der Datenerhebung. Diese Regelung soll Alltagssituationen Rechnung tragen, in denen personenbezogene Daten für eigene Geschäftszwecke benötigt werden, aber kein Vertrag als Grundlage für die Verarbeitung der Daten abgeschlossen wurde. Die Stelle, die personenbezogene Daten verarbeiten will, muss in diesen Fällen nachweisen, dass sie an den personenbezogenen Daten ein berechtigtes Interesse hat und dass dieses bei einer Abwägung gegenüber den schutzwürdigen Interessen des Betroffenen überwiegt.

Die erste Frage ist also, wann ein berechtigtes Interesse an einer Erhebung, Speicherung, Übermittlung oder Nutzung personenbezogener Daten angenommen werden kann. Voraussetzung hierfür sind zunächst eigene Belange der datenverarbeitenden Stelle und die Erforderlichkeit der personenbezogenen Daten hierfür. Diese Belange – also dieses Interesse – muss auch von der Rechtsordnung gedeckt sein, sonst handelt es sich nicht um ein berechtigtes

Interesse. Es kann sich dabei auch um ein wirtschaftliches Interesse handeln, allerdings darf das Interesse nicht gegen das »allgemeine Rechtsempfinden« verstoßen.[2] Liegt ein berechtigtes Interesse vor und sind die personenbezogenen Daten für den eigenen Geschäftszweck erforderlich, ist eine Abwägung mit den schutzwürdigen Interessen des oder der Betroffenen im jeweiligen Einzelfall vorzunehmen. Überwiegen die schutzwürdigen Interessen der Betroffenen das rechtliche Interesse, so ist die Datenverarbeitung unzulässig.

Eine entscheidende Rolle spielt die Frage, um welche personenbezogenen Daten des Betroffenen es geht. Je sensibler die personenbezogenen Daten sind, um so schwergewichtiger ist das Interesse der Betroffenen im Rahmen der Abwägung zu werten. Von besonderer Bedeutung ist das individuelle Interesse der Betroffenen, wenn es sich etwa um Gesundheitsdaten, Steuerdaten oder Daten über Straftaten handelt.

Dazu ein Beispiel: Wird etwa eine Arztpraxis veräußert, überwiegen die schutzwürdigen Interessen der Patientinnen und Patienten das Interesse des veräußernden Arztes oder der Ärztin an einer Überlassung der Patientendaten an die erwerbende Person. Etwas anderes gilt nur, wenn von Patientenseite vorher in die Übermittlung der Daten eingewilligt wurde.

Der Gesetzgeber hat keine Kriterien vorgegeben, um diese Interessenabwägung zu erleichtern. Sie ist im Hinblick auf das informationelle Selbstbestimmungsrecht der Betroffenen immer vor dem Hintergrund durchzuführen, dass für die Datenverarbeitung ein Verbot mit Erlaubnisvorbehalt gilt und damit strenge Kriterien für diese Erlaubnis gelten.

4 Erlaubnisregeln für besondere Bereiche

Allgemein zugängliche Daten

§ 28 Absatz 1 Nummer 3 BDSG erlaubt regelmäßig die Verarbeitung personenbezogener Daten, wenn sie allgemein zugänglich sind oder wenn sie veröffentlicht werden dürfen. Dies gilt nur dann nicht, wenn die schutzwürdigen Interessen des Betroffenen ganz offensichtlich das berechtigte Interesse an der Verarbeitung oder Nutzung der Daten überwiegen. Allgemein und damit für jede Person ohne Einschränkung zugänglich sind Daten in Massenmedien wie Zeitungen und Fernsehen einschließlich der *Online*-Medien, Telefon- und Adressverzeichnissen sowie Lexika. Für jeden zugänglich sind auch bestimmte öffentliche Register wie das Handels- oder das Vereinsregister, bei denen keine besonderen Zugangsvoraussetzungen geprüft werden.

Privilegierung von Adresshandel und Werbung

§ 28 Absatz 3 BDSG erlaubt die Nutzung personenbezogener Daten für den Adresshandel und Zwecke der Werbung. Voraussetzung hierfür ist grundsätzlich die Einwilligung der Betroffenen. Dieser Grundsatz wird allerdings wieder aufgeweicht durch die Privilegierung von Listen mit zusammengefassten personenbezogenen Daten für Zwecke der Werbewirtschaft. Diese Privilegierung bezeichnet man auch als → Listenprivileg (siehe dazu auch den Beitrag von Heckmann in diesem Band, S. 267 ff.). § 28 Absatz 4 BDSG regelt das Recht des Widerspruchs (siehe dazu auch die Beiträge von Dix, S. 290 ff. und Fiedler, S. 165 ff. in diesem Band).

Auskunfteien

Mit § 28a BDSG hat der Gesetzgeber erstmals einen ausdrücklichen Erlaubnistatbestand für Datenübermittlungen an → Auskunfteien geschaffen. Der Vertragspartner einer Auskunftei darf jede Forderung eintragen lassen, die von einem Schuldner trotz Fälligkeit nicht erfüllt worden ist.

§ 28a Absatz 2 BDSG regelt die Übermittlung personenbezogener Daten durch Kreditinstitute an Auskunfteien zur Durchführung eines Bankgeschäftes.

Absatz 3 des § 28a BDSG verpflichtet die übermittelnde Stelle, der Auskunftei jede nachträgliche Änderung bezüglich der von ihr übermittelten Daten nachzumelden. Damit soll sichergestellt werden, dass die Auskunftei nicht mit falschen Daten arbeitet. Ebenso wichtig ist die Pflicht, der Auskunftei auch eine Löschung der Daten mitzuteilen. Auch dies dient dem Schutz des Betroffenen vor fehlerhaften Daten.

Scoring-Verfahren

Im Jahr 2009 wurde in das Bundesdatenschutzgesetz eine gesetzliche Regelung von Anforderungen an sogenannte mathematisch-statistische Verfahren zur Berechnung der Wahrscheinlichkeit zukünftigen Verhaltens, dem sogenannten → *Scoring*, aufgenommen. Der neue § 28b BDSG regelt nun Anforderungen an die Berechnung eines *Score*-Wertes (Punktzahl) als Entscheidungshilfe über einen Vertragsabschluss, seine Durchführung oder seine Beendigung. Insgesamt sind die Regelungen des *Scoring*-Verfahrens allerdings nur punktuell. Der Gesetzgeber hat zunächst klargestellt, dass es sich bei den dabei eingesetzten Methoden um anerkannte wissenschaftliche Verfahren handeln muss. Darüber hinaus darf

keine Berechnung allein auf der Grundlage der Andressdaten einer Person erfolgen. Soweit bei der Durchführung des Verfahrens auch Anschriftendaten mit genutzt werden, ist der Betroffene hierüber zu unterrichten und ist dies zu dokumentieren. Mit der gesetzlichen Regelung der Rahmenbedingungen hat der Gesetzgeber derartige Verfahren, die durch die Verknüpfung mit einer individuellen Person neue personenbezogene Daten erschaffen, nunmehr endgültig als legitim anerkannt.

Geschäftsmäßiges Erheben und Verarbeiten personenbezogener Daten

§ 29 BDSG erlaubt das geschäftsmäßige Erheben und Verarbeiten von personenbezogenen Daten, um diese Dritten zu übermitteln, als eigenen Geschäftszweck. Diese Vorschrift stellt damit eine Rechtsgrundlage für den → Adresshandel und die → Auskunfteien dar. Für beide Bereiche sind personenbezogene Daten die Grundlage der geschäftlichen Betätigung. § 29 BDSG regelt in Absatz 1 die Voraussetzungen, unter denen die verantwortliche Stelle personenbezogene Daten erheben, speichern, verändern und nutzen darf, und in welchem Rahmen sie Daten gewinnen darf. Der Kern des Geschäftsbereichs, die Datenübermittlungen, wird in Absatz 2 geregelt.

Sowohl die Datenerhebung als auch die Übermittlung an Dritte sind nur zulässig, wenn kein Grund für die Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an einem Ausschluss hat. Dies bedeutet jedoch nicht, dass regelmäßig eine echte Abwägung der Interessen des Unternehmens und des Betroffenen stattfindet. Die verantwortliche Stelle dürfte ohne zusätzliche Informationen keine genaueren Kenntnisse besitzen, um ein schutzwürdiges Interesse des Betroffenen erkennen zu können.

Bei der Übermittlung der Daten an einen Dritten muss dieser vor der Übermittlung ein berechtigtes Interesse an ihrer Kenntnis glaubhaft machen. Da dies bei einem Massenverfahren ein besonders fehleranfälliger Punkt ist, hat der Gesetzgeber hier zumindest ein verpflichtendes Stichprobenverfahren vorgesehen, mit dem die übermittelnde Stelle überprüfen muss, ob tatsächlich ein berechtigtes Interesse des Datenempfängers vorgelegen hat. Außerdem sind die Datenübermittlungen zu protokollieren (§ 29 Absatz 2 Satz 3 und 4 BDSG). Insgesamt wird deutlich, dass der Gesetzgeber die betroffenen Wirtschaftszweige erkennbar privilegieren wollte und die Grenzen der Einzelfallprüfung in einem Massenverfahren auch in seiner gesetzlichen Regelung aufgezeigt hat.

5 Spezielle Erlaubnisse im öffentlichen Bereich

Im Verhältnis zwischen Bürgerinnen und Bürgern und dem Staat kommt speziellen gesetzlichen Erlaubnissen zur Datenverarbeitung eine entscheidende Bedeutung zu.

Polizei und Eingriffsverwaltung

Für den Bereich des staatlichen Handelns hat der Gesetzgeber deshalb insbesondere in den Bereichen der Eingriffsverwaltung (vor allem die Aufgabenbereiche Polizei und die Ordnungsämter) gesetzliche Regelungen für die Verarbeitung personenbezogener Daten verabschiedet (zur Datenverarbeitung durch die Polizei siehe auch den Beitrag von Petri in diesem Band, S. 115 ff.). Sie sollen sicherstellen, dass jeder weiß, welche Daten der Staat erheben darf. Sie stellen die Grenze für zulässiges staatliches Handeln gegenüber dem Einzelnen dar.

Wichtige spezialgesetzliche Regelungen finden sich beispielsweise in

- den Polizeigesetzen der Länder
- dem Bundespolizeigesetz
- der Strafprozessordnung (StPO)
- den Sozialgesetzbüchern.

So erlaubt etwa § 100a Absatz 1 StPO der Polizei die heimliche Überwachung der Telekommunikation einer Person, wenn aufgrund bestimmter Tatsachen der Verdacht besteht, dass sie eine schwere Straftat – etwa einen Mord – begangen hat.

Darüber hinaus gibt es im Bereich der öffentlichen Verwaltung unzählige weitere datenschutzrechtliche Erlaubnisnormen, zum Beispiel

- im Melderecht,
- im Steuerrecht,
- im Personenstandsrecht,
- in der Gesundheitsverwaltung.

So dürfen etwa die Meldeämter aufgrund der Regelungen in den Landesmeldegesetzen den Namen, die Anschrift, das Geburtsdatum und weitere Information von Personen erheben und speichern, um die Melderegister zu führen.

Voraussetzungen der Spezialgesetze

Allen speziellen Erlaubnisnormen für die Verarbeitung personenbezogener Daten ist gemeinsam, dass sie klar – das heißt inhaltlich bestimmt – regeln müssen, was erlaubt ist. Dabei dürfen sie nicht über das hinaus gehen, was an personenbezogenen Daten für die Aufgabenerfüllung im Einzelfall tatsächlich erforderlich ist. Der Zweck, zu dem die Daten verarbeitet werden, muss immer erkennbar sein. Je tiefer der Eingriff in die Rechte des Einzelnen geht, desto größer sind die Anforderungen an die Bestimmtheit und Klarheit der gesetzlichen Vorschrift.

6 Erlaubnis durch andere Rechtsvorschriften

In § 4 BDSG und in den entsprechenden landesrechtlichen Vorschriften ist die Rede von »anderen Rechtsvorschriften«, die die Erhebung und Verarbeitung personenbezogener Daten erlauben können. Unter den Begriff »andere Rechtsvorschriften« fallen nicht nur Gesetze, die Parlamente verabschiedet haben. Darunter fallen auch Rechtsverordnungen und Satzungen. Satzungen können im öffentlichen wie auch im privat-rechtlichen Bereich erlassen werden.

Satzungen

Bei Satzungen handelt es sich um Rechtsnormen, die nicht von Parlamenten erlassen werden, sondern von juristischen Personen, die eine Befugnis zur Rechtsetzung in eigenen Angelegenheiten haben. Am bekanntesten sind sicherlich die Satzungen, die von Gemeinden erlassen werden können. Wenn eine Satzung nicht nur die inneren Angelegenheiten der Gemeinde regelt, sondern auch in Rechte Dritter eingreift – das heißt in diesen Fall der Bürgerinnen und Bürger –, muss die jeweils zuständige datenschutzrechtliche Aufsichtsbehörde der Gemeinde der Satzung zustimmen. Beispiele dafür sind Satzungen zur Hundesteuer, zu Zweitwohnungen, zu Abfallgebühren oder zu Elternbeiträgen für den Besuch von Kindertageseinrichtungen.

Im nicht-öffentlichen Bereich werden ebenfalls Satzungen erlassen. Hier sind Satzungen schriftliche Grundordnungen, die sich Zusammenschlüsse von privat-rechtlichen Vereinigungen selber per Beschluss geben. Das bekannteste Beispiel sind Vereinssatzungen. Sie regeln das Miteinander der Vereinsmitglieder sowie ihre Rechte und Pflichten –

und in diesem Zusammenhang etwa auch, welche personenbezogenen Daten die Vereinsmitglieder für eine Vereinsmitgliedschaft von sich angeben müssen.

Betriebsvereinbarungen

Eine wichtige Gruppe anderer Rechtsvorschriften, die Erlaubnisnormen für die Verarbeitung personenbezogener Daten sein können, sind Betriebsvereinbarungen in Unternehmen und Betrieben.[3]

Das Bundesdatenschutzgesetz hat zunächst für den Unternehmensbereich keine konkreten Regelungen getroffen, sondern lässt mit seinen unbestimmten Rechtsbegriffen Auslegungsspielräume, die zu Streitigkeiten zwischen Arbeitgebern und Betriebsrat führen können. Hier kann die Regelung problematischer und strittiger Fragen durch eine Betriebsvereinbarung sinnvoll sein. Sie haben für die Parteien einen rechtsverbindlichen Charakter und dienen der Herstellung von Rechtssicherheit für beide Parteien (siehe zum Beschäftigtendatenschutz auch die Beiträge von Däubler, S. 188 ff., Wolf, S. 199 ff. und Perreng, S. 206 ff. in diesem Band).

Anmerkungen

1 Schriftform bedeutet gemäß § 126 des Bürgerlichen Gesetzbuchs, dass eine eigenhändige Unterschrift vorliegen muss.
2 Vgl. Peter Gola/Rudolf Schomerus, BDSG Kommentar, § 28, Rd. 24, 10. Aufl., München 2010.
3 Bettina Sokol in: Spiros Simitis, BDSG-Kommentar, § 4 Rd. 11, 7. Aufl., Baden-Baden 2011.

Alexander Dix

Betroffenenrechte im Datenschutz

Datenschutz ist Grundrechtsschutz. Es geht beim Datenschutz nicht um den Schutz von Daten um ihrer selbst willen, sondern um den Schutz der Freiheit des einzelnen Menschen. Die Autonomie des Einzelnen setzt Rechtsansprüche voraus, mit denen Bürgerinnen und Bürger – in der Sprache der Datenschutzgesetze »die (von der Datenverarbeitung) Betroffenen« – die Verarbeitung ihrer Daten kontrollieren können. Diese Kontrolle hat mehrere Aspekte: Sie soll die Datenverarbeitung transparent machen und es den Einzelnen darüber hinaus ermöglichen, die Verarbeitung ihrer Daten – in bestimmten Grenzen – zu beeinflussen und unter bestimmten Umständen zu stoppen. Allerdings drohen die Betroffenenrechte im digitalen Zeitalter zunehmend leerzulaufen. Deshalb muss die Frage gestellt werden, in welcher Weise sie den neuen technologischen Gegebenheiten anzupassen sind.

Das Bundesdatenschutzgesetz (BDSG) und im Wesentlichen auch die Datenschutzgesetze der Länder[1] sehen folgende Rechte vor:

- Transparenzrechte (auf Auskunft und Benachrichtigung),
- Steuerungsrechte (auf Berichtigung, Löschung, Sperrung, Gegendarstellung, Widerspruch),
- Sanktionsrechte (auf Schadensersatz, Anrufung der Datenschutzkontrolle, Strafanzeige).

Die Betroffenenrechte sind die entscheidenden Werkzeuge für den Selbstdatenschutz, sie sind unabdingbar. Die Betroffenen können also auch durch einen faktisch überlegenen Vertragspartner (beispielsweise gegenüber Arbeitgebern) nicht dazu gezwungen werden, auf diese Rechte zu verzichten.[2]

Die Ausübung dieser Rechte darf grundsätzlich nicht ihrerseits registriert werden. Wenn dies ausnahmsweise doch zulässig ist[3], dann dürfen Betroffene nicht wegen der Wahrnehmung ihrer Rechte gemaßregelt oder anders benachteiligt werden.[4]

Diese gesetzlichen Garantien verdeutlichen die zentrale Stellung im Kontext des Datenschutzes. Sie sind sowohl im Bereich der Verwaltung als auch in der Privatwirtschaft Teil des gesetzlichen Kontrollsystems

zur Durchsetzung des Datenschutzes, zu dem außerdem die interne und externe Kontrolle durch Datenschutzbeauftragte und Aufsichtsbehörden gehören (siehe auch den Beitrag von Kamp/Thomé in diesem Band, S. 298 ff.). Die Betroffenenrechte sind vor Gericht einklagbar. Werden sie von den verantwortlichen Stellen (Behörden, Unternehmen) missachtet, kann dies zu Beanstandungen, zur Verhängung von Bußgeldern oder zu strafrechtlichen Sanktionen führen. Die Betroffenenrechte unterliegen bestimmten Ausnahmen, deren Interpretation wesentlich über die praktische Reichweite der Ansprüche entscheidet.

1 Datenschutzrechtliches Auskunftsrecht

Das wichtigste Betroffenenrecht ist das Recht auf Auskunft, mit dem Betroffene folgende Informationen erfragen können:

- welche Daten konkret über sie zu welchem Zweck verarbeitet werden,
- woher diese Informationen stammen,
- wer sie erhalten hat.[5]

Erst durch das Auskunftsrecht erhalten Betroffene die Möglichkeit, die Rechtmäßigkeit der Verarbeitung ihrer Daten zu beurteilen und – falls nötig – weitere Rechte (beispielsweise auf Korrektur oder Löschung) geltend zu machen. Das Bundesverfassungsgericht hat bereits 1983 im Volkszählungsurteil[6] betont, dass eine Gesellschaftsordnung, in der Einzelne »nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß, mit der Verfassung unvereinbar« wäre (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.). Schon aus der Verwendung des Begriffs »Gesellschaftsordnung« ergibt sich, dass sich Auskunftsrechte nach dem Willen des Grundgesetzes nicht auf die staatliche Datenverarbeitung beschränken, sondern auch gegenüber Unternehmen gelten.

Das Recht auf Auskunft im europäischen Recht

Ein Menschenrecht auf Auskunft enthält auch die Charta der Grundrechte der Europäischen Union[7], die seit Dezember 2009 als Teil des Europäischen Unionsrechts gilt.[8] Nach der Rechtsprechung des Europäischen Gerichtshofs ist es unzulässig, das Recht der Betroffenen auf Auskunft über die Empfänger von zurückliegenden Datenübermittlungen auf einen kurzen Zeitraum zu beschränken, während die Basisdaten sehr viel länger aufbewahrt werden dürfen.[9]

Das Recht auf Auskunft kann eine Hol- oder Bringschuld darstellen

Allerdings führt das Auskunftsrecht nur dann zur erwünschten Transparenz, wenn es auch geltend gemacht wird. Daten über die Betroffenen sind insoweit als »Holschuld« zu verstehen. Mit anderen Worten: Die/der Betroffene muss sich selbst bemühen, um Informationen über die Art und den Umfang der Verarbeitung persönlicher Daten zu erhalten.

Demgegenüber und darüber hinaus sind Datenverarbeiter in bestimmten Fällen – insbesondere bei einer Datenerhebung hinter dem Rücken der Betroffenen – dazu verpflichtet, diese von sich aus davon zu benachrichtigen, welche Art von Daten über sie verarbeitet werden.[10] Informationen sind in diesen Fällen ein »Bringschuld«. Diese Pflichten zur unaufgeforderten Benachrichtigung sind umso wichtiger, da die Bürgerinnen und Bürger häufig gar nicht wissen, dass und von wem Daten über sie verarbeitet werden.

Auskunftsrechte können in bestimmten Fällen eingeschränkt werden

Die Transparenzrechte gelten nicht ausnahmslos. Wichtig ist aber, dass die datenverarbeitende Stelle im Einzelfall prüfen und darlegen muss, dass und inwieweit sie ausnahmsweise nicht benachrichtigen oder keine Auskunft erteilen muss. Das gilt auch für die Sicherheitsbehörden (Nachrichtendienste, Strafverfolgungsbehörden und Polizei), die bis 1990 selbst dann noch die Auskunft verweigern konnten, wenn kein Ausnahmetatbestand vorlag (zur Datenverarbeitung durch die Sicherheitsbehörden siehe auch den Beitrag von Petri in diesem Band, S. 115 ff.).

Keine für Datenverarbeitung verantwortliche Person, die Auskunft erteilen soll, darf dieses Recht dadurch umgehen, dass sie eventuell zu Unrecht gespeicherte Daten kurzerhand löscht, bevor die Betroffenen sie zu Gesicht bekommen. Die Liste der Ausnahmetatbestände ist zwar lang, aber abschließend, und die Ausnahmen sind eng auszulegen, damit der Zweck der gesetzlichen Transparenzgebote nicht konterkariert wird (siehe zum Verhältnis von Transparenz und Datenschutz auch den Beitrag von Hustinx in diesem Band, S. 322 ff.).

Die Auskunft darf vor allem verweigert werden, soweit Geheimhaltungsinteressen des Staates oder privater Dritter der Auskunft entgegenstehen.[11] Wenn eine öffentliche Stelle (etwa im Sicherheitsbereich) die Auskunftsverweigerung aus Gründen der Geheimhaltung nicht begründet, muss sie die Betroffenen darauf hinweisen, dass sie sich an den jeweiligen Datenschutzbeauftragten des Bundes oder des Landes wen-

den können, der die Auskunftsverweigerung auf ihre Rechtmäßigkeit hin überprüfen kann. Allerdings darf auch er den Betroffenen Auskünfte nur mit Zustimmung der verantwortlichen Stellen erteilen.[12]

Die Auskunft ist in den meisten Fällen unentgeltlich

Die Auskunftserteilung ist unentgeltlich.[13] Im Bereich der Wirtschaft kann jede Person von →Auskunfteien und anderen Unternehmen, die Daten geschäftsmäßig zum Zweck der Übermittlung verarbeiten, einmal im Jahr eine unentgeltliche Auskunft in Textform (also auch per E-Mail) verlangen. Für jede weitere Auskunftserteilung kann ein kostendeckendes Entgelt verlangt werden, wenn Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen können (beispielsweise um als Wohnungsinteressent die Zahlungsfähigkeit gegenüber dem Vermieter zu belegen).

In jedem Fall ist die Auskunft aber dann unentgeltlich, wenn entweder besondere Umstände vermuten lassen, dass Daten unrichtig oder unzulässig gespeichert werden oder wenn die Auskunft ergibt, dass die Daten unrichtig sind oder wegen unzulässiger Speicherung gelöscht werden müssen.[14] Schließlich muss den Betroffenen stets die Möglichkeit gegeben werden, unentgeltlich persönlich Einsicht in ihre Daten zu nehmen.[15]

2 Steuerungsrechte

Sobald Betroffene eine Auskunft erhalten haben, können sie weitere Rechte geltend machen. Es bieten sich folgende Möglichkeiten:

- Haben sie festgestellt, dass Daten über sie zu Unrecht gespeichert sind – sei es, dass sie nie hätten erhoben werden dürfen, sei es, dass sie nicht mehr erforderlich sind – können sie von der Behörde oder vom Unternehmen Löschung verlangen.[16]
- Sind die Daten dagegen unrichtig, hat die datenverarbeitende Stelle sie zu korrigieren.[17]
- Schließlich müssen solche Daten gesperrt werden, deren Richtigkeit die Betroffenen bestreiten, wenn sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.[18]

Bei Daten aus allgemein zugänglichen Quellen besteht nur ein Recht auf Gegendarstellung

Unternehmen, die unrichtige oder bestrittene Daten geschäftsmäßig zum Zweck der Übermittlung speichern (beispielsweise →Auskunfteien wie die →SCHUFA), müssen sie weder korrigieren noch sperren, wenn sie aus allgemein zugänglichen Quellen entnommen wurden und zu Dokumentationszwecken gespeichert sind. In diesen Fällen haben Betroffene das Recht, den Daten eine Gegendarstellung beizufügen, ohne die die Daten nicht übermittelt werden dürfen.[19] Handelt es sich allerdings um sensitive Daten (über rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten), so müssen Unternehmen, die solche Daten verarbeiten, ohne ihre Richtigkeit beweisen zu können, sie in jedem Fall löschen.[20] Für Behörden sieht das Gesetz aus nicht nachvollziehbaren Gründen keine entsprechende Pflicht vor.

Widerspruchsrecht auch bei rechtmäßiger Verarbeitung

Schließlich können Betroffene sogar einer rechtmäßigen Verarbeitung ihrer Daten widersprechen. Dieser Widerspruch führt zum Verbot der Datenverarbeitung, wenn eine Prüfung ergibt, dass das schutzwürdige Interesse der Betroffenen wegen ihrer besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Datenverarbeitung überwiegt.[21]

Ohne dies besonders begründen zu müssen, kann jede Person der Nutzung ihrer Daten für Zwecke der Werbung oder Markt- und Meinungsforschung auch nachträglich widersprechen.[22] Auf dieses Recht sind die Betroffenen rechtzeitig, das heißt bei der ersten Ansprache hinzuweisen. Eine Verletzung dieser Hinweispflicht kann zur Verhängung von Bußgeld führen.[23]

3 Sanktionsrechte bei Rechtsverstößen

Bei Verstößen gegen datenschutzrechtliche Vorschriften haben die Betroffenen folgende rechtlichen Möglichkeiten:

- sie können die Datenschutzbehörden anrufen,[24]
- sie können Schadensersatz verlangen und notfalls gerichtlich einklagen[25] oder
- sie können Strafantrag stellen, falls das Datenschutzrecht in strafbarer Weise verletzt wurde.[26]

Während die Tätigkeitsberichte der Datenschutzbehörden die ständig wachsende Zahl der Eingaben von Bürgerinnen und Bürgern belegen,[27] sind praktisch keine Fälle bekannt geworden, in denen verantwortliche Stellen durch ein Gericht zum Schadensersatz verurteilt wurden. Das ist umso erstaunlicher, als das Gesetz bei privaten Datenverarbeitern von einem vermuteten Verschulden in Bezug auf die Verletzung des Rechts auf informationelle Selbstbestimmung ausgeht[28] und bei automatisierter Verarbeitung durch Bundesbehörden sogar eine Gefährdungshaftung vorsieht,[29] das heißt die Ersatzpflicht tritt unabhängig davon ein, ob überhaupt ein Verschulden nachgewiesen ist.

4 Notwendige Erweiterung der Betroffenenrechte im Internetzeitalter

Im Zeitalter des Internets sind Betroffenenrechte besonders gefährdet. Zwar gelten sie auch gegenüber Anbietern von Webseiten, Suchmaschinen und →sozialen Netzwerken, sind aber insbesondere dann schwer durchsetzbar, wenn diese Anbieter im außereuropäischen Ausland sitzen. Das betrifft vor allem US-amerikanische Unternehmen wie *Google* und *Facebook*. Grundsätzlich haben auch solche Unternehmen die Betroffenenrechte nach deutschem Recht zu beachten, da ihre Angebote natürlich auch auf den deutschen Markt zielen.

Ein Recht auf Vergessen

Von zentraler Bedeutung im Internet ist das Recht auf Löschung. Zwar vergisst das Internet in seiner gegenwärtigen Struktur nichts, denn jeder Inhalt, der auf einer Webseite gelöscht worden ist, kann zuvor tausendfach kopiert und andernorts abgelegt worden sein. Dennoch ist das Recht jedes Einzelnen auf Vergessen gleichwohl legitim. Gegenwärtig werden verschiedene Möglichkeiten diskutiert, wie es zumindest teilweise durchgesetzt werden kann. Neben der rechtlich durchsetzbaren Löschung durch die Stelle, die die Daten erstmals im Internet angeboten hat (beispielsweise ein →soziales Netzwerk), könnte man an kryptographisch (→Kryptographie) mit dem jeweiligen Datensatz verknüpfte »Verfallsdaten« denken, bei deren Ablauf die Betroffenen gefragt werden, ob sie gegen die Löschung (beispielsweise einer Fotosammlung) Einwände haben. Schließlich wären auch eine Sperrung oder ein Verwendungsverbot für solche Daten denkbar, die nach einer partiellen Löschung noch an anderer Stelle im Netz gefunden werden.

Die Europäische Kommission hat beschlossen, im Rahmen ihres Gesamtkonzepts für den Datenschutz[30] in der Europäischen Union, ein »Recht auf Vergessen« auch für die Fälle einzuführen, in denen ein Betroffener seine Zustimmung zur Datenverarbeitung widerrufen hat. Außerdem hat die Kommission zu Recht darauf hingewiesen, dass jeder das Recht haben muss, seine Daten (beispielsweise Fotos oder Verzeichnisse von Freunden) von einem Anbieter oder einer Plattform zurückzuholen (Datenübertragbarkeit).[31] Nur so kann im Zeitalter des Internets die Autonomie der Nutzenden aufrechterhalten werden.

5 Stärkung der Betroffenenrechte durch Technikgestaltung

Gerade in der Informationsgesellschaft des 21. Jahrhunderts sind Betroffenenrechte von entscheidender Bedeutung dafür, dass Datenschutz (oder mit den Worten des Bundesverfassungsgerichts: informationelle Selbstbestimmung) gelebt und durchgesetzt werden kann. Dafür genügt es nicht, dass Gesetze auf nationaler und europäischer Ebene dieses Recht garantieren, auch die informationstechnischen Geräte (Computer, Handys etc.) und die Internet-Angebote (zum Beipiel →soziale Netzwerke) müssen die technischen Voraussetzungen für die Ausübung von Betroffenenrechten von vornherein enthalten (vgl. hierzu auch den Beitrag von Schaar in diesem Band, S. 363 ff.).

Anmerkungen

1 Im Folgenden wird nur auf Regelungen des BDSG verwiesen.
2 § 6 Abs. 1 BDSG.
3 Eine Registrierung kann beispielsweise erfolgen, wenn das Auskunftsrecht nicht persönlich, sondern durch eine vertretungsberechtigte Person ausgeübt wird.
4 § 6 Abs. 3 BDSG.
5 Vgl. § 19 BDSG für die öffentliche Verwaltung, § 34 BDSG für die Wirtschaft.
6 BVerfGE 65, 1; Az. 1 BvR 209/83 u. a.
7 Artikel 8 Abs. 2 Satz 2.
8 Ein entsprechendes »Transparenzrecht« enthält auch Artikel 12a der EG-Datenschutzrichtlinie (siehe dazu den Beitrag von Hijmans/Langfeldt in diesem Band, S. 403 ff.).
9 EuGH, Urteil vom 7.5.2009, Europäische Grundrechte-Zeitschrift 2009, S. 229 ff. (Rechtssache C-553/07).
10 § 19a BDSG für die Verwaltung, § 33 BDSG für die Wirtschaft.

11 § 19 Abs. 3 und 4; § 34 Abs. 4 in Verbindung mit § 33 Abs. 2 S. 1 Nr. 3 und 6 BDSG.
12 Vgl. § 19 Abs. 6 S. 2 BDSG.
13 Vgl. §§ 19 Abs. 7, 34 Abs. 8 S. 1 BDSG.
14 § 34 Abs. 8 S. 3 bis 5 BDSG.
15 § 34 Abs. 9 BDSG.
16 §§ 20 Abs. 2, 35 Abs. 2 Nr. 1, 3 BDSG.
17 §§ 20 Abs. 1, 35 Abs. 1 BDSG.
18 §§ 20 Abs. 4, 35 Abs. 4 BDSG.
19 § 35 Abs. 6 BDSG.
20 § 35 Abs. 2 Nr. 2 BDSG.
21 §§ 20 Abs. 5, 35 Abs. 5 BDSG.
22 § 28 Abs. 4 BDSG.
23 § 43 Abs. 1 Nr. 3 BDSG.
24 Vgl. § 21, 38 Abs. 1 Satz 8 BDSG.
25 §§ 7, 8 BDSG.
26 § 44 BDSG; einen Strafantrag können außer den Betroffenen auch die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Aufsichtsbehörde stellen.
27 Vgl. die Webseite des virtuellen Datenschutzbüros: http://www.datenschutz.de.
28 § 7 BDSG.
29 § 8 Abs. 1 BDSG.
30 Vgl. Artikel 17 des Entwurfs der EU-Kommission für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM (2012) 11 endgültig vom 25.1.2012, siehe auch Entschließung des Europäischen Parlaments vom 6.7.2011 zum Gesamtkonzept für den Datenschutz in der Europäischen Union (2011/2025(INI), im Internet unter http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2011-0323&language=DE&ring=A7-2011-0244.
31 Vgl. Artikel 18 des Entwurfs einer Datenschutz-Grundverordnung (s. Anm. 30).

Meike Kamp/Sarah Thomé

Die Kontrolle der Einhaltung der Datenschutzgesetze

Dieser Beitrag soll einen Überblick darüber bieten, wie die Kontrolle der Datenschutzgesetze organisiert ist. Zu diesem Zweck werden zunächst die wichtigsten Akteure im Bereich der Datenschutzkontrolle vorgestellt (Sarah Thomé). Anschließend wird beschrieben, welche Aufgaben diese Kontrollstellen haben und wie diese ausgeübt werden (Meike Kamp).

1 Wer kontrolliert die Einhaltung der Datenschutzgesetze?

Es gibt eine Vielzahl unterschiedlicher Kontrollstellen im Bereich des Datenschutzes, so

- den Bundesbeauftragten für den Datenschutz,
- die Landesdatenschutzbeauftragten,
- die Aufsichtsbehörden über den nicht-öffentlichen Bereich,
- betriebliche und behördliche Datenschutzbeauftragte,
- die Datenschutzbeauftragten der Kirchen,
- die Datenschutzbeauftragten der Rundfunkanstalten,
- den Europäischen Datenschutzbeauftragten.

Die Vielzahl dieser Akteure ergibt sich daraus, dass für verschiedene datenverarbeitende Bereiche jeweils eigene Kontrollstellen geschaffen wurden. Das Bundesdatenschutzgesetz (BDSG) unterscheidet hinsichtlich der jeweils zuständigen Kontrolleure zunächst zwischen Datenverarbeitung im öffentlichen Sektor (Einrichtungen des Bundes und der Länder, wenn sie öffentliche Aufgaben wahrnehmen) und Datenverarbeitung im nicht-öffentlichen Sektor (beispielsweise natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, vgl. zu dieser Unterscheidung auch § 2 BDSG).

Während die Datenschutzbeauftragten des Bundes und der Länder die Kontrolle über den öffentlichen Bereich ausüben, sollen die sogenannten Aufsichtsbehörden den nicht-öffentlichen Bereich überwachen. Die Datenschutzbeauftragten und die Aufsichtsbehörden führen eine externe Kontrolle aus, das heißt, dass sie »von außen« prüfen, ob Bestimmungen

des Datenschutzes eingehalten werden. Zusätzlich gibt es eine sogenannte interne Kontrolle, die von den betrieblichen oder behördlichen Datenschutzbeauftragten jeweils innerhalb eines Unternehmens oder innerhalb einer Behörde ausgeübt wird. Die Kirchen sowie die Rundfunkanstalten haben jeweils besondere Datenschutzbeauftragte für ihren Bereich. Neben diesen Institutionen auf nationaler Ebene gibt es einen Europäischen Datenschutzbeauftragten, dessen Hauptaufgabe darin besteht, die Verarbeitung persönlicher Daten durch Organe der Europäischen Union (beispielsweise durch die Kommission oder das Parlament) zu kontrollieren (siehe dazu auch den Beitrag von Hijmans/Langfeldt in diesem Band, S. 403 ff.).

Im Folgenden werden die für Deutschland wichtigsten datenschutzrechtlichen Kontrollorgane beschrieben. Dies sind der Bundesdatenschutzbeauftragte, die Landesdatenschutzbeauftragten und die Aufsichtsbehörden als externe Kontrollstellen sowie die betrieblichen und behördlichen Datenschutzbeauftragten als interne Kontrollstellen.

2 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Die Kontrollbehörde für öffentliche Stellen des Bundes ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI).

Öffentliche Stellen des Bundes sind:[1]

- Behörden des Bundes (beispielsweise Bundesministerium für Finanzen),
- Organe der Rechtspflege des Bundes (beispielsweise Bundesverfassungsgericht),
- andere öffentlich-rechtlich organisierte Einrichtungen im Bundesbereich (beispielsweise Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts unter Bundesaufsicht),
- bestimmte Vereinigungen öffentlicher Stellen des Bundes und bestimmte von diesen beherrschte Unternehmen, Gesellschaften oder Einrichtungen, auch in privater Rechtsform (beispielsweise Bundesdruckerei).

Die Person des BfDI wird gemäß § 22 Absatz 1 BDSG auf Vorschlag der Bundesregierung durch das Parlament gewählt. Ihre Amtsdauer beträgt fünf Jahre, sie darf nur einmal wiedergewählt werden. Der BfDI ist in der Ausübung seines Amtes unabhängig. Damit ist gemeint, dass er nur dem Gesetz unterworfen sein soll. Er unterliegt jedoch der Rechtsaufsicht der Bundesregierung und der Dienstaufsicht des Bundesinnenministeriums.

Das bedeutet, dass die Bundesregierung einschreiten kann, wenn der BfDI offensichtlich gegen geltendes Recht verstößt. Das Bundesinnenministerium ist gesetzlich verpflichtet, dem BfDI die zur Erfüllung seiner Aufgaben erforderliche Personal- und Sachausstattung zur Verfügung zu stellen. Dies muss im Haushaltsplan des Ministeriums in einem eigenen Kapitel ausgewiesen werden. So soll verhindert werden, dass der BfDI aus Personalmangel oder aus finanziellen Gründen gehindert wird, seine Aufgaben effektiv wahrzunehmen.

3 Die Landesdatenschutzbeauftragten

Die Landesbeauftragten für Datenschutz kontrollieren die Verarbeitung persönlicher Daten durch öffentliche Stellen der Länder. Öffentliche Stellen der Länder sind:[2]

- Landesbehörden,
- Organe der Rechtspflege der Länder,
- andere öffentlich-rechtlich organisierte Einrichtungen im Landes- und Kommunalbereich,
- bestimmte Vereinigungen, Gesellschaften, Unternehmen und Einrichtungen öffentlicher Stellen eines Landes, auch in privater Rechtsform.

Die Organisation der Landesdatenschutzbeauftragten ist in den verschiedenen Bundesländern unterschiedlich ausgestaltet. Vorgaben für die Organisation finden sich in den jeweiligen Landesdatenschutzgesetzen. In den meisten Fällen genießen die Landesdatenschutzbeauftragten eine dem BfDI vergleichbare Unabhängigkeit. Auch die Regelungen über den Haushalt und das Personal entsprechen vielfach den Regelungen, die für den BfDI gelten.

4 Die Aufsichtsbehörden

Die Datenschutzaufsicht über den sogenannten nicht-öffentlichen Bereich (im Wesentlichen juristische Personen und Personenvereinigungen, aber auch natürliche Personen, soweit sie personenbezogene Daten verarbeiten, vgl. § 2 Absatz 4 BDSG) liegt nach § 38 BDSG bei den sogenannten Aufsichtsbehörden. Wer dies ist, wird von den Bundesländern bestimmt. Die Länder haben von dieser Befugnis in sehr unterschiedlicher Weise Gebrauch gemacht. In fünfzehn Bundesländern wurden

die Landesdatenschutzbeauftragten und die Aufsichtsbehörde in einer Stelle zusammengefasst. In Bayern gibt es getrennte Stellen (Stand Juli 2012).[3]

5 Unabhängigkeit der Kontrollstellen

Die Arbeit der datenschutzrechtlichen Kontrollstellen ist auch Gegenstand der Europäischen Datenschutzrichtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995.[4] Gemäß Artikel 28 der Datenschutzrichtlinie müssen die Kontrollstellen ihre Aufgaben in »völliger Unabhängigkeit« wahrnehmen. Dies trifft nach Ansicht des Europäischen Gerichtshofs (EuGH) nicht auf die Aufsichtsbehörden in Deutschland zu.

In einem Urteil des EuGH[5] wurde Deutschland dazu verpflichtet, die Organisation dieser Stellen zu ändern und ihnen »völlige Unabhängigkeit« zu gewährleisten. Das Verfahren gegen die Bundesrepublik Deutschland wurde im Jahr 2005 durch die Beschwerde eines Bürgers eingeleitet. Dieser begründete seine Beschwerde gegenüber der EU-Kommission damit, dass die ministerielle Aufsicht die Unabhängigkeit der Datenschutzbeauftragten behindere. Besonders im Bereich der Polizeiarbeit könne es zu Interessenkonflikten zwischen den Datenschutzbehörden und den Innenministerien kommen.

Während, wie oben beschrieben, die Landesdatenschutzbeauftragten und der BfDI nur einer beschränkten Rechtsaufsicht unterliegen, sahen bis zu diesem Urteil des EuGH die meisten Landesdatenschutzgesetze vor, dass die Aufsichtsbehörden der Fachaufsicht eines Ministeriums unterliegen. Dadurch hatten die Ministerien theoretisch die Möglichkeit, der Aufsichtsbehörde Weisungen zu erteilen und Einfluss auf die Entscheidungen der Aufsichtsbehörde zu nehmen. Die deutsche Regierung hielt diese Regelung für rechtmäßig, da die Aufsichtsbehörden nicht in einer Abhängigkeit zu den privaten Stellen standen, sondern nur zu öffentlichen Stellen, die sie aber nicht zu kontrollieren hatten. Diese Interpretation von Unabhängigkeit bezeichnet man als funktionale Unabhängigkeit. Der EuGH hat jedoch deutlich gemacht, dass die Datenschutzrichtlinie nicht nur eine funktionale Unabhängigkeit fordert, denn »die Kontrollstellen (müssen) bei der Wahrnehmung ihrer Aufgaben objektiv und unparteiisch vorgehen. Hierzu müssen sie vor jeglicher Einflussnahme von außen, einschließlich der unmittelbaren oder mittelbaren Einflussnahme des Bundes oder der Länder, sicher sein und nicht nur vor der Einflussnahme seitens der kontrollierten Einrichtungen«.[6]

Abschaffung der Rechts- und Fachaufsicht

Das Urteil bezieht sich zunächst nur auf die Aufsichtsbehörden für den nicht-öffentlichen Bereich. In seiner Entscheidung betonte das Gericht jedoch, dass jede Möglichkeit der Einflussnahme auf alle datenschutzrechtlichen Kontrollstellen auszuschließen ist.

Folgt man der Argumentation des Gerichts, dann können berechtigte Zweifel daran bestehen, ob die derzeitigen Formen der Rechtsaufsicht über den Bundes- und die Landesdatenschutzbeauftragten mit den Anforderungen des EuGH an eine »völlige Unabhängigkeit« übereinstimmen. Der EuGH hat deutlich gemacht, dass die Unabhängigkeit notwendig ist, um einen effektiven Grundrechtsschutz zu gewährleisten. In dem Urteil heißt es: »Die Unabhängigkeit der Behörden wurde eingeführt, um die von ihren Entscheidungen betroffenen Personen und Einrichtungen stärker zu schützen, und nicht, um diesen Kontrollstellen selbst oder ihren Bevollmächtigten eine besondere Stellung zu verleihen.«[7] Schon das Bundesverfassungsgericht hat in seiner Volkszählungsentscheidung (siehe den Beitrag von Papier in diesem Band, S. 67 ff.) betont, dass unabhängige Kontrollstellen ein wichtiges Element des Grundrechtsschutzes darstellen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, die Rechts- und Fachaufsicht auch für die Landesdatenschutzbeauftragten und den BfDI abzuschaffen. Die Dienstaufsicht soll darüber hinaus so gestaltet werden, dass keine mittelbare oder unmittelbare Einflussnahme möglich ist.[8]

6 Behördliche und betriebliche Datenschutzbeauftragte

Wie eingangs erwähnt, unterscheidet das BDSG zwischen einer externen und einer internen Kontrolle der datenverarbeitenden Stelle. Zunächst existierte diese Unterscheidung nur für den nicht-öffentlichen Bereich. Als das BDSG geschaffen wurde, stellte aus Sicht der Wirtschaft die externe Kontrolle einen Eingriff in die unternehmerische Betätigungsfreiheit dar. Viele Wirtschaftsvertreter hätten sich gewünscht, dass gar keine externe Kontrolle stattfinden würde. Der Gesetzgeber entschied sich jedoch im Jahr 1977, für den nicht-öffentlichen Bereich eine Kombination aus Fremd- und Selbstkontrolle einzuführen. Für den öffentlichen Bereich gab es zunächst keine interne Kontrolle. Die behördlichen Datenschutzbeauftragten sind also eine neuere Entwicklung im Bereich der datenschutzrechtlichen Kontrolle. Gesetzlich notwendig sind sie erst seit dem Jahr 2001.

Gesetzliche Pflicht zu deren Bestellung

Sowohl die betrieblichen als auch die behördlichen Datenschutzbeauftragten sollen die Arbeit der externen Datenschutzbehörden (Landesdatenschutzbeauftragter, Bundesdatenschutzbeauftragter und Aufsichtsbehörden) nicht ersetzen, sondern ergänzen. Sie sollen intern auf die Einhaltung der datenschutzrechtlichen Vorschriften hinwirken. Die europäische Datenschutzrichtlinie sieht vor, dass Behörden und Unternehmen einen eigenen Datenschutzbeauftragten bestellen *können*. Ist das der Fall, muss nicht jede automatisierte Datenverarbeitung vorher bei der Datenschutzbehörde angemeldet werden. In Deutschland ist die Bestellung eines Datenschutzbeauftragten jedoch grundsätzlich Pflicht (von der es landesgesetzliche Ausnahmen gibt), wenn bestimmte Voraussetzungen erfüllt sind, die vor allem auf größere Betriebe und alle öffentlichen Stellen zutreffen, die Daten automatisiert verarbeiten.

Rechtsstellung

Wer die Aufgabe des oder der Datenschutzbeauftragten ausübt, kann die datenverarbeitende Stelle entscheiden. Es kann auch eine Person sein, die nicht bei dieser Stelle beschäftigt ist. Das BDSG fordert aber hinsichtlich deren Qualifikation das Vorhandensein der erforderlichen Fachkunde und Zuverlässigkeit. Es darf also keine Person bestellt werden, die die technischen, organisatorischen und rechtlichen Gegebenheiten der Datenverarbeitung nicht beurteilen kann. Ebenso darf keine Person ernannt werden, deren Position darauf schließen lässt, dass datenschutzrechtliche Vorschriften eher als »Hindernis« empfunden werden könnten (etwa Beschäftigte des internen Sicherheitsdienstes).

Auch die internen Datenschutzbeauftragten sollen ihre Aufgaben frei von Interessenkonflikten wahrnehmen. Da ihnen daher ein hohes Maß an Unabhängigkeit eingeräumt werden muss, sind sie bei der Ausübung ihres Amtes weisungsfrei. In der Praxis lässt sich das oftmals schwer durchsetzen, etwa wenn gegenüber den Beschäftigten neue Überwachungsmaßnahmen eingeführt werden sollen (beispielsweise maschinelle Erfassung der Arbeitszeiten). Wie alle Beschäftigten stehen interne Datenschutzbeauftragte hier und in anderen Situationen jedoch vor dem Problem, dass sie ihren Arbeitsplatz durch Kritik an der Unternehmensleitung nicht gefährden möchten. Der Gesetzgeber begegnet diesem Interessenskonflikt unter anderem dadurch, dass interne Datenschutzbeauftragte besonders vor Kündigungen geschützt werden. Ob die internen Kontrollstellen wirksam zum Schutz des

Rechts auf informationelle Selbstbestimmung beitragen können, ist aber letztlich davon abhängig, wie wichtig die jeweiligen Beauftragten und die Leitungsebene ihrer Organisation diese Aufgabe nehmen.

7 Mechanismen der Datenschutzkontrolle

Die Hauptaufgabe der Datenschutzbehörden besteht darin, die Einhaltung der Datenschutzvorschriften zu kontrollieren und durch Beratung sowie Erteilung von Informationen und Auskünften auf die Einhaltung der Datenschutzvorschriften hinzuwirken. Zur Erfüllung dieser Aufgaben wurden ihnen gesetzlich verschiedene Befugnisse eingeräumt. Im Folgenden soll beschrieben werden, wie diese Befugnisse in der Praxis umgesetzt werden.

Wann werden die Datenschutzbehörden tätig?

Zumeist werden die Datenschutzbehörden aufgrund von Beschwerden tätig. Nach dem BDSG kann sich jede Person an die jeweils zuständige Kontrollstelle wenden, wenn sie der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten durch öffentliche Stellen des Bundes oder durch nicht-öffentliche Stellen in ihren Rechten verletzt worden zu sein.[9] Die Landesdatenschutzgesetze enthalten für die Anrufung der Landesdatenschutzbeauftragten entsprechende Regelungen. Solche Beschwerden von Bürgerinnen und Bürgern, die im Datenschutzbereich »Eingaben« heißen, bedürfen keiner besonderen Form. Sie können schriftlich, elektronisch oder telefonisch erfolgen und auch anonym eingelegt werden. Häufig gehen die Datenschutzbehörden auch Hinweisen nach, die sie durch die Berichterstattung über Datenschutzverletzungen in den Medien erhalten.

Auch ohne Hinweise oder Beschwerden dürfen die Datenschutzbehörden jederzeit überprüfen, ob eine Stelle bei der Verarbeitung personenbezogener Daten die Datenschutzvorschriften einhält. In der Praxis finden solche anlasslosen Kontrollen beispielsweise als Stichproben- oder Branchenprüfungen statt. Dabei können etwa zufällig ausgewählte Unternehmen einer Branche zu den in der Branche üblicherweise durchgeführten Datenverarbeitungen befragt werden. Außerdem werden anlasslose Kontrollen vielfach dann durchgeführt, wenn geprüft werden soll, ob Unternehmen sich an eine neue Gesetzeslage halten oder wenn besonders viele bzw. besonders sensible Daten, etwa Gesundheitsdaten, in einem Unternehmen verarbeitet werden.

Wie werden die Datenschutzbehörden tätig?

Unabhängig davon, ob eine öffentliche oder eine nicht-öffentliche Stelle personenbezogene Daten verarbeitet, nehmen die Datenschutzbehörden Beschwerden von Betroffenen in der Regel zum Anlass, die verantwortliche Stelle entweder telefonisch bzw. schriftlich zur Stellungnahme aufzufordern oder eine Vor-Ort-Prüfung durchzuführen. Die verantwortliche Stelle bzw. deren leitendes Personal ist verpflichtet, den Datenschutzbehörden Auskunft zu erteilen. Bei einer schriftlichen Anfrage fordern die Datenschutzbehörden die Stelle auf, den Sachverhalt aus ihrer Sicht zu schildern oder auf konkrete Fragen zu antworten. Die Datenschutzbehörden prüfen dann die Stellungnahme der angeschriebenen Stelle und bewerten, ob die Verarbeitung personenbezogener Daten rechtmäßig war. Kommen die Datenschutzbehörden zu dem Ergebnis, dass kein Verstoß gegen Datenschutzvorschriften vorliegt, werden die Betroffenen und die verantwortliche Stelle abschließend darüber informiert.

In der Praxis kommt es bei nicht-öffentlichen Stellen, beispielsweise Unternehmen, nicht selten vor, dass die Datenschutzbehörden zunächst gar keine Antwort erhalten. Dieses Verhalten kann unangenehme Konsequenzen haben: Wer die Auskunft vorsätzlich oder fahrlässig verweigert oder nur unvollständig oder gar falsch antwortet, kann mit einem Bußgeld von bis zu 50 000 Euro belegt werden. Die Datenschutzbehörden nehmen solches Verhalten häufig auch zum Anlass, eine Vor-Ort-Kontrolle durchzuführen. Die Mitarbeiterinnen und Mitarbeiter der Datenschutzbehörden sind befugt, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der kontrollierten Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Dabei dürfen sie Geschäftsunterlagen, Verzeichnisse aller Datenverarbeitungsverfahren, personenbezogene Daten und Datenverarbeitungsprogramme einsehen. Die kontrollierte Stelle bzw. deren Leitungspersonen müssen diese Maßnahmen dulden. Weigert sich die kontrollierte Stelle bzw. deren Leitungspersonal, die Beschäftigten der Datenschutzbehörden einzulassen, erfüllt auch dieses Verhalten einen Bußgeldtatbestand, der mit bis zu 50 000 Euro geahndet werden kann.

Bei den öffentlichen Stellen der Länder sind die Befugnisse der Landesbeauftragten für den Datenschutz je nach Landesgesetz unterschiedlich. Dies gilt jedenfalls für das Recht, in Datenverarbeitungssysteme und Unterlagen Einsicht zu nehmen. Allen Landesgesetzen ist allerdings gemein, dass die Datenschutzbeauftragten zur Ausübung ihrer Kontrollbefugnisse jederzeit Zugang zu allen Diensträumen erhalten sollen.

Wie die Datenschutzbehörden im Einzelfall vorgehen, um den Sachverhalt zu ermitteln, liegt in ihrem Ermessen. Bei dieser Entscheidung spielen Kapazitätsfragen eine Rolle. Eine Vor-Ort-Prüfung ist häufig aufwändig, so dass die erste Kontaktaufnahme durch die Datenschutzbehörden üblicherweise telefonisch oder schriftlich stattfindet.

8 (Sanktions-)Befugnisse der Datenschutzbehörden

Wenn die Datenschutzbehörden zu dem Ergebnis kommen, dass ein Verstoß gegen Datenschutzgesetze vorliegt, stehen ihnen verschiedene Rüge- bzw. Sanktionsbefugnisse zur Verfügung. Sie können als schwächste Form des Vorgehens eine »Beanstandung« aussprechen. Damit stellen sie fest, dass ein Datenschutzverstoß vorliegt, und fordern die kontrollierte Stelle auf, diesen abzustellen.

Bußgeldverfahren

Datenschutzverstöße können auch im Wege von Bußgeldverfahren sanktioniert werden. Dies betrifft insbesondere nicht-öffentliche Stellen. Die Datenschutzbehörden der Länder können Bußgelder in Höhe von bis zu 300 000 Euro erlassen, wenn Datenschutzverstöße vorsätzlich oder fahrlässig begangen wurden. Wenn der Täter höhere wirtschaftliche Vorteile dadurch erlangt hat, dass er die Datenschutzvorschriften nicht beachtet, kann auch eine höhere Geldbuße festgesetzt werden. Für die Bemessung der Höhe eines Bußgeldes spielen etwa die wirtschaftlichen Verhältnisse der Person, gegen die sich das Bußgeldverfahren richtet, und das Ausmaß des Verstoßes sowie die Umstände der Begehung eine Rolle.

Gegen einen Bußgeldbescheid können die Betroffenen innerhalb von zwei Wochen Einspruch einlegen. Der Einspruch führt dazu, dass das Verfahren vor dem zuständigen Amtsgericht eingeleitet wird. Das Gericht entscheidet darüber, ob der Betroffene freigesprochen, eine Geldbuße festgesetzt oder das Verfahren eingestellt wird. Das Gericht darf von der im Bußgeldbescheid getroffenen Entscheidung nicht zum Nachteil des Betroffenen abweichen, das heißt die Höhe des Bußgeldes darf nur herabgesetzt werden.

Bußgeldverfahren, statt bloßer Beanstandungen, werden beispielsweise eingeleitet, wenn es sich um einen besonders schwerwiegenden Verstoß gegen Datenschutzvorschriften handelt oder wenn die Stelle schon mehrfach durch Datenschutzverstöße aufgefallen ist. Ein Bußgeldver-

fahren kommt auch dann in Betracht, wenn die datenverarbeitende Stelle die Beanstandung und rechtliche Bewertung der Aufsichtsbehörde nicht anerkennt und eine Veränderung ihrer Datenverarbeitungsverfahren ablehnt.

Verpflichtung zur Durchführung bestimmter Maßnahmen

In einem Bußgeldbescheid wird (nur) festgestellt, dass ein bestimmtes Verhalten rechtswidrig war; Handlungsanweisungen für die Zukunft werden nicht erteilt. Anders verhält es sich, wenn die Datenschutzbehörde eine Anordnung nach § 38 Absatz 5 BDSG, das heißt einen Verwaltungsakt, erlässt: Die Anordnung erlegt der nicht-öffentlichen Stelle die Verpflichtung auf, entsprechend der angeordneten Maßnahmen zu handeln. Die Anordnung muss konkret und bestimmt beschreiben, welche Maßnahmen zu ergreifen sind, und darf keine unverhältnismäßigen Anforderungen stellen. Die betroffene Stelle hat die Möglichkeit, hiergegen Widerspruch einzulegen.

Bei schwerwiegenden Verstößen oder Mängeln dürfen die Datenschutzbehörden sogar die Datenverarbeitung als Ganzes oder den Einsatz einzelner Verfahren untersagen. Daneben kann die Aufsichtsbehörde beispielsweise bei schwerwiegenden Verstößen gegen das Bundesdatenschutzgesetz die Gewerbeämter unterrichten, die wegen der Unzuverlässigkeit des Gewerbetreibenden gewerberechtliche Maßnahmen ergreifen können.

Unterrichtung der Betroffenen

Bei einem Verstoß gegen das Bundesdatenschutzgesetz unterrichten die Datenschutzbehörden außerdem die Betroffenen. Im Falle einer unüberschaubaren Anzahl von Betroffenen kann es erforderlich sein, die Datenschutzverstöße öffentlich zu machen, um die Betroffenen zu benachrichtigen.[10] Solche negativen Schlagzeilen treffen die Unternehmen manchmal empfindlicher als Geldbußen oder Anordnungen.

Sind Datenschutzverstöße strafbar?

Verstöße gegen Datenschutzvorschriften stellen in den meisten Fällen nur eine Ordnungswidrigkeit dar, die mit den oben beschriebenen Bußgeldern geahndet werden kann. Wer schwerwiegende Datenschutzverstöße vorsätzlich, das heißt mit Wissen und Wollen, begeht und dafür Geld erhält oder in der Absicht handelt, sich oder jemand anderen zu bereichern oder

zu schädigen, begeht jedoch gemäß § 44 BDSG eine Straftat und kann mit einer Freiheitsstrafe von bis zu zwei Jahren bestraft werden. Solche Straftaten werden nur auf Antrag verfolgt. Neben den Betroffenen sind auch die Datenschutzbehörden berechtigt, einen Strafantrag bei den Strafverfolgungsbehörden zu stellen.

Darüber hinaus gibt es Vorschriften im Strafgesetzbuch (§§ 201 ff. StGB), die unter anderem Verletzungen der Privatsphäre unter Strafe stellen und somit ebenfalls Verstöße gegen das Recht auf informationelle Selbstbestimmung ahnden. In diesen Fällen sind aber nur die Betroffenen berechtigt, einen Strafantrag zu stellen.

9 Gesetzlicher Modernisierungsbedarf für eine effiziente Datenschutzkontrolle

Durch die Novellierung des Bundesdatenschutzgesetzes im Jahr 2009 wurden die Anordnungs- und Untersagungsbefugnisse der Aufsichtsbehörden erweitert. Es ist davon auszugehen, dass die Aufsichtsbehörden von diesen Instrumenten mehr und mehr Gebrauch machen werden, nicht zuletzt aufgrund der verbesserten Durchsetzungsmöglichkeiten. Dies hat nicht zwingend zur Konsequenz, dass die Anzahl der Bußgeldverfahren zukünftig zurückgehen wird, da beide Instrumente nebeneinander stehen können. Sowohl Anzahl als auch Höhe der Geldbußen haben in den vergangenen Jahren rapide zugenommen. Dies ist sicherlich auf die vielen Datenschutzskandale zurückzuführen. Durch die Höhe der erlassenen Bußgelder wurden ebenfalls neue Maßstäbe gesetzt, die sich in der Praxis verfestigen werden. Diese Entwicklungen ändern allerdings nichts daran, dass die Datenschutzbehörden an ihre Grenzen stoßen, wenn die Datenschutzgesetze nicht modernisiert und an die Herausforderungen des Informationszeitalters angepasst werden (siehe auch den Beitrag von Roßnagel in diesem Band, S. 331 ff.).

Anmerkungen

1 Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (Hrsg.), Bundesdatenschutzgesetz – Text und Erläuterungen (BfDI-Info 1), Bonn 2011, S. 15, im Internet unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO1_Januar_2011.html?nn=409164.

2 Ebd., S. 15 f.

3 Eine Übersicht bietet die Website des BfDI im Internet unter http://www.bfdi.bund.de/DE/AnschriftenUndLinks/AufsBehoerdFuerDenNichtOeffBereich/AufsBehoerdFuerDenNichtOeffBereich_node.html (eingesehen: Mai 2012).
4 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.
5 Urteil des EuGH vom 9.3.2010 – C 518/07; im Internet unter http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=de&alljur=alljur&jurcdj=jurcdj&jurtpi=jurtpi&jurtfp=jurtfp&numaff=C-518/07&nomusuel=&docnodecision=docnodecision&allcommjo=allcommjo&affint=affint&affclose=affclose&alldocrec=alldocrec&docor=docor&docav=.
6 Ebd., Rd. 25.
7 A. a. O.
8 »Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle!«, Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17./18.3.2010, im Internet unter http://www.datenschutz-berlin.de/content/deutschland/konferenz.
9 § 21 Satz 1 bzw. § 38 Abs. 1 Satz 7 in Verbindung mit § 21 Satz 1 BDSG.
10 Die datenverarbeitende Stelle selbst hat gemäß § 42a BDSG die Pflicht, die Betroffenen zu informieren, etwa wenn durch ein Datenleck bestimmte Arten von Daten, beispielsweise besonders sensible Informationen wie Gesundheitsdaten, an Dritte offenbart werden und für die Betroffenen schwerwiegende Beeinträchtigungen drohen.

Kirsten Bock

Marktwirtschaftlicher Datenschutz

Mit personenbezogenen Daten lässt sich viel Geld verdienen. Das ist nicht immer im Sinne der Betroffenen. Wer mit Kreditkarte bezahlt, schätzt zwar die Vorteile des bargeldlosen Einkaufs, rechnet aber nicht notwendig damit, dass seine Einkaufsgeschichte(n) analysiert und gewinnbringend weiterverkauft werden. Wer in →sozialen Netzwerken unterwegs ist, schätzt die problemlose Kontaktaufnahme und Kommunikation mit Gleichgesinnten, nicht aber die Analyse seiner Vorlieben und Verhaltensweisen durch die Anbieter. Das kommerzielle Abgreifen, Auswerten, Verketten und Weiterverkaufen von Informationen über Personen hat mittlerweile eine hohe marktwirtschaftliche Relevanz erreicht und stellt ein zunehmendes Problem der Informationsgesellschaft dar, weil diese Praktiken das Vertrauen der Nutzenden in die angebotenen Dienste unterlaufen. Unbeobachtete Freiräume schmelzen wie die Eismassen der Pole. Für Unternehmen kommen technische Herausforderungen hinzu: Sie müssen die ihnen von Kundinnen und Kunden anvertrauten Daten schützen – vor kriminellen Attacken, vor ungeschütztem Zugriff über das Internet und vor internen Datenlecks.

1 Datenschutz als Strukturaufgabe

Marktwirtschaftlicher Datenschutz soll sich an den Interessen der Akteure des Marktes orientieren. Dem geht die Erkenntnis voraus, dass ein moderner Datenschutz nur dann umzusetzen ist, wenn die für die Datenverarbeitung verantwortlichen Organisationen ein eigenes Interesse an der Umsetzung datenschutzrechtlicher Vorgaben haben.[1] Die Idee eines marktwirtschaftlichen Datenschutzes beinhaltet, Unternehmen zur Einhaltung staatlicher Vorschriften nicht nur durch Ge- und Verbote, sondern mithilfe marktwirtschaftlicher Anreize zu bewegen.

Beim Datenschutz kann es auch nicht darum gehen, isolierte Antworten auf einzelne Sachprobleme bestimmter Geschäftsmodelle aus dem Boden zu stampfen, wie zum Beispiel das »Geodatengesetz« zur Erfassung von →Geodaten durch → *Google Street View* und andere vergleichbare Dienste. Bereits die Weiterentwicklung der Informationstechnik und mit ihr die

Entstehung neuer Geschäftsmodelle innerhalb der letzten zehn Jahre zeigt anschaulich, wie schnell solche Gesetze überholt sein können. Datenschutz ist vielmehr eine Strukturaufgabe, der sich der Staat stellen muss. Problemen, wie sie beispielsweise im Zusammenhang mit Geodaten auftreten, muss man mit grundsätzlichen strukturellen Lösungen entgegenwirken. Dies erfordert im Wesentlichen zwei Dinge:

- Erforderlich ist ein Codex, der unabhängig von der technischen Entwicklung Datenschutz-Schutzziele bestimmt (siehe den Beitrag von Rost in diesem Band, S. 353 ff.).
- Diese Schutzziele müssen in eine praktische Systematik eingebunden werden, die mindestens vier Elemente berücksichtigt:
  - Grundsätze der Datenverarbeitung (siehe den Beitrag von Heckmann in diesem Band, S. 267 ff.)
  - Legitimität der Datenverarbeitung (siehe den Beitrag von Hartge in diesem Band, S. 280 ff.)
  - technisch-organisatorische Maßnahmen (siehe den Beitrag von Schaar in diesem Band, S. 363 ff.)
  - Betroffenenrechte (siehe den Beitrag von Dix in diesem Band, S. 290 ff.).

Eine solche Systematik böte eine verlässliche Grundlage für Unternehmen, im täglichen Handeln aber auch bei Forschung und Entwicklung den Datenschutz nicht aus dem Blick zu verlieren (→ *Privacy by Design*).

Neben einer solchen datenschutzrechtlichen Verlässlichkeit durch eine Kodifikation[2] von Schutzzielbestimmungen kann der Staat Instrumente zur Förderung marktwirtschaftlicher Anreize schaffen. Erfahrungen wurden bereits mit folgenden Instrumenten gesammelt:

- Zertifizierungsaudits in Form von Verfahrensaudits,
- produkt- und servicebezogene Gütesiegel,
- vergleichende Tests,[3]
- Datenschutz als Kosten- und Wettbewerbsfaktor.

Ein marktwirtschaftlicher Datenschutz soll sich an den Interessen der Akteure orientieren. Er muss sich deshalb mit der Frage befassen, welche Voraussetzungen zu erfüllen sind, damit der Datenschutz, das heißt die Beachtung des Rechts auf informationelle Selbstbestimmung, die Situation eines Unternehmens im Markt verbessern kann. Aus Unternehmenssicht wird Datenschutz noch immer als kostspieliges Hemmnis betrachtet, dem kein direkter Nutzen gegenübersteht. Das liegt auch daran, dass Datenschutzverstöße oftmals unentdeckt bleiben und überwiegend keine Folgekosten verursachen. Erst in letzter Zeit haben Datenschutzskandale das

Thema in den Blickpunkt der Öffentlichkeit gerückt und zu Imageschäden und einigen wenigen hohen Bußgeldern geführt. Während Daten- und Identitätsdiebstähle bei den Unternehmen direkt zu erheblichen Schäden und so zu einer Verstärkung des Schutzniveaus bei der IT-Sicherheit geführt haben, bleiben die Rechte der Betroffenen im Wettbewerb weitgehend auf der Strecke: Mit der zunehmenden Nutzung des Internets durch Private geraten die Nutzenden als potentielle Kundinnen und Kunden immer öfter ins Visier der Marketinganalysten, die sich über bestehendes Recht bewusst oder unbewusst hinwegsetzen. In diesen Fällen gerät die Missachtung des Datenschutzes zu einem direkten Wettbewerbsvorteil. Auf eine Durchsetzung des bestehenden Datenschutzrechts zu achten, dient auch der Herstellung eines fairen Wettbewerbs zwischen Unternehmen.

2 Appelle an die Wirtschaft sind nicht zielführend

Die letzten zehn Jahre haben gezeigt, dass bloße Appelle an die Wirtschaft, wenn überhaupt, nur zögerlich zum Ziel führen. Zwar geben inzwischen fast alle Unternehmen eine Datenschutzerklärung ab. Diese lassen jedoch meist von ihrem Informationsgehalt wie von ihrer Verständlichkeit zu wünschen übrig. Auch Ansätze, Nutzende durch die Möglichkeiten des Identitätsmanagements[4] besser zu schützen, haben in den vergangenen Jahren kaum sichtbare Fortschritte gebracht. Dafür hat sich die Situation der Betroffenen zugespitzt.

Beobachtung des Verhaltens

Webtracking lässt das unbeobachtete Surfen im Netz der Vergangenheit angehören. Folgende Beispiele zeigen wie *Webtracking* (→ *Tracking*) eingesetzt wird:

- Mit → *Cookies* kann das Klick-Verhalten von Nutzenden auf einer oder sogar verschiedenen Webseiten gesammelt und dann ausgewertet werden.
- Durch die Einstellungen des Browsers in Kombination mit dem Betriebssystem des Rechners und den Erweiterungen wie Werbeblockern oder *Toolbars* (Werkzeugleiste des Browsers) können Nutzende im Netz wiedererkannt (*Browser Fingerprint*[5]) und ihr Surfverhalten beobachtet werden.

Diese Art der Datenerhebung ist für Unternehmen kostengünstig und einfach. Für die Anwender erfolgt die Datenerhebung jedoch versteckt, sie haben kaum die Möglichkeit zu widersprechen.

3 Datenschutzmärkte

Während der Markt für Technologien zur Überwachung und zum Sammeln von Informationen über Menschen wächst, trifft dies auf den Markt für datenschutzfreundliche Technologien nicht zu. Das könnte daran liegen, dass den Menschen die Beachtung ihres Rechts auf Bestimmung darüber, wer, was und wann über sie weiß, nicht sonderlich wichtig erscheint.

Wissenschaftliche Untersuchungen[6] zeigen aber, dass dies nicht stimmt. Trotzdem treffen viele, auch datenschutzbewusste Menschen, oftmals unbewusst Entscheidungen zum Nachteil ihrer Privatsphäre. Sie tun dies, weil sie die Vor- und Nachteile ihrer Entscheidungen nicht bedenken oder weil sie die Wirkzusammenhänge nicht kennen (können). Die für eine rationale Entscheidung erforderlichen Informationen sind meist nicht verfügbar, oder die Konsequenzen der Entscheidung liegen unabsehbar in der Zukunft, oder es wird ihnen beispielsweise in →sozialen Netzwerken gar keine andere (kostenlose) Wahl gelassen. Diese Ursachen führen zu einem Nachfragemangel nach Datenschutz. Der Staat könnte diese Nachfragen stärken, indem er bestimmte Maßnahmen selbst anordnet, beispielsweise:

- Konsumgebote oder -verbote,
- Subventionen für datenschutzfreundliche Systeme,
- Abgaben für Systeme, die nicht datenschutzfreundlich sind,
- Informations- und Aufklärungskampagnen.

Mit diesen Mitteln würde der Staat regulierend in den Wettbewerb der Unternehmen eingreifen. Zum Schutz von wichtigen Rechten und Gütern kann das erforderlich sein (etwa Verbot der Kinderpornographie). In den meisten Fällen ist es aber besser, die Unternehmen wetteifern miteinander um die Kundinnen und Kunden sowie die besten Produkte, so dass keine Beeinträchtigung der Wettbewerbsfreiheit erfolgt.

Den Markt für personenbezogene Daten auf die Verbrauchermärkte zu beschränken, ist aber zu kurz gegriffen. Längst spielen personenbeziehbare Informationen auch eine Rolle im Handel zwischen den Unternehmen. Am augenscheinlichsten ist das im Adresshandel und Marketing der Fall. In diesem Bereich hat die Verbraucherseite keinen direkten Einfluss auf die Auswertung und Bearbeitung von Informationen, die aus ihrem Verhalten generiert wurden. Oftmals ist sie sich des Informationsgehaltes gar nicht bewusst oder sie ist, wie beim →*Scoring* der Versicherungs- und Finanzbranche, der Macht großer Konzerne ausgeliefert. In solchen Fällen kann nur ein gesetzlich geregeltes (Belohn-)System zusätzliche Anreize für die Einhaltung datenschutzrechtlicher Regelungen schaffen.

4 Wettbewerbsanreize

Wie kann man einen marktwirtschaftlichen Datenschutz attraktiv für die Unternehmen machen? Als grundlegende Voraussetzung wurde schon die ausreichende Durchsetzung des bestehenden Datenschutzrechts betrachtet. Hier gilt der Grundsatz: Die Missachtung datenschutzrechtlicher Vorgaben darf keinen Wettbewerbsvorteil darstellen!

Für Unternehmen muss sich die Einhaltung der datenschutzrechtlichen Vorgaben finanziell positiv oder zumindest neutral im Verhältnis zum Wettbewerber auswirken. Zur Beurteilung des Kosten-Nutzen-Verhältnisses ist es erforderlich, die negative Kostenseite für Datenschutzverstöße abschätzen zu können. Darüber gibt es im Moment nur vage Informationen. Auf der Negativseite stehen Imageschäden und Bußgelder. Imageschäden sind schwer zu beziffern. Bußgelder werden nur in seltenen Fällen verhängt und betragen im Regelfall zwischen 50 000 Euro und 300 000 Euro, was insbesondere für größere Unternehmen keine hohen Summen sind. Demgegenüber stehen die meist höheren Kosten für Investitionen in die Datensicherheit und eine datensparsame, transparente, beschäftigtenfreundliche und nutzerzentrierte – eben eine datenschutzfreundliche – Ausgestaltung von Produkten und Geschäftsprozessen. Soll sich der Einsatz datenschutzfreundlicher Technologien und Praktiken für ein Unternehmen lohnen, so muss sich dieses Verhalten auf den geschäftlichen Erfolg auswirken. Dazu können folgende Faktoren beitragen:

- Kundenvertrauen,
- Image,
- Glaubwürdigkeit,
- Beschäftigtenzufriedenheit,
- Rechtssicherheit,
- Wettbewerbsvorteil,
- Marktnische Datenschutz.

Unabhängig von den Marktfaktoren kann der Staat rechtliche Anreize beim Einsatz und Nachweis datenschutzfreundlicher Technologien und Prozesse schaffen durch

- Steuervorteile oder Subventionen,
- Bevorzugung bei öffentlichen Ausschreibungen,
- administrative Erleichterungen.

Der Staat kann freiwillige Angebote schaffen, die sich auf den Wettbewerb in einem Markt auswirken, ohne direkt in das Marktgefüge einzugreifen, so beispielsweise durch

- Audit-Zertifikate, etwa in Form von Gütesiegel und Verfahrensaudit
- vergleichende Tests.

Die Bundesregierung will Audits und vergleichende Tests wie bei der Stiftung Warentest durch eine Stiftung Datenschutz fördern. Das soll für mehr Vertrauen und eine höhere Nachfrage sorgen. Audits und Vergleichstests werden im Folgenden näher betrachtet.

5 Audit-Zertifikate

Unter einem Audit wird gemeinhin ein Untersuchungsverfahren verstanden, das sich auf einen vorab exakt bestimmten Untersuchungsgegenstand (Auditierungsgegenstand oder engl.: *Target of Evaluation*) bezieht und diesen hinsichtlich der Erfüllung von vorher festgelegten Anforderungen überprüft (statisches Überprüfungsaudit). Hauptziel des Audit-Zertifikates ist es, einen Nachweis für Qualität zu erbringen und dadurch Vertrauen zu schaffen.

Für den Datenschutz regelt § 9a Bundesdatenschutzgesetz (BDSG) die Einführung eines allgemeinen →Datenschutzaudits. Danach können »zur Verbesserung des Datenschutzes und der Datensicherheit (…) Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen.« Die genauen Anforderungen, die an ein solches Verfahren zu stellen sind, sollen jedoch in einem speziellen Gesetz geregelt werden.[7] Bisher gibt es jedoch keine besondere Vorschrift, die eine Auditierung auf Bundesebene regelt. Die Einführung eines freiwilligen bundesweiten Datenschutzaudits wird von Datenschützern immer wieder gefordert.[8] Die Landesgesetzgeber haben teilweise Vorschriften zur Auditierung im öffentlichen Bereich erlassen.[9] Schleswig-Holstein[10] und Bremen[11] haben darüber hinaus auch Vorschriften erlassen, die die nähere Ausgestaltung der Verfahren regeln.

Zertifikate im Bereich des Datenschutzes haben einen unterschiedlichen Aussagegehalt. Er hängt von der Relevanz der Kriterien ab, die im Anforderungskatalog für die Prüfung enthalten sind. Zertifizierungen können in Bereichen, in denen ansonsten Geschäftsgeheimnisse oder die Komplexität der Abläufe einer Offenlegung entgegenstehen, zu mehr Transparenz beitragen. Voraussetzung dafür ist aber, dass die Anforderungskataloge, auf deren Basis eine Zertifizierung erfolgt, öffentlich gemacht werden. Pauschale Ver-

weise auf gesetzliche Vorgaben genügen dazu nicht. Eine freie Veröffentlichung der Kriterienkataloge erfolgt aber meist nicht.[12] In diesen Fällen führt eine Zertifizierung nicht zu mehr Transparenz und Verbraucherinformation.

Neben der Veröffentlichung der Zertifizierungskriterien spielt die Fachkunde und Neutralität der Zertifizierungsstelle eine wesentliche Rolle für die Aussagekraft eines Zertifikats. Kriterien für die Kompetenz einer solchen Stelle gibt es mangels des noch immer fehlenden Ausführungsgesetzes zum § 9a BDSG nicht. Dafür reichen Kompetenzen im Bereich technischer Datensicherheit nicht aus, es bedarf darüber hinaus auch besonderer Kenntnisse im Datenschutz.

Prozess- und Verfahrensaudits

In einem Prozess- und Verfahrensaudit wird überprüft, ob ein vom Unternehmen festgelegtes Verfahren so durchgeführt wird, wie es das Unternehmen in der Verfahrensbeschreibung niedergelegt hat (Soll-Ist-Vergleich). Bei einer Überprüfung des Datenschutzmanagements spielen die unternehmensinternen Regelungen, die eine datenschutzkonforme Datenverarbeitung gewährleisten sollen, eine herausragende Rolle (siehe auch den Beitrag von Martin in diesem Band, S. 390 ff.). Ob diese Maßnahmen konkret geeignet sind und den rechtlichen Anforderungen genügen, wird in der Regel bei einem Verfahrensaudit nicht geprüft.

6 Datenschutz-Gütesiegel

Ein Datenschutz-Gütesiegel ist ein Zertifikat, das die Qualität eines (Muster-)Produktes bestätigt. Wichtig für die Aussagekraft des Gütesiegels sind die verwendeten Kriterien und – wie auch beim Verfahrensaudit – die Unabhängigkeit und Fachkunde der Gutachter, die die Prüfung durchführen. Werden die Kriterien vom Hersteller selbst auch nur mitbestimmt, leiden die Aussagekraft und Glaubwürdigkeit eines Siegels erheblich.[13] Im Folgenden werden zwei unterschiedliche Gütesiegel beschrieben.

Gütesiegel des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD)

Ein gesetzlich normiertes Datenschutzgütesiegel gibt es bislang nur für IT-Produkte, die in schleswig-holsteinischen Behörden eingesetzt werden können. Die Prüfung wird von freien Gutachtern anhand eines öffent-

lichen Kriterienkataloges[14] durchgeführt und vom ULD auf Vollständigkeit und Richtigkeit überprüft. Die doppelte Prüfung soll ein Gleichgewicht zwischen den Interessen der Unternehmen und den Verbraucherinteressen nach Vertrauenswürdigkeit und Vergleichbarkeit der Zertifikate herstellen. Die Überprüfung durch eine unabhängige dritte Stelle stellt sicher, dass alle relevanten Fragen von den Gutachtern mit der gleichen Intensität und angemessenem Aufwand behandelt werden. Dadurch werden die Ergebnisse vergleichbar.

Abb. 1: Gütesiegel des ULD Schleswig-Holstein

* vom ULD zum Einsatz bei öffentlichen Stellen in Schleswig-Holstein empfohlen gemäß § 4 Absatz 2 LDSG. Quelle: ULD Schleswig-Holstein, https://datenschutzzentrum.de.

Europäisches Datenschutz-Gütesiegel

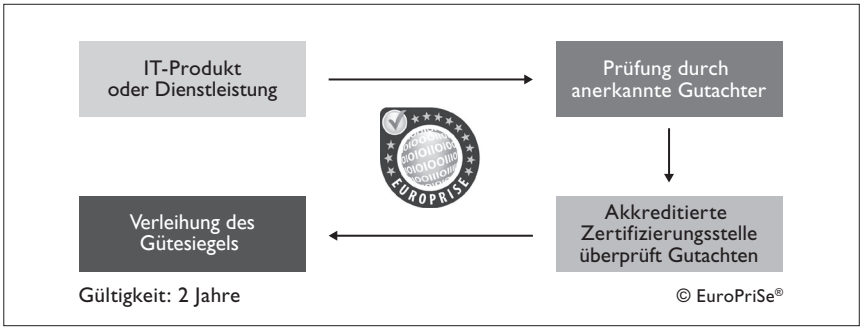
Das europäische Datenschutz-Gütesiegel (EuroPriSe)[15] wurde nach dem Vorbild aus Schleswig-Holstein entwickelt[16] und richtet sich an Hersteller und Anbieter von IT-Produkten und IT-basierten Dienstleistungen, insofern also nicht nur an öffentliche Stellen. Das europäische Datenschutz-Gütesiegel wird nach Erfüllung der Zertifizierungsanforderungen auf der Grundlage der Europäischen Datenschutzrichtlinie verliehen.

Abb. 2: Europäisches Datenschutz-Gütesiegel EuroPriSe

Quelle: EuroPriSe/ULD, https://www.european-privacy-seal.de.

Zu den Anforderungen gehören zudem die Vorlage der Datenschutzerklärung(en) und Auftragsdatenverarbeitungsverträge[17], die Absolvierung einer erfolgreichen Prüfung durch unabhängige Gutachter nach technischen und rechtlichen Kriterien, sowie schließlich die Vorlage und Akzeptanz eines umfassenden Evaluationsberichts.[18] Es wird nach dem in Abbildung 3 dargestellten Schema verliehen.

Abb. 3: Ablauf zur Verleihung des europäischen Datenschutz-Gütesiegels



Die EuroPriSe-Kriterien basieren auf den Regeln, die in Europa durch alle nationalen Datenschutzgesetze verwirklicht werden sollen. Das ist vor allem für jene Unternehmen praktisch und kostensparend, die ihr Produkt oder ihren Dienst in mehreren europäischen Ländern anbieten. Die Unternehmen können sich als Inhaber des Gütesiegels darauf berufen, dass sie die europäischen Datenschutzvorschriften einhalten. Im Gegenzug können die Verbraucher sich auf dieses Gütesiegel verlassen.

7 Vergleichende Tests

Vergleichende Tests kennen wir von der Stiftung Warentest oder dem Öko-Test. Es werden vergleichbare Produkte (zum Beispiel Versicherungsprodukte oder →soziale Netzwerke) nach vorher bestimmten Kriterien geprüft. Die Ergebnisse werden ausgewertet und nebeneinander gestellt, um der Verbraucherseite einen Vergleich zu ermöglichen. Auch auf dem Gebiet des Datenschutzes gibt es Bestrebungen, solche Tests einzuführen, die beispielsweise eine unabhängige »Bundesstiftung Datenschutz« durchführen soll.[19] Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat angemerkt, dass dieses Vorhaben folgende Punkte voraussetzt:

- Die Stiftung nimmt ihre Aufgaben unabhängig von den datenverarbeitenden Stellen und der IT-Wirtschaft wahr.
- Die größtmögliche Transparenz der Tätigkeit der Stiftung wird garantiert.
- Die Stiftung kooperiert eng mit den Datenschutzbehörden des Bundes und der Länder.
- Die Stiftung nimmt keine Aufgaben wahr, die den Datenschutzbehörden gesetzlich zugeteilt ist.[20]

Im Unterschied zu Gütesiegeln erfolgt der Test in der Regel nicht freiwillig. Die Tester haben nur die Informationen zu Verfügung, die durch eine Analyse aus dem Produkt selbst oder den dazu bereitgestellten Informationen (beispielsweise Produktbeschreibungen) zu erlangen sind. Dies ist problematisch, wenn ohne Herstellerwissen eine Analyse kaum möglich ist (etwa bei Softwareprodukten) oder Teile des Produktes oder Dienstes nur beim Anbieter selbst geprüft werden können. So kann bei einem Test von sozialen Netzwerken beispielsweise nicht geprüft werden, welche Informationen über die Nutzenden beim Anbieter analysiert und möglicherweise weitergegeben werden. Vergleichende Tests sind auch nur sinnvoll für Produkte und Dienste, die den Verbraucherinnen und Verbrauchern direkt angeboten werden. Ein vergleichender Test etwa von Adresshändlern dürfte weder auf das Verbraucherverhalten noch auf die Anbieter maßgeblichen Einfluss haben. Auch ist zu bedenken, dass bei vergleichenden Tests die geprüften Kriterien regelmäßig auf ein überschaubares Maß begrenzt werden, um den Test für die Verbraucherseite verständlich und übersichtlich zu halten.

8 Vorteile von Tests und Gütesiegeln

Funktionierende Märkte brauchen Vertrauen. Gütesiegel, Audits und Tests sollen auf Verbraucherseite Vertrauen schaffen. Vertrauen lässt sich nur über Transparenz sowie unabhängige und fachlich kompetente Prüfungen erreichen. Die Ergebnisse der Prüfungen müssen daher öffentlich zugänglich und überprüfbar sein. Dann können die Verbraucherinnen und Verbraucher ihre Entscheidungen auf sachgerechte Informationen stützen. Die Vorteile liegen auch darin, dass die Unternehmen mehr Vertrauen in ihre Produkte erzielen und gleichzeitig neue datenschutzfreundlichere Märkte erschaffen. Sachgerecht ausgeführte Prüfungen entlasten außerdem die Aufsichtsbehörden bei ihrer Arbeit und tragen dazu bei, dass

die Rechte der Nutzerinnen und Nutzer besser geschützt werden. Eine Stiftung Datenschutz kann diesen Prozess sinnvoll unterstützen, wenn sie Verbraucherinitiativen und Datenschutzbehörden in ihren Anliegen unterstützt, mehr Transparenz und Wissen über Probleme des Datenschutzes und die Bedeutung von Verbraucherverhalten zu schaffen. Sie kann zu einem wachsenden Markt für datenschutzfreundliche Produkte und der Stärkung des Prinzips → *Privacy by Design* beitragen (siehe auch den Beitrag von Schaar in diesem Band, S. 363 ff.).

Anmerkungen

1 Alexander Roßnagel, Marktwirtschaftlicher Datenschutz im Datenschutzrecht der Zukunft, in: Helmut Bäumler/Albert von Mutius (Hrsg.), Datenschutz als Wettbewerbsvorteil, Wiesbaden 2002; Alexander Roßnagel/Andreas Pfitzmann/Hansjürgen Garstka, Modernisierung des Datenschutzrechts, Berlin 2001, im Internet unter http://www.lda.brandenburg.de/sixcms/media.php/2473/dsmodern.pdf.

2 Dies bedeutet, dass bestimmte Ziele oder Inhalte in einem Gesetz festgeschrieben (kodifiziert) werden.

3 Für Schleswig-Holstein bestimmt § 4 Abs. 2 S. 1 LDSG dass »Produkte, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde, (…) vorrangig eingesetzt werden« sollen. Untersuchungen zur Wirksamkeit dieser Regelung liegen bislang nicht vor. Weitere Formen marktwirtschaftlicher Anreize wurden bislang aber kaum entwickelt oder untersucht.

4 Identitätsmanagementsysteme im Bereich des Internets dienen vornehmlich der Verwaltung verschiedener Benutzerprofile. Sie sollen Nutzenden die Möglichkeit geben, bestimmte Dienste unter → Pseudonym nutzen zu können bzw. nur die im jeweiligen Kontext nötigen Daten preiszugeben (z. B. beim Einkaufen im *Online*shop oder im *Online*forum der Autofans).

5 Dt.: Fingerabdruck des Browsers. Aus den genannten Einstellungen können unter Umständen Rückschlüsse auf die Nutzenden und ihre Gewohnheiten gezogen werden. Dies gilt besonders, wenn weniger verbreitete Browser genutzt werden.

6 Vgl. z. B. bei Alessandro Acquisti, Privacy in Electronic Commerce and the Economics of Immediate Gratification, im Internet unter http://www.heinz.cmu.edu/~acquisti/papers/privacy-gratification.pdf.

7 Auf Bundesebene wurde bisher kein Datenschutzaudit-Gesetz erlassen. Es gab einen Entwurf für ein solches Gesetz (BT-Drs. 16/12011), der jedoch stark kritisiert wurde und daher letztlich scheiterte. Der Entwurf sah vor, dass nicht-öffentliche Stellen ihr Datenschutzkonzept oder ihre Produkte und Dienstleistungen mit einem Datenschutzauditsiegel kennzeichnen können, sobald dies beim Bundesbeauftragten für Datenschutzschutz und Informationsfreiheit (BfDI) angezeigt wird.

Erst nach dieser Anzeige war eine Kontrolle durch eine vom BfDI zuzulassende Kontrollstelle vorgesehen (vgl. Peter Gola/Rudolf Schomerus, Kommentar zum BDSG, § 9a Rn. 2).

8 Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Ein modernes Datenschutzrecht für das 21. Jahrhundert (Eckpunkte) 2010, S. 27. Auch die Europäische Kommission plant, im Rahmen ihres Gesamtkonzeptes für den Datenschutz in der Europäischen Union Verfahren der Selbstregulierung zu fördern.

9 Beispiele sind: § 11c BbgDSG; § 7b BremDSG; § 10a DSG NRW; § 4 Abs. 2 LDSG SH.

10 Landesverordnung über ein Datenschutzaudit (GS Schl.-H., S. 51–Gl. Nr. 204–4–2).

11 Bremer Datenschutzauditverordnung vom 15.10.2004; Brem.GBl. S. 515.

12 Nicht öffentlich waren zum Zeitpunkt der Erstellung dieses Beitrags z. B. die ISO-Standards der 27000-Reihe (gegen Entgelt) sowie die Kriterien für das Datenschutz-Zertifikat des TÜV Saarland.

13 TÜV-Siegel: Alles andere als unfehlbar, in: Öko-Test Kompakt »Gütesiegel«, Frankfurt/M. 2010.

14 Im Internet unter: https://www.datenschutzzentrum.de/guetesiegel/infos_gutachter.htm.

15 S. https://www.european-privacy-seal.eu.

16 Dem EuroPriSe-Projektkonsortium unter Leitung des ULD gehörten neun Partner aus acht EU-Mitgliedsstaaten an: die Datenschutzaufsichtsbehörden von Madrid, Agencia de Protección de Datos de la Communidad de Madrid (APDCM), und Frankreich, Commission Nationale de l'Informatique et de Libertés (CNIL), die Österreichische Akademie der Wissenschaften, die London Metropolitan University, Borking Consultancy aus den Niederlanden, Ernst and Young AB aus Schweden, TÜV Informationstechnik GmbH aus Deutschland und VaF s. r. o. aus der Slowakei. Seit Ende der Projektphase 2009 wird EuroPriSe beim ULD weitergeführt.

17 Werden Daten durch einen Dritten im Auftrag verarbeitet, muss zwischen dem Auftraggeber und dem Auftragnehmer ein schriftlicher Vertrag geschlossen werden, der die in § 11 Absatz 2 BDSG benannten Kriterien zu erfüllen hat.

18 Weitere Informationen im Internet unter https://www.european-privacy-seal.eu.

19 Erstmals angekündigt wurde eine solche Stiftung auf Seite 106 des Koalitionsvertrages zwischen FDP und CDU. Zusätzlich beschreiben ein Eckpunkte-Papier der FDP und ein »Diskussionspapier für eine Konzeption der Stiftung Datenschutz« des BfDI vom 1.2.2011 die Aufgaben der Stiftung.

20 Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3./4.11.2010 zum Thema »Förderung des Datenschutzes durch Bundesstiftung«, im Internet unter http://www.datenschutz.hessen.de/k80.htm.

Peter Hustinx

Informationsfreiheit und Datenschutz in der Europäischen Union

Dieser Beitrag geht der Frage nach, wie das Recht auf freien Zugang zu staatlichen Informationen und das Recht auf Datenschutz in Einklang gebracht werden können.

1 Das Recht auf Zugang zu amtlichen Informationen

Das Recht auf Zugang zu staatlichen Informationen ist eine wichtige Ausprägung des Transparenzgrundsatzes, der wiederum ein Grundprinzip in der Europäischen Union (EU) darstellt.[1] Transparenz ist einer der grundlegenden Werte demokratischer und rechtsstaatlich organisierter Gesellschaften. Nur wenn die Bürgerinnen und Bürger Informationen über das Handeln staatlicher Organe erhalten, können sie deren Tätigkeiten nachvollziehen, bewerten und kontrollieren. Dementsprechend muss es auch ein Recht darauf geben, dass Bürgerinnen und Bürger diese Informationen einsehen können, wenn staatliche Organe die Informationen nicht freiwillig veröffentlichen.

Transparenz ist auch ein wichtiger Grundsatz im Datenschutzrecht. Durch das Recht auf Auskunft[2] soll die Speicherung und Verarbeitung personenbezogener Daten für die Betroffenen transparent gemacht werden (siehe auch den Beitrag von Dix in diesem Band, S. 290 ff.).

2 Rechtliche Grundlagen für die Transparenz staatlichen Handelns

Der Grundsatz der Transparenz staatlichen Handelns wird durch viele rechtliche Instrumente abgesichert und konkretisiert. Zum Beispiel beinhaltet die EU-Grundrechtecharta einen Anspruch auf Zugang zu amtlichen Informationen.[3] Ein solcher Anspruch findet sich auch in vielen nationalen Verfassungen. Fast alle EU-Mitgliedstaaten haben sogenannte Informationsfreiheitsgesetze verabschiedet, mit denen ein spezifisches Recht auf Informationszugang konkretisiert wird.

Auf der Ebene der Europäischen Union ist Transparenz ein Schlüsselprinzip gemäß Artikel 1 des EU-Vertrages, wonach »Entscheidungen so offen wie möglich zu treffen« sind. Das Recht auf öffentlichen Zugang zu EU-Dokumenten wurde zudem als ein grundlegendes Recht im Jahr 2000 bei der feierlichen Verkündung der EU-Grundrechtecharta anerkannt.

Der Europäische Gerichtshof für Menschenrechte (EGMR) hat schon einmal das Recht auf Zugang zu amtlichen Dokumenten in den Kontext des Rechts auf freie Meinungsäußerung nach Artikel 10 der Europäischen Menschenrechtskonvention gestellt.[4] Außerdem gibt es eine Konvention[5] des Europarates über den Zugang zu amtlichen Dokumenten, die nicht nur EU-Mitgliedsstaaten unterzeichnet haben.[6]

Auskunftsansprüche nach dem deutschen Informationsfreiheitsgesetz

In Deutschland formuliert das Informationsfreiheitsgesetz des Bundes (IFG) für Bürgerinnen und Bürger einen Anspruch auf Zugang zu amtlichen Dokumenten gegenüber Behörden und anderen Einrichtungen des Bundes. Auf Landesebene gibt es teilweise entsprechende Regelungen.[7] Dieser Anspruch gilt aber nicht uneingeschränkt. Die Behörden können die Herausgabe von Dokumenten verweigern, wenn bestimmte Voraussetzungen vorliegen. So darf etwa der Zugang zu Informationen, die persönliche Daten enthalten, nur gewährt werden, soweit das Informationsinteresse des Antragstellers das schutzwürdige Interesse des Dritten am Ausschluss des Informationszugangs überwiegt oder der Dritte eingewilligt hat. Ob ein Zugang zu den Dokumenten gewährt wird, entscheidet die Behörde, bei der sich die Dokumente befinden. Die Interessenabwägung ist dabei oftmals schwierig zu treffen.

3 Interessenabwägung zwischen Informationsfreiheit kontra Datenschutz und Schutz der Privatsphäre

Informationszugangsrechte sind also auf europäischer und nationaler Ebene gut etabliert. Dies bedeutet jedoch nicht, dass alle Informationen ohne jede Ausnahme der Öffentlichkeit zugänglich sein sollten.

Behörden können die Freigabe der Informationen in bestimmten Fällen verweigern, denn es gibt berechtigte Interessen, die eine Geheimhaltung rechtfertigen können. Es kann sich entweder um Interessen des Staates handeln (etwa bestimmte Sicherheitserwägungen) oder aber um Interes-

sen von einzelnen Personen, die nicht möchten, dass Informationen über sie bekannt werden, die in den öffentlichen Akten enthalten sind.

Bürgerinnen und Bürger sind in Europa in zweifacher Hinsicht davor geschützt, dass Informationen über ihre Person ungewollt veröffentlicht werden

- durch das Recht auf Privatsphäre,[8]
- durch den Schutz personenbezogener Daten.[9]

Die Rechte auf Privatsphäre und auf Datenschutz haben grundsätzlich die gleiche Wertigkeit wie das Recht auf Informationszugang. Das heißt in Fällen, in denen ein Interessenskonflikt entsteht, kann man nicht von vornherein sagen, dass ein bestimmtes Interesse überwiegt. Beispiele für solche Konflikte sind, wenn etwa

- ein Bürger die Offenlegung der Gesundheitsakte eines Beamten verlangt,
- eine Zeitung Einblick in die Ausgaben eines Mitgliedes eines nationalen oder des Europäischen Parlaments haben möchte.

Es bedarf in diesen Fällen einer präzisen Abwägung der zugrunde liegenden Interessen. Dabei gilt: eine korrekte Abwägung zwischen im Konflikt stehenden Grundrechten (hier: Datenschutz und das Recht auf Privatsphäre einerseits und Informationszugang andererseits) erfolgt am besten im konkreten Einzelfall und unter Berücksichtigung aller relevanten Umstände. Die genannten Rechtsinstrumente bieten jedoch selten eine klare Handlungsanweisung, wie man Konflikte zwischen diesen Interessen lösen kann.

In grundrechtlicher Hinsicht sind, wie schon erwähnt, die Informationsfreiheit und das Recht auf Privatsphäre als gleichwertige Rechtsgüter anzusehen. Deshalb bedarf es gesetzlicher Vorschriften, die den Ausgleich auf nationaler (in Deutschland beispielsweise durch das IFG) oder europäischer Ebene regeln. Solche Gesetze müssen einen klaren Rahmen abstecken, innerhalb dessen eine angemessene Abwägung des Informationszugangsrechts mit konkurrierenden Rechtsgütern (Datenschutz, Privatsphäre, staatliche Sicherheit etc.) erreicht werden kann. Ohne einen solchen Rahmen ist es schwierig, im Einzelfall zu entscheiden, ob etwa eine Zeitung bestimmte Informationen erhalten darf oder nicht.

Ein solcher Rahmen gibt den Bürgerinnen und Bürgern, aber auch der Verwaltung die nötige rechtliche Klarheit und Gewissheit und sollte zwei Risiken vermeiden:

- Personen dürfen durch die Veröffentlichung ihrer Daten nicht unverhältnismäßig beeinträchtigt werden. Die Veröffentlichung einer Ge-

sundheitsakte eines Beamten darf beispielsweise grundsätzlich nicht erlaubt sein, denn das Interesse des Beamten am Schutz seiner Gesundheitsdaten und seiner Privatsphäre wird immer das Informationsinteresse des Anfragenden oder der Allgemeinheit überwiegen;
- Datenschutzregeln dürfen nicht unberechtigt genutzt werden, um die Veröffentlichung von Informationen zu verhindern.

Insbesondere auf EU-Ebene zeigt die Praxis, dass unklare Regelungen zur Informationsfreiheit zu Verunsicherung, nicht endenden Diskussionen und gar zum Missbrauch führen. Es fehlt bisher jene gesetzliche Regelung, die solche Konflikte zuverlässig lösen kann.

Schutz der Privatsphäre als Grenze des Informationszugangsrechts

Für die Entscheidung, ob Dokumente veröffentlicht werden können, wenn sie Angaben über Personen enthalten, ist die Unterscheidung zwischen Privatsphäre (Schutz des privaten Lebens) und Datenschutz (Schutz personenbezogener Daten) relevant. Zwar sind beide Rechte eng miteinander verknüpft und überlappen sich teilweise, sie sind aber nicht identisch. Beleg hierfür ist die EU-Grundrechtecharta, wo diese beiden Rechte in Nachbarschaft zueinander stehen (Artikel 7 und 8). Die Unterscheidung soll hier nachfolgend verdeutlicht werden.

Privatsphäre

Das Recht auf Privatsphäre soll allen Menschen einen Raum oder einen Bereich garantieren, in dem sie ihr Leben frei von Eingriffen (zum Beispiel staatlicher Überwachung) gestalten können. Wie weit dieser Raum reicht und wie genau man die Privatsphäre bestimmt, ist nicht eindeutig definiert. Das Recht auf Privatsphäre wurde schon Ende des 19. Jahrhunderts sehr anschaulich als »*Right to be let alone*« (Recht, alleine gelassen zu werden) bezeichnet.[10]

Datenschutz

Das Datenschutzrecht dagegen sieht vor, dass persönliche Daten nicht erhoben und verarbeitet werden dürfen, wenn dies nicht gesetzlich erlaubt ist (siehe auch den Beitrag von Hartge in diesem Band, S. 280 ff.). Im deutschen Recht spricht man darüber hinaus vom Recht auf informationelle Selbstbestimmung (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.). Datenschutznormen sind auf jede Form der (automatisierten) Verarbeitung von Informationen anwendbar, die sich auf eine identifizierte

oder identifizierbare natürliche Person beziehen. Dabei ist es nicht relevant, ob die Daten einen Bezug zur Privatsphäre haben.[11]

Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte zum Informationsanspruch über Personen des öffentlichen Lebens

Die Unterscheidung zwischen dem Recht auf Privatsphäre und Datenschutz hat praktische Folgen. Trotz großer Überschneidungen gibt es Situationen, bei denen das Datenschutzrecht anwendbar ist, nicht aber der Schutz der Privatsphäre.

Dies zeigen Entscheidungen des Europäischen Gerichtshofs für Menschenrechte (EGMR). Der Gerichtshof legt im Allgemeinen den Begriff »privates Leben« sehr weit aus. Damit werden auch Teile des Berufslebens mit abgedeckt. Dennoch ist die Auslegung dieses Begriffs nicht unbegrenzt. Der Gerichtshof hat beispielsweise wiederholt festgestellt, dass die Veröffentlichung von Informationen über Politiker oder andere Personen des öffentlichen Lebens durch Zeitungen nicht in jedem Fall mit dem Schutz der Privatsphäre dieser Personen in Konflikt steht.

In dem Verfahren »Prinzessin von Monaco« stellte der Europäische Gerichtshof für Menschenrechte klar, dass auch öffentliche Personen ein Recht auf Privatsphäre haben.[12] Selbst wer berühmt ist, darf eine legitime Erwartung auf Privatleben haben. Dennoch müssen öffentliche Personen mit der Preisgabe von Informationen rechnen, die mit der Ausübung ihrer offiziellen Funktion oder ihren öffentlichen Aufgaben oder ihrer Rolle verbunden sind.

Das Datenschutzrecht hat einen viel weiteren Anwendungsbereich als das Recht auf Privatsphäre, denn es ist unabhängig von solchen Erwägungen anwendbar. Die Anwendbarkeit des Datenschutzrechts hängt nicht von den Privatsphärenansprüchen der Menschen im Hinblick auf den Umgang mit ihren Informationen ab. Diese Ansprüche können zwar bei der Bestimmung der rechtlichen Zulässigkeit der Verarbeitung der betreffenden Informationen eine Rolle spielen; sie entziehen der betroffenen Person aber nicht ihre von den Datenschutzregelungen zugestandenen Rechte und Mittel. Anders ausgedrückt: Auch wenn bestimmte Daten keinen Bezug zur Privatsphäre haben, aber einen Bezug zu einer natürlichen Person aufweisen, findet das Datenschutzrecht Anwendung. Zum Beispiel wird die Privatsphäre einer Person nicht allein dadurch verletzt, dass jemand das Kennzeichen ihres Autos notiert und an einen Dritten weiterleitet. Das Datenschutzrecht findet dennoch auf dieses Beispiel Anwendung, denn das Kennzeichen hat einen Personenbezug.

Das Recht auf Privatsphäre steht im Zentrum einer Abwägung mit dem Informationsinteresse

Eine Abwägung beim öffentlichen Informationszugang sollte auf die Privatsphäre abstellen und nicht auf den Datenschutz, wenngleich dieser nicht vernachlässigt werden darf. Dieser Vorschlag geht von der Erfahrung aus, dass genau in jenen Situationen, in denen es nicht um den Schutz des Privatlebens geht, die Anwendung von Datenschutzregeln unvernünftig ist oder gar missbraucht wird, um Informationsansprüche abzuwehren. Anders gesagt: In solchen Situationen überwiegt eindeutig das Interesse an der Veröffentlichung der Informationen gegenüber dem Interesse der betroffenen Person am Schutz ihrer persönlichen Daten. Die Informationen müssten also veröffentlicht werden, auch wenn datenschutzrechtliche Vorschriften vielleicht entgegenstehen.

Darüber hinaus sind Eingriffe in das Recht auf Privatsphäre aber nicht völlig ausgeschlossen. Es gibt Konstellationen, die in den Bereich des Schutzes der Privatsphäre fallen, und bei denen das Interesse an einer Veröffentlichung überwiegt. Das Recht auf Privatsphäre wird nicht grenzenlos gewährleistet. Staatliche Eingriffe in den Schutzraum der Privatsphäre sind zulässig, wenn ein legitimer Zweck verfolgt wird. Das Ergebnis dieser Prüfung ist jedoch von den spezifischen Umständen der konkreten Situation abhängig. Der Gesetzgeber sollte den Verwaltungsbehörden insofern für konkrete Feststellungen Raum lassen, indem die Informationszugangsgesetze einen Bezug zum Schutz der Privatsphäre herstellen.

4 Diskussionen über Informationsfreiheit in der Europäischen Union

Die Verordnung 1049/2001 über den öffentlichen Zugang zu Dokumenten[13] regelt einen Informationsanspruch gegenüber Einrichtungen der Europäischen Union (dazu zählen etwa die EU-Kommission und das Europäische Parlament). Darin wird sowohl auf die Privatsphäre als auch auf den Datenschutz Bezug genommen. Die dortige Wortwahl ist aber vieldeutig, eine eindeutige Entscheidung im Einzelfall daher schwierig. Die Erwähnung der Privatsphäre in dieser Verordnung war Anlass mancher Diskussionen und löste Irritationen aus, etwa im »Bavarian-Lager-Fall«[14].

Bavarian-Lager-Fall

In diesem Fall ging es um den Zugang zu Protokollen eines Treffens der Kommission, an dem Kommissionsbeamte, Vertreter der britischen Regierung und Vertreter eines Wirtschaftsverbandes teilnahmen. Da die Letztgenannten der Preisgabe ihrer Namen im Protokoll nicht zustimmten, legte die Kommission das Protokoll nur nach Schwärzung dieser Namen vor und berief sich auf Datenschutzregelungen. Die Klägerin begehrte aber die Vorlage ohne die entsprechenden Schwärzungen.

Im November 2007 urteilte das Gericht erster Instanz und wies die Ansicht der Kommission zurück, die auf die Privatsphäre der betroffenen Personen abstellte: »Der reine Umstand, dass ein Dokument Personendaten enthält, bedeutet nicht zwangsläufig, dass die Privatsphäre oder Integrität der betroffenen Person verletzt wird, auch wenn berufliche Tätigkeit im Grundsatz nicht von dem Konzept des privaten Lebens ausgeschlossen ist.« Es entschied, dass die Offenlegung der Namen »nicht das private Leben der fraglichen Personen beeinträchtigte«.

Die Europäische Kommission legte Berufung beim Europäischen Gerichtshof ein. Leider schloss sich der Gerichtshof der Meinung der Kommission und auch des Rates an und erklärte den Datenschutz ohne weitere Abwägung in einem Urteil vom 29. Juni 2010 für vorrangig. Das Dokument wurde also nicht ohne die Schwärzungen veröffentlicht. Die genauen Konsequenzen dieses Urteils für andere – ähnliche oder nicht ähnliche – Fälle sind zum jetzigen Zeitpunkt noch nicht deutlich und bedürfen der weiteren Präzisierung in späteren Urteilen des Gerichtshofs.[15]

5 Gesetzgebung sollte mehr Rechtssicherheit schaffen

Kurz zusammengefasst betont der von mir entwickelte Regelungsvorschlag[16] den Aspekt der Privatsphäre sowie die Integrität der Person. Genauer benannt werden darin Situationen, in denen eine Offenlegung von Informationen normalerweise nicht die Privatsphäre und die Integrität der betroffenen Person beeinträchtigt.

Informationen müssen beispielsweise offenbart werden, wenn sie sich lediglich auf berufliche Aktivitäten der betroffenen Person beziehen – es sei denn, dass angesichts der besonderen Umstände im Einzelfall Grund zu der Annahme besteht, dass die Person durch die Offenlegung negativ beeinträchtigt werden könnte – oder wenn sie schon mit dem Einverständnis der betroffenen Person veröffentlicht worden sind.

Aus meiner Sicht fördert die Nennung dieser spezifischen Beispiele Rechtssicherheit und verhindert Missbrauchsmöglichkeiten.

Eine Gesetzgebung mit weitergehenden Regelungen zu Informationszugang und Datenschutz muss meines Erachtens einen klaren Rahmen liefern, in dem ein gerechter Ausgleich gefunden werden kann. Bei sachgerechter Umsetzung wird dies die Missbrauchsrisiken der Regeln vermindern und auch Rechtsklarheit und -sicherheit schaffen. Hierauf haben die Bürgerinnen und Bürger in Europa einen Anspruch.

Anmerkungen

1 Der Transparenzgrundsatz ist in Art. 1 Abs. 2 des EUV niedergelegt. Darin heißt es: »Dieser Vertrag stellt eine neue Stufe bei der Verwirklichung einer immer engeren Union der Völker Europas dar, in der die Entscheidungen möglichst offen und möglichst bürgernah getroffen werden.« Die Transparenz bezieht sich auf die Entscheidungen staatlicher Organe. Jene sollen offen und nachvollziehbar getroffen werden.

2 Welches in Artikel 12 der Europäischen Datenschutzrichtlinie verpflichtend für alle Mitgliedsstaaten normiert ist.

3 Art. 41 Abs. 2 EU-Grundrechtecharta, im Internet unter http://www.europarl.europa.eu/charter/pdf/text_de.pdf.

4 Europäischer Gerichtshof für Menschenrechte, Fall »Társaság a Szabadságjogokért vs. Ungarn«, Urteil vom 14.4.2009 (37374/05).

5 Bei den Konventionen des Europarates handelt es sich um völkerrechtliche Verträge, die Staaten unterzeichnen können. Europarats-Konventionen sind keine verbindlichen Rechtsinstrumente, im Gegensatz zu den Richtlinien der EU. Letztere müssen von den Mitgliedern der EU in nationales Recht umgesetzt werden.

6 CETS No. 205. Inzwischen erfolgten vierzehn Unterschriften und fünf Ratifizierungen, unter anderem durch Schweden – das Land mit einer langen Tradition und vielfaches Vorbild in Sachen Transparenz (Stand: Juli 2012).

7 Beispielsweise Berliner Informationsfreiheitsgesetz, Brandenburger Akteneinsichts- und Informationszugangsgesetz, Gesetz über die Freiheit des Zugangs zu Informationen für das Land Bremen. Diese Regelungen beziehen sich auf den Zugang zu Informationen von Behörden oder anderen Einrichtungen der Länder.

8 Art. 7 EU-Grundrechtecharta.

9 Art. 8 EU-Grundrechtecharta.

10 Samuel D. Warren/Louis D. Brandeis, The Right to Privacy, in: Harvard Law Review Bd. IV (5/1890), im Internet unter http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (20.11.2011).

11 Bevor Datenschutzregeln in Deutschland und anderen EU-Ländern existierten, waren persönliche Daten nur geschützt, wenn sie einen Bezug zur Privatsphäre aufwiesen.

12 Europäischer Gerichtshof für Menschenrechte (III. Sektion), Urteil vom 24.6.2004 – Individualbeschwerde Nr. 59 320/00 (Caroline von Hannover vs. Deutschland).
13 Verordnung (EG) Nr. 1 049/2001 des Europäischen Parlaments und des Rates vom 30.5.2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission (Amtsblatt Nr. L 145 vom 31.5.2001 S. 0043 – 0048).
14 EuGH-Urteil vom 8.11.2007 – T-194/04 und EuGH-Urteil vom 29.6.2010 – C-28/08 P.
15 Siehe hierzu auch das Hintergrunddokument des EDSB zum öffentlichen Zugang zu Dokumenten mit personenbezogenen Daten nach dem Urteil in der Rechtssache Bavarian Lager, 24.3.2011, im Internet unter http://www.edps.europe.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers-03-24_Bavarian_Lager_DE.pdf.
16 Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission (2009/C 2/03), im Internet unter http://www.edps.europa.eu/EDPSWEB/edps/cache/off/lang/de/Consultation/OpinionsC/OC2008.

Alexander Roßnagel

Modernisierung des Datenschutzrechts

1 Modernisierungsbedarf

Das geltende Datenschutzrecht stammt konzeptionell aus den 1960er und 1970er Jahren. In dieser Zeit fand die Datenverarbeitung in Rechenzentren statt. Die Daten wurden in Formularen erfasst und per Hand eingegeben. Die Datenverarbeitung betraf nur einen kleinen Ausschnitt des Lebens und war – soweit die Daten direkt bei den Betroffenen (und nicht aus anderen Datenquellen) erhoben wurden – für diesen weitgehend kontrollierbar. Wurde die Zweckbindung beachtet, wussten die Betroffenen in der Regel, wo welche Daten über sie verarbeitet wurden. Für diese Stufe der Datenverarbeitung sind die Schutzkonzepte der ersten Datenschutzgesetze entwickelt worden. Aus dieser Zeit stammen die Regelungen zur Zulässigkeit der Datenverwendung, die Anforderungen an Unterrichtung und Benachrichtigung, an Zweckbestimmung und Zweckbindung, an die Erforderlichkeit der Datenverwendung, an die Rechte der Betroffenen und die Kontrolle durch Aufsichtsbehörden. Auch die 1995 in Kraft getretene europäische Datenschutzrichtlinie gehört zur Generation dieser Datenschutzgesetze. Die Nutzung von PCs in den 1980er Jahren hat die Datenschutzrisiken zwar erhöht, aber nicht auf eine neue qualitative Stufe gehoben.

Die zweite, qualitativ neue Entwicklungsstufe wurde mit der – weltweiten – Vernetzung der Rechner erreicht. Dadurch entstand ein eigener virtueller Sozialraum, in den nahezu alle Aktivitäten aus der körperlichen Welt übertragen wurden. Jede Handlung in diesem viele Lebensbereiche erfassenden *Cyberspace* hinterlässt Datenspuren, die ausgewertet werden können und auch werden. Weder die Erhebung der Daten noch deren – letztlich weltweite – Verbreitung und Verwendung können von den Betroffenen kontrolliert werden. → Web 2.0 oder → *Cloud-Computing* sind typische Ausprägungen dieser Entwicklungsstufe. Für sie gilt: Jeder Klick im elektronischen Kaufhaus, jede Suchanfrage, jedes Navigieren im Web, jeder Besuch in einem → sozialen Netzwerk, jedes Betrachten eines Bildes, jeder Download eines Songs, jedes → *Streamen* eines Filmes, letztlich: jede Regung in dieser virtuellen Welt hinterlässt eine Datenspur. Diese personenbezogenen Daten werden ausgewertet und genutzt. Kein Betroffener weiß, wer diese Daten erhält und wofür sie genutzt werden. Die damit

verbundenen Risiken versuchen die in den 1990er Jahre erlassenen Multimedia-Datenschutzgesetze in den Griff zu bekommen. Sie haben für die Internetdienste die Anforderungen an Transparenz, Zweckbindung und Erforderlichkeit verschärft und vor allem das neue Prinzip der Datensparsamkeit eingeführt.

Diese normativen Vorgaben können allerdings nur im Wirkungsbereich des Nationalstaats zur Geltung gebracht werden. Die neue Datenverarbeitung betrifft je nach Nutzung des Internets einen großen oder kleinen Ausschnitt des täglichen Lebens, diesen aber potenziell vollständig. Allerdings kann der Betroffene diesen Risiken zumindest noch dadurch entgehen, dass er den virtuellen Sozialraum meidet.

Mit →allgegenwärtigem Rechnen gelangt die Datenverarbeitung in die Alltagsgegenstände der körperlichen Welt – und damit auf eine neue, dritte Entwicklungsstufe. Mobiles Internet, →*Location Based Services*, →Geodatenverarbeitung und Automobil-EDV sind Vorboten dieser neuen Ära. Allgegenwärtige Datenverarbeitung erfasst potenziell alle Lebensbereiche und diese potenziell vollständig. In dieser Welt wachsen Körperlichkeit und Virtualität zusammen. Informationen aus der virtuellen Welt werden in der körperlichen Welt verfügbar, Informationen aus der realen Welt in die virtuelle Welt integriert. Aus dieser Welt und der in ihr stattfindenden Datenverarbeitung gibt es aber keinen Ausweg mehr. Insofern verschärft sich das Problem des Datenschutzes radikal und seine Lösung wird existenziell. Für diese neuen Herausforderungen gibt es noch keine spezifischen Regelungen.

Es lassen sich also drei Entwicklungsstufen im Verhältnis von Datenverarbeitung und Datenschutzrecht ausmachen: zentrale Datenverarbeitung in Rechenzentren; virtuelle Realität im Web; allgegenwärtiges Rechnen und →Internet der Dinge. Diese drei Stufen der Datenverarbeitung bestehen heute parallel und beeinflussen sich gegenseitig. Für alle drei besteht ein spezifischer Modernisierungsbedarf im Hinblick auf den Datenschutz.

- Für die erste Stufe besteht er vor allem in der Vereinfachung, Systematisierung und Effektivierung der unübersichtlichen Fülle Hunderter von Datenschutzregelungen mit unterschiedlichen Datenschutzniveaus, Ausnahmen und Gegenausnahmen.
- Für die zweite Stufe besteht der Modernisierungsbedarf vor allem darin, der technischen Mächtigkeit der globalen Systeme mit Konzepten des Selbst- und Systemdatenschutzes zu begegnen (siehe auch die Beiträge von Schaar, S. 363 ff., Schallbruch, S. 372 ff. und Thomsen, S. 381 ff. in diesem Band) und informationelle Selbstbestimmung auch in neuen Nutzungsformen (beispielsweise sozialen Netzwerken) zu sichern.

- Für die dritte Stufe besteht der Modernisierungsbedarf vor allem darin, neue Schutzkonzepte für die informationelle Selbstbestimmung zu entwickeln, weil die bisherigen normativen Schutzkonzepte zur Sicherung der Transparenz, der Zweckbindung, der Erforderlichkeit und der Wahrnehmung von Betroffenenrechten gegenüber den neuen Technikanwendungen leer laufen[1] (siehe auch den Beitrag von Rost in diesem Band, S. 353 ff.).

2 Modernisierungsprojekte

Die Modernisierungsdiskussion begann mit der zweiten Entwicklungsstufe. Als Reaktion auf die Herausforderungen des Internets wurden neue Konzepte entwickelt wie Datensparsamkeit und Datenschutz durch Technik, Selbst- und Systemdatenschutz, Datenschutzaudit und Zertifizierung. Sie wurden in der Internetaufbruchstimmung der 1990er Jahre im Teledienstedatenschutzgesetz (TDDSG) und Mediendienstestaatsvertrag ansatzweise realisiert und sollten bei Bewährung auch in andere Datenschutzgesetze übernommen werden.

Die eigentliche Modernisierung des Datenschutzrechts sollte breit angelegt sein. Es war geplant, in einem ersten kleinen Schritt die überfällige Anpassung an die europäische Datenschutzrichtlinie von 1995 durchzuführen (siehe auch den Beitrag von Hijmans/Langfeldt in diesem Band, S. 403 ff.) sowie den Grundsatz der Datensparsamkeit und die Ankündigungsnorm für ein Datenschutzaudit ins Bundesdatenschutzgesetz (BDSG) zu übernehmen. Zugleich wurde ein Gutachten vergeben, um eine umfassende Modernisierung vorzubereiten, die dann in einem zweiten Gesetzgebungsschritt umgesetzt werden sollte.[2] Im Jahr 2000 wurden Andreas Pfitzmann, Hansjürgen Garstka und der Autor vom Bundesinnenministerium beauftragt, ein Gutachten zu erstellen, wie das deutsche Datenschutzrecht den damaligen und künftigen Anforderungen angepasst werden könnte. Unterstützt wurde der Gutachtensauftrag von den Regierungsfraktionen der SPD und Bündnis 90/Die Grünen. Die politische Stimmung für eine Modernisierung des Datenschutzrechts war günstig. Es bestand ein hoher Konsens, dass das Datenschutzrecht einer Modernisierung bedarf und dass für diese auch neue Wege beschritten werden müssen.

Das Gutachten war Ende August 2001 fertig gestellt. Es enthielt eine Bestandsaufnahme, eine Bestimmung des Modernisierungsbedarfs, neue konzeptionelle Entwürfe für alle drei Modernisierungsebenen und sogar Vorschläge für die Formulierung einzelner Kapitel und Vorschriften eines

grundlegenden Datenschutzgesetzes.[3] Die Pressekonferenz für seine Übergabe an Bundesinnenminister Schily war für den 20. September 2001 vorgesehen. Mit dem Anschlag auf das *World Trade Center* am 11. September war jedoch das Interesse der Politik an einer Modernisierung des Datenschutzrechts wie weggeblasen.

Da der objektive Handlungsbedarf weiter bestand, wurde in den folgenden Jahren immer wieder eine Modernisierung des Datenschutzrechts gefordert[4] und auch in Koalitionsvereinbarungen angekündigt.[5] Doch glichen die Stimmen in der Literatur, die sich mit Analysen und Vorschlägen für sie einsetzten, einsamen Rufern in der Wüste und die Koalitionäre, die sie in ihre Agenda aufnahmen, politischen Wunschträumern. Datenschutzpolitik beschränkte sich im letzten Jahrzehnt vor allem darauf, die immer weiter gehenden Vorschläge für Überwachungsmaßnahmen zum Zweck der »inneren Sicherheit« zu begrenzen. Eine substanzielle Modernisierung des Datenschutzrechts passte nicht in die politische »Großwetterlage«.

Dennoch wurde bei jeder Novelle eines Datenschutzgesetzes erwartet, dass sie zumindest auch zur notwendigen Modernisierung beiträgt.[6] Dies war aber weder beim Erlass des Telemediengesetzes (TMG) 2006,[7] noch beim Entwurf eines Datenschutzauditgesetzes (DAG) 2007[8] noch bei den drei Novellen des BDSG 2009 der Fall. Das TMG schreibt nur die Regelungen des TDDSG fort, der Entwurf eines DAG hat die Idee eines Datenschutzaudits[9] völlig verkehrt und ist zu Recht gescheitert. Die → *Scoring*-Novelle hat zwar kleine Verbesserungen gebracht,[10] in der Novelle zum Adresshandel wurden jedoch selbst die bescheidenen Ansätze des Bundesinnenministeriums zur Realisierung des *Opt-in*-Prinzips durch Abgeordnete zunichte gemacht, die dem Druck eines massiven Lobbyismus erlagen.[11] Die Novellen zum Datenschutzrecht enthalten daher kaum Schritte zu einer Modernisierung des Datenschutzrechts.

Vielleicht ist jetzt – zehn Jahre nach dem Modernisierungsgutachten – die Zeit reif, einen neuen Versuch zu wagen. Hoffnung gibt zum einen die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die im Frühjahr 2010 »Eckpunkte für eine Modernisierung des Datenschutzrechts« vorgelegt hat.[12] Es ist schon als ein Fortschritt anzusehen, dass sich die Datenschutzbeauftragten aller Bundesländer zwar nicht auf einen Entwurf, aber doch auf eine Skizze möglicher Ansatzpunkte einigen konnten. Die Eckpunkte greifen viele Vorschläge des Modernisierungsgutachtens auf und passen sie in die gegenwärtige Diskussion ein. Dabei konzentrieren sie sich auf die Beseitigung von Defiziten in der Umsetzung von Datenschutzgrundsätzen aus der ersten und zweiten Entwicklungsstufe. Die Vorschläge der Datenschutzbeauftragten gehen von der Erkenntnis aus, dass datenschutzrechtliche Vorgaben an die

Datenverarbeitung praktisch wertlos sind, wenn sie nicht durch technisch-organisatorische Vorkehrungen abgesichert werden. Datenschutzrechtliche Regelungen müssen sich daher künftig stärker an Hersteller und Entwickler richten und auf durchsetzbare technische und organisatorische Maßnahmen des Datenschutzes zielen (siehe auch den Beitrag von Schaar in diesem Band, S. 363 ff.).

Weiterhin gibt die europäische Diskussion Anlass zur Hoffnung. Sie wurde im Januar 2012 dadurch eröffnet, dass die Europäische Kommission einen Entwurf für eine Datenschutz-Grundverordnung vorlegte.[13] Dieser zielt vor allem auf die Beseitigung von Defiziten in der Umsetzung von Datenschutzgrundsätzen aus der ersten Entwicklungsstufe. Hierfür bietet der Entwurf weiterführende Ansätze. Die Kommission will jedoch nicht nur die Rechte der Betroffenen stärken, sondern auch den Transfer personenbezogener Daten im Binnenmarkt und weltweit erleichtern. Diese Zielsetzung führt jedoch nur dann zu einer Modernisierung des Datenschutzes, wenn der Grundsatz des freien Verkehrs der Daten durch Datenschutz konsequent durchgehalten wird.[14] Enttäuschend ist allerdings, dass die Kommission die Bedeutung datenschutzfreundlicher Technologien[15] und Datenschutz durch Technik[16] nur allgemein anerkannt hat, ohne sie jedoch gegenüber den Herstellern zu regeln. Die notwendige Verknüpfung von Recht und Technik wurde nicht in der notwendigen Klarheit in den Entwurf aufgenommen. In diesem fehlen Vorgaben für Herstellung und Technikgestaltung zum Selbst- und Systemdatenschutz.

3 Modernisierungsinhalte

Die Präzisierung relevanter Begriffe, die Konkretisierung bestehender Regelungen, die Erweiterung geltender Anforderungen, die Verringerung bürokratischen Aufwands, die Ausweitung von Sanktionstatbeständen bei Rechtsverstößen, die Ergänzung von Eingriffsmöglichkeiten für die Aufsichtsbehörden – das alles sind wichtige Maßnahmen, um das Datenschutzrecht zu verbessern. Die notwendige Modernisierung des Datenschutzrechts bewirken sie aber auch in ihrer Gesamtheit nicht. Dieses Risiko, den Modernisierungsbedarf zu verfehlen, besteht vor allem für den Entwurf der Europäischen Kommission. So bietet er keine Lösungen für die Probleme der zweiten Entwicklungsstufe wie etwa das Kopplungsverbot oder den Selbstdatenschutz. Die grundlegenden Herausforderungen der dritten Entwicklungsstufe hat die Kommission bisher überhaupt nicht in ihren Entwurf aufgenommen.

Eine Modernisierung, die ein zukunftsfähiges Datenschutzrecht entwickeln will, muss aber Antworten für die absehbaren Probleme aller drei Entwicklungsstufen bieten. Insbesondere muss sie sich mit den Herausforderungen der allgegenwärtigen Verarbeitung personenbezogener Daten auseinandersetzen, die nicht nur neue und weitere Missbrauchsmöglichkeiten hervorbringt, sondern zentrale Schutzkonzepte des Datenschutzrechts in Frage stellt. In einer Welt allgegenwärtiger Datenverarbeitung laufen die bekannten Anforderungen der Zweckbindung, der Erforderlichkeit, der Transparenz, der Einwilligung und der Betroffenenrechte ins Leere. Die neuen Technikanwendungen verursachen daher nicht nur ein weiteres Vollzugs-, sondern ein grundlegendes Konzeptproblem.[17] Bedingung informationeller Selbstbestimmung ist deshalb ein grundsätzlich modifiziertes Schutzprogramm des Datenschutzrechts, das den tief greifenden Umwälzungen durch allgegenwärtige Datenverarbeitung gerecht wird. In welche Richtung daher eine Modernisierung des Datenschutzrechts gehen muss, soll kurz angedeutet werden.[18]

Gestaltungs- und Verarbeitungsregeln

Das bisher geltende Prinzip der Zulassungsregeln muss durch Gestaltungs- und Verarbeitungsregeln ergänzt werden. Derzeit gilt: Weit vor dem Entstehen neuer Datendienste (Beispiel: → *Google Street View*), entscheidet der Gesetzgeber grundsätzlich, ob eine Datenverarbeitung zulässig ist. Fehlt eine solche Entscheidung, entscheiden die Betroffenen einmalig, meist im Zusammenhang mit der erstmaligen Daten*erhebung* durch Einwilligung über die Zulässigkeit. Derartige Zulassungsentscheidungen, die lange vor der Verarbeitung und Nutzung der Daten liegen, bieten dem Gesetzgeber wie den Betroffenen nur unzureichende Möglichkeiten, die Bedingungen der weiteren Verarbeitung und Nutzung der Daten zu beeinflussen. Datenschutz sollte künftig vorrangig durch Gestaltungs- und Verarbeitungsregeln bewirkt werden, die permanent zu beachten sind.[19]

Solche Regeln können beispielsweise in Transparenzanforderungen bestehen. Statt die Betroffenen nur einmalig und nur über einzelne Daten zu unterrichten, sollten ihnen stärker Strukturinformationen über die Datenverarbeitung zur Verfügung gestellt werden. Mit Blick auf die Zukunft des allgegenwärtigen Rechnens könnte dies etwa dadurch gewährleistet werden, dass ein mit Sensoren oder →RFID ausgestattetes Produkt mit einem einfachen Symbol gekennzeichnet ist. Durch das Zeigen auf dieses Symbol mit dem → *Smartphone* könnte jeder Betroffene eine ständig einsehbare Datenschutzerklärung auf der Homepage des »intelli-

genten« Produkts einsehen. Darüber hinaus könnten Sensoren, die aktiv sind, eine technisch auswertbare Signalisierung und Kennung aussenden, die von »Datenschutzagenten« auf dem *Smartphone* des Betroffenen aufgenommen werden und je nach Einstellung durch den Nutzer zu einem Warnhinweis oder einer elektronischen Einwilligung führen.

Ein anderes Beispiel: Nutzen Betroffene freiwillig Techniksysteme und -dienste, die ihre individuellen Fähigkeiten unterstützen und verstärken sollen (zum Beispiel Navigationssysteme, die aus dem Verhalten des Nutzenden lernen, welche Präferenzen er hat und welche Informationen er in welcher Situation benötigt), könnte dies als *Opt-in* angesehen werden, das für die Verarbeitung der notwendigen Daten ausreicht. Zum Ausgleich müssten solche Systeme und Dienste so gestaltet sein, dass sie über konfigurierbare Datenschutzfunktionen verfügen. Die Benutzer des adaptiven Navigationssystems etwa könnten dann auswählen, ob das Profil ihrer Vorlieben bei dem Diensteanbieter oder auf ihrem Endgerät gespeichert wird.

Eine weiterreichende Gestaltungsregel wäre folgende: Jede Technikanwendung muss ihre Funktionen so wählen, dass sie mit möglichst wenig oder keinen personenbezogenen Daten auskommt. Bisher leitet allerdings die Europäische Kommission das Ziel der Datensparsamkeit aus dem Prinzip der Zweckbindung ab, und die Konferenz der Datenschutzbeauftragten leitet es aus dem Prinzip der Erforderlichkeit ab.[20] So verstanden, wäre das besondere Ziel der Datensparsamkeit überflüssig. Tatsächlich ist es jedoch ein eigenständiges Prinzip, das über die Zweckbindung und die Erforderlichkeit weit hinausgeht.[21] Es ist daher nicht auf die vom Datenverarbeiter gewählten Zwecke begrenzt, sondern beeinflusst diese Zweckwahl. Dies muss als Gestaltungsregel wirksam werden.

Letztes Beispiel: Bei individualisierten, adaptiven Systemen, die den Kontext des Nutzenden (in einer Besprechung, auf einer Reise, im Kino) über Sensoren erkennen können und ihre Leistungen danach ausrichten, stößt das Zusammenspiel zwischen enger Zwecksetzung und strenger Erforderlichkeit an seine Grenzen. Die Anpassungsleistung (der »Trainingserfolg«) solcher Systeme beruht auf der statistischen Auswertung möglichst großer Datenmengen. Hier muss das Datenschutzrecht stärker die Möglichkeiten sinnvollen anonymen und pseudonymen Handelns einfordern.[22] Zugleich sollte die Zweckbindung stärker auf Missbrauchsvermeidung und die Erforderlichkeit stärker auf Löschungsregeln hin konzentriert werden (»Recht auf Vergessen«[23]).

Vereinfacht und effektiviert würde der Datenschutz für viele Anwendungen, wenn zwischen einer Datenverarbeitung mit und ohne geziel-

ten Personenbezug unterschieden würde.[24] Für eine Datenverarbeitung ohne gezielten Personenbezug würde als zulässiger Zweck das Erbringen einer rein technischen Funktion anerkannt. Als Ausgleich für diesen weiten Erlaubnistatbestand müssten aber die Daten auf das erforderliche Minimum begrenzt und ihre Verwendung strikt auf diese Funktion begrenzt werden. Während ihrer Verarbeitung müssen sie gegen Zweckentfremdung geschützt und nach der Verarbeitung sofort gelöscht werden. Die Daten müssen außerdem einer strengen Zweckbindung unterliegen und durch ein Verwertungsverbot geschützt sein. Als Erleichterung sollte auf eine vorherige Unterrichtung des Betroffenen verzichtet und der Auskunftsanspruch auf eine Strukturauskunft reduziert werden.

Datenschutz durch Technikgestaltung

Die (rechtlichen) Gestaltungs- und Verarbeitungsregeln sind heute mehr denn je auf eine technische Umsetzung angewiesen.[25] Informationelle Selbstbestimmung muss durch Infrastrukturen unterstützt werden, die es ermöglichen, auf Gefährdungen automatisch zu reagieren, ohne dass dies aufdringlich oder belästigend wirkt. Die Einhaltung von Verarbeitungsregeln zu kontrollieren, darf – in einer Welt allgegenwärtiger Datenverarbeitung – nicht die permanente persönliche Aufmerksamkeit erfordern. Bei der Vielzahl solcher Datenverarbeitungsprozesse wäre jeder Nutzende damit schlicht überfordert. Eine effektive Prüfung auf eine datenschutzkonforme Verarbeitung muss deshalb technikgestützt, automatisiert erfolgen.

Ein ideales Szenario sähe etwa so aus: Wenn datenverarbeitende Alltagsgegenstände ein Signal aussenden, wird dieses von einem Endgerät erkannt, das für den Betroffenen die Funktion eines »Datenschutz-Assistenten« (ähnlich P3P[26]) erfüllt. Das Gerät wertet die zugehörige Datenschutzerklärung des jeweiligen Gegenstandes automatisch aus. Entsprechend der von seinem Besitzer voreingestellten Datenschutzpräferenzen erteilt der Assistent eine Einwilligung in die Datenverarbeitung oder lehnt diese ab. In Zweifelsfällen kann der Assistent je nach Voreinstellung den Betroffenen warnen und ihm die Erklärung in der von ihm gewählten Sprache anzeigen oder akustisch ausgeben. Die Hinweis- und Warndichte muss einstellbar sein. Der Vorteil einer solchen Technik liegt auf der Hand: Sie fordert vom Betroffenen keine ständige Aufmerksamkeit. Die von ihm gewählten Verarbeitungsregeln werden im Normalfall durch Technik und nicht durch sein persönliches Handeln durchgesetzt.[27]

Technischer Datenschutz hat gegenüber rein rechtlichen Vorgaben Effektivitätsvorteile: Was technisch verhindert wird, muss nicht verbo-

ten werden. Gegen Verhaltensregeln kann verstoßen werden, gegen technische Begrenzungen nicht. Datenschutztechnik kann so Kontrollen und Strafen überflüssig machen.

Die Umsetzung dieser Ziele sollte vor allem durch ein Datenschutzmanagementsystem erreicht werden. Die verantwortliche Stelle sollte in ihrem Datenschutzkonzept nachweisen, dass sie die Gestaltungsziele erreicht hat[28] (siehe auch Beitrag von Martin in diesem Band, S. 390 ff.).

Vorsorge für informationelle Selbstbestimmung

Wie in anderen Rechtsbereichen muss Vorsorge die Gefahrenabwehr ergänzen, zum einen durch die Reduzierung von Risiken und zum anderen durch präventive Folgenbegrenzungen potenzieller Schäden (siehe auch den Beitrag von Albers in diesem Band, S. 102 ff.). Die Risiken für die informationelle Selbstbestimmung sind in der zweiten und dritten Entwicklungsstufe der Datenverarbeitung nicht mehr ausreichend zu bewältigen, wenn nur auf die Verarbeitung personenbezogener Daten geachtet wird. Vielmehr sollten vorbeugend auch Situationen geregelt werden, in denen noch keine personenbezogenen Daten entstanden sind.

Das gilt zum Beispiel für Sammlungen von Sensorinformationen (etwa Bewegungsprofile), von Umgebungsdaten (etwa Einsatzprofile bei der Berufsausübung) oder von pseudonymen Präferenzen (etwa Einkaufsprofile). Sie sollten einer vorsorgenden Regelung unterstellt werden, falls die Möglichkeit oder gar die Absicht besteht, diese Daten irgendwann einmal mit einem Personenbezug zu versehen.[29]

Zur Risikobegrenzung sind daher von vornherein Anforderungen an eine transparente, datensparsame, kontrollierbare und missbrauchsvermeidende Technikgestaltung zu formulieren, wobei die Risiken vorab abzuschätzen und entsprechende Sicherheitskonzepte auszuarbeiten sind.[30] Ebenso entspricht es dem Vorsorgegedanken, die einzusetzenden Techniksysteme präventiven (freiwilligen) Prüfungen ihrer Datenschutzkonformität zu unterziehen und diese Prüfungen zu dokumentieren.

Wer die Technik gestaltet, sollte Regelungsadressat sein

Regelungen, die sich nur an die Datenverarbeitung richten, dürften viele Gestaltungsziele nicht erreichen. In viel stärkerem Maß sind daher diejenigen anzusprechen, die die Technik gestalten (siehe auch den Beitrag von Schaar in diesem Band, S. 363 ff.). Diese sollten vor allem Prüfpflichten für eine datenschutzkonforme Gestaltung ihrer Produkte, eine Pflicht

zur Dokumentation dieser Prüfungen für bestimmte Systeme und Hinweispflichten für verbleibende Risiken treffen.[31] Auch sollten sie ihre Produkte mit datenschutzfreundlichen Standardeinstellungen (*Privacy by Default*) ausliefern müssen.

Anreize und Belohnungen

Die datenschutzgerechte Gestaltung der künftigen Welt, insbesondere die Umsetzung von Zielen wie Datensparsamkeit oder Anonymität, fordert die aktive Mitwirkung der Entwickler, Gestalter und Anwender. Sie werden hierfür aber nur zu gewinnen sein, wenn sie davon einen Vorteil haben. Daher sollte die Verfolgung legitimen Eigennutzes in Formen ermöglicht werden, die zugleich auch Gemeinwohlbelangen dienen. Datenschutz muss zu einem Werbeargument und Wettbewerbsvorteil werden. Dies ist möglich durch die freiwillige Auditierung von Anwendungen, die Zertifizierung von Produkten und die Präsentation von Datenschutzerklärungen. Werden diese von Datenschutzrankings oder durch die Berücksichtigung bei öffentlichen Auftragsvergaben begleitet, kann ein Wettbewerb um den besseren Datenschutz entstehen (siehe auch den Beitrag von Bock in diesem Band, S. 310 ff.). Dann werden die Gestaltungsziele beinahe von selbst erreicht.[32]

Auch sollte Selbstregulierung in Bereichen, in denen dies möglich ist, durch Ziel- und Rahmensetzungen angeleitet, aber auch durch Entscheidungsmöglichkeiten und Erleichterungen angereizt werden.[33]

Institutionalisierte Grundrechtskontrolle

Der Schutz der informationellen Selbstbestimmung bedarf einer objektiven Ordnung, die in der Praxis zunehmend die Notwendigkeit individueller Rechtewahrnehmung überflüssig macht. Die Einhaltung von Datenschutzvorgaben darf künftig nicht von der individuellen Kontrolle des Betroffenen abhängig sein. Sie muss stellvertretend Kontrollverfahren und Kontrollstellen übertragen werden, die das Vertrauen der Betroffenen genießen.

Die Datenschutzbeauftragten sind zu stärken sowie Konkurrenten- und Verbandsklagen zu ermöglichen.[34] Die Kontrollen müssen stärker auf datenverarbeitende Systeme und deren Funktionen und Strukturen ausgerichtet werden, nicht so sehr die individuellen Daten. Ziel der Kontrolle muss es sein, die individuellen und gesellschaftlichen Wirkungen der technischen Systeme zu überprüfen und diese datenschutzgerecht zu gestalten.

4 Modernisierungschancen

Die bisherigen Novellen zum Datenschutzrecht zeigen, wie schwierig eine Modernisierung dieses Rechtsbereichs sein wird, der quer zu allen anderen Gesellschafts- und auch Rechtsbereichen liegt. Für die Modernisierung des Datenschutzrechts gilt erst recht die Forsthoff'sche Regel, dass Interessen umso schwerer zu organisieren und durchzusetzen sind, je allgemeiner sie sind. In den bisherigen Novellen ging es nur um beschränkte Korrekturen. Dennoch konnte sich das Interesse aller auf Schutz ihrer informationellen Selbstbestimmung kaum gegen den hoch organisierten und effektiven Lobbyismus derer durchsetzen, die individuelle Nachteile befürchteten. Dies lässt für die noch immer anstehende Modernisierung des Datenschutzrechts wenig hoffen.

Eine Modernisierung des Datenschutzrechts in einem Guss[35] dürfte für die Bundesrepublik Deutschland eine politisch zu anspruchsvolle Aufgabe sein. Neben der Unfähigkeit der Politik, eine so umfassende Neuordnung durchzusetzen, dürften hierfür vor allem die Ungleichzeitigkeiten des objektiven Modernisierungsdrucks in unterschiedlichen Lebensbereichen und ihre unterschiedliche Wahrnehmung entscheidend sein. Auch wird der Bedarf an rechtlicher Vorsorge für künftige Entwicklungen unterschiedlich eingeschätzt. Daher spricht viel dafür, die Modernisierung des Datenschutzrechts in mehreren Schritten umzusetzen. Um hierfür die Zielerreichung und Kohärenz zu sichern, sollte auf der Grundlage des Vorschlags der Konferenz der Datenschutzbeauftragten ein Mustergesetz erarbeitet werden, das als Orientierungsrahmen für die einzelnen Modernisierungsnovellen dient.

Für die Modernisierung des Datenschutzrechts ist die Überarbeitung der europäischen Datenschutzregeln von größter Bedeutung. Die Bewertung des Entwurfs der Datenschutz-Grundverordnung der Europäischen Kommission muss auf zwei Ebenen erfolgen. Hinsichtlich einer notwendigen umfassenden inhaltlichen Modernisierung des Datenschutzrechts springt der Entwurf inhaltlich zu kurz. Neben einigen hilfreichen Vorschlägen für einzelne Instrumente enthält er kein durchgängiges Modernisierungskonzept. Hierfür ist er noch zu sehr den Fragen der ersten und (zum Teil) der zweiten Entwicklungsstufe verhaftet. Hinsichtlich eines Datenschutzes durch Technik fallen die Regelungen – trotz großer Ankündigungen – enttäuschend aus.

Noch problematischer ist der kompetenzielle Aspekt. Die angestrebte Vollharmonisierung für den gesamten europäischen Binnenmarkt behindert die notwendige Modernisierung. Sie lässt, würde der Entwurf so in

Kraft gesetzt, bis zur nächsten Überarbeitung der Verordnung – und das bedeutet praktisch in den nächsten ein bis zwei Jahrzehnten – keine Fortschritte im Datenschutzrecht durch die Mitgliedstaaten zu. Angesichts der Schnelligkeit der technischen Entwicklung und der Vielfalt ihrer Anwendungen müssen jedoch Freiräume für gesetzgeberische Experimente in den Mitgliedstaaten offen gehalten werden.[36] Zwar lässt sich die Kommission in fast allen wichtigen Regelungen ermächtigen, die getroffenen Regelungen durch eigene Vorgaben zu konkretisieren. Dies führt aber zu einer Zentralisierung und verhindert den Wettbewerb der Mitgliedstaaten um neue Ideen und Konzepte. Außerdem ist die Europäische Kommission keine Institution, die auf große Erfahrung im Datenschutz zurückblicken kann, und ist alles andere als politisch unabhängig – was sie jedoch selbst von allen Datenschutzbehörden in Europa fordert. Der Entwurf darf daher so nicht beschlossen werden, sondern bedarf einer umfassenden Diskussion.

Anmerkungen

1 S. näher Alexander Roßnagel, Datenschutz in einem informatisierten Alltag, 2007, im Internet unter http://library.fes.de/pdf-files/stabsabteilung/04548.pdf.

2 Jörg Tauss/Cem Özdemir, Umfassende Modernisierung des Datenschutzrechtes in zwei Stufen, in: Recht der Datenverarbeitung (RDV) 2000, S. 143.

3 Alexander Roßnagel/Andreas Pfitzmann/Hansjürgen Garstka, Modernisierung des Datenschutzrechts, Gutachten für das BMI, 2001.

4 S. beispielsweise Volker Ahrend u. a., Modernisierung des Datenschutzes?, in: Datenschutz und Datensicherheit (DuD) 2003, S. 433; Johann Bizer, Ziele und Elemente der Modernisierung des Datenschutzrechts, in: DuD 2001, S. 274; ders., Strukturplan modernes Datenschutzrecht, in: DuD 2004, S. 6; Alexander Roßnagel, Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, in: Multimedia und Recht (MMR) 2005, S. 71; ders., Die Zukunft informationeller Selbstbestimmung: Datenschutz ins Grundgesetz und Modernisierung des Datenschutzkonzepts, in: Kritische Justiz (Hrsg.), Verfassungsrecht und gesellschaftliche Realität, Beiheft 1/2009, S. 99; Thilo Weichert, Dauerbrenner BDSG-Novellierung, in: DuD 2010, S. 7; Jürgen Kühling/Simon Bohnen, Zur Zukunft des Datenschutzrechts – Nach der Reform ist vor der Reform, in: Juristenzeitung 2010, S. 600; 32. Sitzung des BT-Innenausschusses am 5.3.2007, Protokoll 16/32; BT-Drs. 16/4882.

5 S. beispielsweise Koalitionsvereinbarung vom 16.10.2002, S. 55; Koalitionsvereinbarung vom 11.11.2005, S. 109; Koalitionsvereinbarung vom 26.10.2009, S. 105 f.

6 S. auch die Stellungnahme des Bundesrats, BT-Drs. 16/12011, S. 48.

7 S. zum Beispiel Thomas Hoeren, Das Telemediengesetz, in: Neue Juristische Wochenschrift (NJW) 2007, S. 801; Alexander Roßnagel, Das Telemediengesetz – Neuordnung für Informations- und Kommunikationsdienste, in: Neue Zeitschrift für Verwaltungsrecht 2007, S. 743.
8 Entwurf des Bundesinnenministeriums vom 7.9.2007.
9 S. hierzu Alexander Roßnagel, Datenschutzaudit, 2000; ders., Datenschutzaudit – ein modernes Steuerungsinstrument, in: Leon Hempel/Susanne Krasmann/Ulrich Bröckling (Hrsg.), Sichtbarkeitsregime – Überwachung, Sicherheit und Privatheit im 21. Jahrhundert, Leviathan Sonderheft 2010, S. 263 ff.
10 BGBl. I, S. 2254; BT-Drs. 16/10529; Alexander Roßnagel, Die Novellen zum Datenschutzrecht – *Scoring* und Adresshandel, in: NJW 2009, S. 2718; Jürgen Kühling/Simon Bohnen 2010 (s. Anm. 4).
11 BGBl. I, S. 2814; BT-Drs. 16/12011; Alexander Roßnagel 2009 (s. Anm. 10), S. 2719 ff.
12 Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Ein modernes Datenschutzrecht für das 21. Jahrhundert – Eckpunkte zur Modernisierung des Datenschutzrechts, 18.3.2010.
13 KOM (2012) 11; s. auch bereits Mitteilung der Kommission, Gesamtkonzept für den Datenschutz in der Europäischen Union, KOM(2010) 609.
14 Ansätze hierfür in Kommission 2010 (Anm. 13), S. 6.
15 Zu *Privacy Enhancing Technologies* (PET) s. Mitteilung der Kommission über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre, KOM(2007) 228; London Economics, Study on the economic benefits of privacy enhancing technologies (PET), im Internet unter http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf.
16 Zu *Privacy by Design* s. Kommission 2010 (Anm. 13), 14 und Mitteilung »Eine Digitale Agenda für Europa«, KOM(2010) 245, S. 19 ff.
17 S. ausführlich Roßnagel 2007 (Anm. 1), S. 75 ff.
18 S. ausführlich Roßnagel 2007 (Anm. 1), S. 175 ff.
19 S. Roßnagel/Pfitzmann/Garstka 2001 (Anm. 3), S. 70 ff.
20 Kommission 2010 (Anm. 13), S. 8; Konferenz 2010 (Anm. 12), S. 12.
21 S. hierzu näher Alexander Roßnagel, Das Gebot der Datenvermeidung und -sparsamkeit, in: Martin Eifert/Wolfgang Hoffmann-Riem (Hrsg.), Innovation, Recht, öffentliche Kommunikation, Berlin 2011.
22 S. Hendrik Skistims/Christian Voigtmann/Klaus David/Alexander Roßnagel, Datenschutzgerechte Gestaltung von kontextvorhersagenden Algorithmen, DuD 2012, 31; grundsätzlich Matthias Schwenke, Datenschutz und Individualisierung – Rechtskonformer Umgang mit personenbezogenen Daten im Kontext der Eigen- und Fremdindividualisierung, Berlin 2006.
23 Ein solches »Recht auf Vergessen« sieht Artikel 17 des Entwurfs einer Europäischen Datenschutzverordnung (s. Anm. 13) vor. Darin heißt es: »Die betroffene Person hat das Recht, von dem für die Verarbeitung Verantwortlichen die

Löschung von sie betreffenden personenbezogenen Daten und die Unterlassung jeglicher weiteren Verbreitung dieser Daten zu verlangen (…).«

24 S. näher Roßnagel/Pfitzmann/Garstka 2001 (Anm. 3), S. 68 ff., 113 ff.; ebenso Konferenz 2010 (Anm. 12), S. 10 f.

25 Marit Köhntopp/Burckhard Nedden, Datenschutz und »Privacy Enhancing Technologies«, in: Alexander Roßnagel (Hrsg.), Allianz von Medienrecht und Informationstechnik?, Baden-Baden 2001, S. 55 ff. und 67 ff.

26 *Platform for Privacy Preferences* – s. Näheres im Intenet unter http://www.w3c.org/P3P.

27 S. beispielsweise für RFID Jürgen Müller/Matthias Handy, RFID und Datenschutzrecht, in: DuD 2004, S. 629.

28 S. Roßnagel/Pfitzmann/Garstka 2001 (Anm. 3), S. 102.

29 S. Alexander Roßnagel/Philip Scholz, Datenschutz durch Anonymität und Pseudonymität, in: Multimedia und Recht 2000, S. 728 ff.; so kann auch Kommission 2010 (Anm. 13), S. 6 verstanden werden.

30 S. auch Konferenz 2010 (Anm. 12), S. 17 f.; Kommission 2010 (Anm. 13), S. 14.

31 S. näher Roßnagel/Pfitzmann/Garstka 2001 (Anm. 3), S. 143 ff.; s. auch Konferenz (Anm. 12), S. 6.

32 Alexander Roßnagel, Datenschutzaudit, in: ders. (Hrsg.), Handbuch Datenschutzrecht, 2003, S. 439 ff.; ders. (Anm. 9).

33 S. Roßnagel/Pfitzmann/Garstka 2001 (Anm. 3), S. 153 ff.; Kommission 2010 (Anm. 13), S. 14.

34 S. Roßnagel/Pfitzmann/Garstka 2001 (Anm. 3), S. 203 ff.; Kommission 2010 (Anm. 13), S. 10.

35 So noch die Aufgabenstellung für das Gutachten von Roßnagel/Pfitzmann/Garstka 2001 (Anm. 3).

36 S. für das Umweltrecht Alexander Roßnagel, Lernfähiges Europarecht – am Beispiel des europäischen Umweltrechts, in: Neue Zeitschrift für Verwaltungsrecht 1997, S. 122 ff.

Thilo Weichert

Codex Digitalis Universalis

Wir befinden uns heute technikbedingt an der Schwelle einer neuen Phase gesellschaftlicher Entwicklung. Nach dem Erwerb der Sprache als Kommunikationsmittel, der Schrift als Mittel der Informations- und Ideenkonservierung und des Buchdrucks als Instrument für die Verbreitung der Ideen haben wir heute mit dem Internet das Werkzeug, Informationen und Ideen weltweit und ohne Zeitverzug zu kommunizieren, zu bearbeiten und hierüber einen Dialog zu führen. Diese neue Phase nennen wir Informationsgesellschaft. Sie löst die Industriegesellschaft des 19. und 20. Jahrhunderts ab.

Die Industriegesellschaft brachte Chancen und Risiken mit sich – etwa die Möglichkeiten allgemeinen Wohlstands und die Risiken der Zerstörung unserer Umwelt und unserer Lebensgrundlagen. Die Informationsgesellschaft ermöglicht, unser Wissen zur Bewältigung der mit der Industriegesellschaft geschaffenen Probleme und Gefahren optimal zu nutzen. Tatsächlich schafft die globale elektronische Kommunikation auch die Voraussetzungen zur Information über und zur Eindämmung von Hungersnöten, Naturkatastrophen und Kriegen. Schon heute kann die Informationstechnologie sinnvoll genutzt werden, um Menschenleben zu retten, etwa wenn mit Sensoren auf dem Land bzw. im Meer sowie Satellitenüberwachung ein Erdbeben- und Tsunami-Frühwarnsystem eingerichtet wird, das in Echtzeit auf eine drohende Katastrophe hinweisen kann.

Zugleich wird die Informationstechnologie zu einer wichtigen Grundlage unserer demokratischen Meinungsbildung und der Inanspruchnahme von Freiheitsrechten. Beim sogenannten Arabischen Frühling im Jahr 2011 wurde moderne Informationstechnologie erfolgreich genutzt, um im Kampf gegen Diktaturen Mitstreiter zu gewinnen und politische Ziele umzusetzen.

Die Bedeutung elektronischer Medien für die Herstellung demokratischer Transparenz und zum Finden demokratischer Entscheidungen ist evident. Doch auch unsere klassischen Freiheitsrechte – vom Schutz der freien Berufsausübung, dem Schutz des Eigentums oder der Wohnung bis zum Schutz von Familie und Religionsausübung – haben inzwischen eine informationstechnische und damit eine digitale Dimension erlangt.

1 Die digitale Bedrohung von Freiheitsrechten

Die globale Informationsgesellschaft hat verschiedene Auswirkungen. Autoritäre Regierungen können mit Hilfe der Informationstechnik elektronische Kommunikation und deren Inhalte ihrer Bürgerinnen und Bürger scannen, speichern, auswerten, kontrollieren und unterbinden. Der oft ungeschützte Austausch von Regierungsgegnern im oben erwähnten »Arabischen Frühling« über Dienste des → Web 2.0 führte oft dazu, dass dieser von Regierungsstellen mitgelesen werden konnte und die Betroffenen eingeschüchtert, verhaftet und gefoltert wurden. Diktaturen importieren für diese Zwecke oft Überwachungstechnik aus westlichen demokratischen Staaten, zum Beispiel auch aus der Bundesrepublik Deutschland.

Globale Informationsgesellschaft bedeutet aber auch, dass private Unternehmen (beispielsweise *Google* oder *Facebook*) die Nutzungsdaten von hunderten von Millionen Internetnutzerinnen und -nutzern weltweit praktisch unbeschränkt speichern und auswerten können, und dass diese Unternehmen unter Umständen mehr Wissen und Macht über Menschen haben als viele Staaten. Wirtschaftsunternehmen können mit solchen Daten Menschen gefügig machen, ohne dass jene dies überhaupt merken. In den USA werden Angaben aus → sozialen Netzwerken (zum Beispiel *Facebook*) automatisiert ausgewertet und mit Bewertungen, sogenannten *Scores*, zusammengeführt, die dann bei der Durchführung von Werbemaßnahmen, bei Bewertung der Bonität oder bei Einstellungsverfahren herangezogen werden.

Eingriffe in Freiheitsrechte sind oft unsichtbar

Die Instrumente hierfür sind für viele noch Fremdwörter: → *Tracking*, → *Scoring*, → *Profiling*, → *Identity Theft*. Dabei werden mit der Datenverarbeitung Menschen überwacht, diskriminiert und manipuliert, mit anderen Worten: Menschen werden durch Informationstechnik ihrer Freiheiten beraubt. In diesen Fällen wird keine Gewalt angewandt und es fließt kein Blut. → Vorratsdatenspeicherungen, *Online*-Durchsuchungen (siehe dazu auch den Beitrag von Petri in diesem Band, S. 115 ff.) und Kundendatenanalysen (siehe dazu auch die Beiträge von Lüke, S. 154 ff. und Billen, S. 172 ff. in diesem Band) kann man zwar nicht sehen, doch sie können unser Leben stark beeinflussen. Die folgenden Beispiele sollen dies verdeutlichen:

- In Wohnungen muss die Polizei heute nicht mehr mit Gewalt eindringen; dies ist auch mit sogenannten → Lausch- und Spähangriffen möglich.
- Für das Plündern des Bankkontos sind nur einige wenige Kontodaten nötig.

- Mit sogenannten elektronischen Fußfesseln können Menschen unsichtbar ihrer Freiheit beraubt werden.
- Um eine Person politischer Verfolgung auszusetzen, genügt die Datenspeicherung als angeblicher Terrorist. Eine solche Datenspeicherung kann ebenso zu einem Anfangsverdacht bei Polizeikontrollen führen wie zur Ablehnung in Bewerbungsverfahren im öffentlichen Dienst.

2 Wie können Grundrechte zukünftig geschützt werden?

Als rechtliche Antwort auf die technische Entwicklung wurde Ende des 19. Jahrhunderts mit der zunehmenden Nutzung der Fotografie der Schutz der Privatsphäre und der Schutz des eigenen Bildes entwickelt. Wegen möglicher elektronischer Tonaufnahmen musste das gesprochene Wort rechtlich geschützt werden. Auf die elektronische Datenverarbeitung reagierte das Bundesverfassungsgericht im Jahr 1983 mit der Ableitung des neuen Grundrechtes auf informationelle Selbstbestimmung (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.). Der Umstand, dass wir für unsere persönlichen Verrichtungen immer mehr die Unterstützung elektronischer Geräte benötigen und dass diese heimlich ausspioniert und sabotiert werden können, veranlasste das Bundesverfassungsgericht im Jahr 2008 erneut, ein neues Grundrecht zu schaffen: So wie unser räumliches Umfeld der Wohnung oder unser soziales Umfeld der Familie grundrechtlich geschützt sind, sprach uns das Gericht ein Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme zu.

Eine zentrale politische Frage der Zukunft wird sein, wie diese neuen digitalen Grundrechte geschützt werden können. Mit welchen Instrumenten können die grundlegenden menschlichen Bedürfnisse im »virtuellen Raum« befriedigt und verteidigt werden – einem Raum, der sich durch Globalität, Intransparenz und Unkörperlichkeit charakterisieren lässt.

Durch die Globalität stellen sich im Bereich des Datenschutzes im Wesentlichen zwei grundlegende Fragen (siehe auch den Beitrag von Körner in diesem Band, S. 426 ff.): Welches nationale oder internationale Recht ist jeweils anwendbar? Mit welchen staatlichen oder überstaatlichen Instrumenten kann das Recht auf informationelle Selbstbestimmung umgesetzt werden?

Die mangelnde Transparenz und Körperlichkeit ist eine neue Herausforderung: Die virtuelle Welt ist nicht mehr materiell greifbar. Eine Folge ist, dass das Ungleichgewicht zwischen Kommunikationspartnern – insbesondere zwischen denen, die die Technik beherrschen und denen, die sie nur benutzen – eklatant zunimmt. Dieses Ungleichgewicht verstärkt

sich dort, wo global organisierte Unternehmen mit einer möglicherweise monopolartigen Wettbewerbsposition oder Staaten mit einer informationstechnischen Dominanz tätig sind. Diese Ungleichgewichte lassen sich durch erhöhte Transparenz oder ein Aufbrechen der Monopole aufheben.

Die globale Informationsgesellschaft provoziert also neue Probleme und löst damit neuen Regelungsbedarf aus (siehe auch den Beitrag von Albers in diesem Band, S. 102 ff.). Dabei lassen sich die alten, für das analoge Leben geschaffenen nationalstaatlichen Instrumente nicht einfach übertragen. Es bedarf neuer Instrumente, es bedarf eines modernen *Codex Digitalis Universalis*.

3 Gestaltung neuer Normen in supranationalem Kontext

Da Staatlichkeit im universellen Netz nicht mehr die zentrale Rolle spielt, können nationale Regelungen nicht mehr – wie in der körperlichen Welt – der zentrale Regelungsansatz bleiben. Europäische, internationale, ja globale Normen sind nötig und inzwischen schon fast überfällig. Dessen ungeachtet müssen nationale Staaten für ihre Bürgerinnen und Bürger grundrechtliche Schutzpflichten wahrnehmen: Gerade wegen des internationalen Charakters der Informationstechnik muss der Staat den Menschen rechtliche, technische, und organisatorische Instrumente bereit stellen, wie sie sich in der globalen Welt selbst schützen und ihre Rechte durchsetzen können.

Regulierung ist nicht mehr allein mit konditional aufgebauten Ge- und Verbotsnormen möglich. Sie setzt vielmehr einen Instrumentenmix voraus, der neben der staatlichen Verwaltung den Markt, die Technik, die Kultur der Kommunikation und Informationsverarbeitung und damit auch das Bewusstsein der einzelnen Menschen erreicht.

Europäisches Datenschutzrecht und seine Bedeutung für einen *Codex Digitalis Universalis*

In vieler Hinsicht ist das europäische Datenschutzrecht wegweisend. Es reagierte bereits 1995 mit der europäischen Datenschutzrichtlinie auf die grenzüberschreitenden Gegebenheiten der Informationstechnik und legte einen möglichst einheitlichen hohen Schutzstandard fest. Dieser Standard basiert nicht allein auf staatlicher Aufsicht, sondern auch auf Kooperation und Koordination, auf regulierter Selbstregulierung der handelnden Stellen, auf Verträgen und Verhaltensregeln. Mit den globalen Netzen ist auch diese

europäische Welt nicht mehr sicher genug. Doch die europäischen Datenschutzstandards strahlen über die Europäische Union (EU) hinaus, beispielsweise indem informationstechnische Handelshemmnisse abgebaut werden, wenn in den Ländern der Kommunikationspartner entsprechende Datenschutzstandards nachgewiesen werden können. Einen gravierenden Sündenfall beging die EU aber im Verhältnis zu den USA, indem sie angesichts der schieren informationstechnischen Macht dieses Landes etwa in einem → *Safe-Harbor*-Abkommen oder in sicherheitsbehördlichen Kooperationsvereinbarungen auf einen vergleichbaren Standard verzichtet mit der Folge, dass bestimmte US-Unternehmen sich europäische Daten beschaffen, ohne dass sie auch nur ansatzweise Datenschutzgarantien vorweisen können.

Gerade das Beispiel der USA zeigt, dass eine ethno- oder kulturzentristische Vorgehensweise des Aufdrängens des eigenen Wertekanons – wie in anderen Bereichen auch – bei der Informationstechnik keinen Erfolg verspricht. Letztlich lässt sich die Notwendigkeit des Werte- und Normenwandels nicht von Außen auferlegen, sondern nur durch innere Einsicht entwickeln – möglicherweise gefördert und unterstützt von außen. Zweifellos gibt es in den USA eine agile Bürgerrechtsbewegung, die digitalen Grundrechtsschutz aus eigenem Antrieb einfordert. Diese Bestrebungen in den USA können durch Dialog und ökonomische Anreize aus Europa gefördert werden. So verlangt der europäische Markt von den in Europa agierenden US-Anbietern Änderungen ihres Angebotes vor Ort, so geschehen etwa bei den Internet-Straßenansichten von → *Google Street View*. Derartigem Zwang sind positive Anreize vorzuziehen, wie sie beispielsweise mit Unterstützung der Europäischen Kommission durch das Europäische Datenschutz-Gütesiegel (*European Privacy Seal*) gegeben werden (siehe auch den Beitrag von Bock in diesem Band, S. 310 ff.).

Globaler Datenschutz braucht allgemeingültige Standards

Ein weiterer Ansatz, bei dem staatliche Regulierung nur noch eine flankierende Rolle spielt, ist die technische Standardisierung, für die über internationale Organisationen wie die *International Standardisation Organisation* (→ ISO) funktionsfähige Strukturen bestehen. Hierbei kann über die Notwendigkeit der weltweiten Kompatibilität von globaler Netztechnik gegenseitiger Respekt für grundlegende Werte und die Notwendigkeit der Grundrechtsverträglichkeit vermittelt werden, der dann möglicherweise standardmäßig festgelegt und schließlich realisiert wird. Die Folge ist, dass die Anbieter im Interesse der Wahrung ihrer globalen Marktchancen von Anfang an diese Standards in ihre Produkte einbauen.

Dringender Handlungsbedarf zur Wahrung digitaler Grundfreiheiten

So sehr auch die Instrumente der globalen – informationstechnisch geförderten – Diskussion und des Marktes zur Durchsetzung digitaler Grundfreiheiten genutzt werden können und müssen – ohne eine materiellrechtliche Fundierung und Flankierung wird dieser Prozess unvollständig bleiben. Angesichts der verheerenden Auswirkungen des zweiten Weltkrieges war die Weltgemeinschaft 1949 bereit, sich auf die Allgemeine Erklärung der Menschenrechte zu verständigen. Es ist zu hoffen, dass es keiner auch nur ansatzweise ähnlichen Katastrophe bedarf, um den Staaten mit ihren verschiedenen Kulturen, Religionen und Gesellschaftsmodellen die Notwendigkeit eines weltweiten digitalen Menschenrechtskatalogs zu vermitteln. Doch wird es ohne Schmerzen und Verluste nicht möglich sein, global zu dieser Einsicht zu kommen. Der Handlungsdruck besteht schon heute und wird durch »digitale Erdbeben« unterschiedlichen Ausmaßes erhöht. Eine dieser Erschütterungen erfasste Estland im April 2007, als ein konzentrierter Angriff auf die informationstechnische Infrastruktur des Landes dazu führte, dass die elektronischen Kommunikationsnetze Estlands fast vollständig zusammenbrachen. Angriffe auf lebenswichtige Einrichtungen, die heute sämtlich mit Informationstechnik gesteuert werden, können nicht nur zu digitalen, sondern auch zu sehr körperlichen Katastrophen führen. Die Möglichkeit eines *Cyber Warfare*, eines digitalen Krieges, sollte genügen, solchen Menschenrechtsverletzungen diplomatisch und rechtlich schon vor deren Verwirklichung vorzubeugen.

Inhalt einer digitalen Menschenrechtscharta

Was kann und sollte in einer digitalen Menschenrechtscharta festgehalten werden? Es geht dabei einerseits um die Sicherung der individuellen und gesellschaftlichen Kommunikation, andererseits um den Schutz informationeller Selbstbestimmung. Ein Aspekt der Gefährdung informationeller Selbstbestimmung ist, dass mit Hilfe der Informationstechnik tief in die genetische Festlegung der Menschen Einblick genommen und hierüber verfügt werden kann (siehe auch den Beitrag von Bartmann in diesem Band, S. 178 ff.). Die Ideen der digitalen Privatsphäre und der digitalen Freiheiten, so fremd diese vielen Kulturen auch noch zu sein scheinen, müssen Bestandteil einer globalen Charta sein. Die Verzahnung der digitalen Rechte mit den analogen Menschenrechten muss im Blick bleiben. Ein Ziel muss es aber auch sein, das gesellschaftliche und demokratische Potenzial digitaler Freiheitsrechte für eine gerechtere und humane globale Informationsgesellschaft freizusetzen.

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*.

Martin Rost

Die Schutzziele des Datenschutzes

Bis Mitte der 1990er Jahre konzentrierten sich Aktivitäten der Datenschutzbeauftragten darauf, die Rechtsgrundlagen des Datenschutzes zu erarbeiten und deren Beachtung zu prüfen. Das führte dazu, dass Datenschutzbeauftragte zunehmend besser begründen konnten, welche Datenverarbeitung datenschutzrechtlich nicht korrekt erfolgt. Die Datenschutzbeauftragten haben seitdem einige Erfolge bei der rechtskonformen Gestaltung der Informationsverarbeitung - insbesondere im Bereich der öffentlichen Verwaltung - vorzuweisen. Allerdings hatten sie bislang immer das Problem, die aus Datenschutzsicht auch durchaus positiven Eigenschaften von Informationsverarbeitungssystemen zu benennen. Hinzu kam, dass die massenhafte Verbreitung und Nutzung der modernen Informationstechnik – allen voran das Internet – seit 1995 offenbarte, dass die globale Technikentwicklung nicht den Gesetzen von Nationalstaaten folgt. Das aktuell gültige Bundesdatenschutzgesetz (BDSG) wurde in seinen wesentlichen Zügen in den 1970er Jahren entwickelt und hat auf das Internet bis heute nicht angemessen reagiert (siehe den Beitrag von Roßnagel in diesem Band, S. 331 ff.).

Mit dem Gewahrwerden der datenschutzrechtlichen Risiken der an das Internet angeschlossenen PCs in den Privathaushalten und Organisationen entstand die Idee, die Informationstechnik gezielt für den Schutz Betroffener zu nutzen. So forderten Datenschützer, dass

- Daten so früh wie möglich zu löschen sind und über den Löschvorgang ein Nachweis erbracht wird.
- die Aktivitäten von Administratoren, die grundsätzlich in der Lage sind, auf den von ihnen betreuten Servern alles einzusehen und zu verändern, durch den Einsatz von Protokollierungstechniken beweisfest protokolliert werden. Missbrauch lässt sich so zwar nicht verhindern, aber im Nachhinein zumindest aufklären.
- über das Internet Daten nur noch verschlüsselt und mit digitaler Unterschrift versehen verschickt werden.

In Bezug auf die Kommunikation von Personen mit Behörden und Unternehmen sind einige dieser Anforderungen im Alltag der Webnutzung inzwischen erfüllt. Insbesondere gewann die Software *PGP (Pretty Good Privacy)* - mittlerweile ein Klassiker unter den Verschlüsselungsprogram-

men - für das Verschlüsseln und Signieren von E-Mails Bedeutung (siehe dazu auch den Beitrag von Thomsen in diesem Band, S. 381 ff.), weil die Nutzenden damit selbst die Kontrolle über das Management der Kommunikation innehaben. Diese den Datenschutz verbessernden Techniken werden als *Privacy Enhancing Technologies (PET)*[1] bezeichnet. Eine der wesentlichen Ideen besteht darin, den Nutzenden Techniken an die Hand zu geben, damit sie die Kontrolle über ihre Daten und ihren Teil der Prozesse behalten können.

Mit dem Einzug solcher Techniken änderten sich die Perspektive und das Interventions-Repertoire der Datenschutzbeauftragten. Sie sehen sich seitdem vor die Aufgabe gestellt, die Datenverarbeitung von Behörden, Unternehmen und Forschungsinstituten nicht nur aus rechtlicher Sicht zu beurteilen und gegebenenfalls öffentlich in ihren Tätigkeitsberichten zu kritisieren sowie darüber hinaus politikwirksam über Pressemitteilungen zu skandalisieren, sondern auch konstruktive Vorschläge zur Verbesserung der Datenverarbeitung in Organisationen zu unterbreiten. Seit der Jahrtausendwende liegen außerdem Konzepte, Kriterienkataloge und Methoden zur Auditierung der Datenschutzeigenschaften von Systemen vor, die in Deutschland entwickelt und inzwischen mindestens europaweit im Einsatz sind. In solchen Audits arbeiten Datenschützer aktiv daran mit, datenschutzgerechte Lösungen zu entwickeln (siehe auch den Beitrag von Bock in diesem Band, S. 310 ff.).

Die Kriterien, an denen sich ein derartig praxisgerechter, ein aus der Sicht der Nutzenden und der Datenschutzaufsicht proaktiver Datenschutz orientiert, sind die *Neuen Schutzziele*, die bislang nicht explizit im BDSG enthalten sind.[2] In der Anlage zu § 9 BDSG sind bisher lediglich Maßnahmen zur Gewährleistung des technisch-organisatorischen Datenschutzes beschrieben (siehe auch den Beitrag von Martin in diesem Band, S. 390 ff.), die nach Auffassung der Konferenz der Datenschutzbeauftragten vom 18. März 2010 einer grundsätzlichen Reform bedürfen und durch die Definition elementarer Schutzziele zu ersetzen seien. Um welche Ziele es sich dabei handelt, was mit ihnen angestrebt wird und warum gerade die sechs genannten Schutzziele für den Datenschutz wichtig sind, ist nachfolgend das Thema.

1 Die elementaren Schutzziele des Datenschutzes

Das Konzept der Schutzziele besteht seit Ende der 1980er Jahre. Es spielte zunächst eine wesentliche Rolle bei der Herstellung von Datensicherheit für Informationstechnik.[3] Anfang 2008 formulierte das Bundesverfas-

sungsgericht unter Rückgriff auf zwei dieser Schutzziele das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme [4] (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.). Im Sommer 2009 wurde das Konzept der Schutzziele der Datensicherheit in ein umfassenderes Konzept der Schutzziele des Datenschutzes aufgenommen und spezifiziert.[5]

Zu den elementaren Schutzzielen des Datenschutzes zählen die drei »klassischen« Schutzziele der Datensicherheit: *Verfügbarkeit, Integrität und Vertraulichkeit*. Diese Schutzziele formulieren Anforderungen an einen sicheren Betrieb von informationstechnischen (IT-)Systemen insbesondere von Organisationen. Diese müssen ihre Informationstechnik (IT) vor Angreifern schützen, die als Hacker auf Prozesse und Daten zugreifen wollen. Datenschutz ist daher ohne Datensicherheit nicht möglich. Ein sicherer Betrieb von Behörden, Unternehmen und Forschungsinstituten liegt im Interesse von Bürgerinnen und Bürgern ebenso wie im Kunden-, Patienten- und Mandanteninteresse.

Datenschutz nimmt jedoch zusätzlich die Perspektive der betroffenen Personen gegenüber Organisationen ein. Aus einer systematischen Datenschutzsicht heraus gilt eine Organisation als Angreiferin auf die Interessen einer Person. Verwaltungen etwa hätten es am liebsten, wenn Bürgerinnen und Bürger selber wie Verwaltungen funktionierten und sich den Maßnahmen zur Sicherstellung der öffentlichen Ordnung kritiklos unterwürfen. Unternehmen wollen maximalen Profit erzielen und versuchen, durch Kundenbindungssysteme zu verhindern, dass Kundinnen und Kunden zur Konkurrenz abwandern. Bis zu den rechtsstaatlich gesetzten Grenzen sind diese Aktivitäten von Organisationen legitim, darüber hinaus aber nicht. Zusätzlich zu den Schutzzielen der Datensicherheit bedarf es deshalb weiterer, spezifischer Schutzziele aus der Sicht der betroffenen Personen, die den Respekt dieser rechtsstaatlichen Grenzen praktisch umsetzen. Diese drei spezifischen Schutzziele des Datenschutzes sind *Transparenz*, *Intervenierbarkeit* und *Nichtverkettbarkeit*. Was darunter zu verstehen ist, wird nachfolgend im Anschluss an die »klassischen« Schutzziele dargelegt.

Verfügbarkeit

Das Schutzziel Verfügbarkeit bezeichnet die Anforderung, dass ein gesicherter Zugriff auf Informationen innerhalb festgelegter Zeit bestehen muss. Hiernach sollen also Informationen zeitgerecht zur Verfügung stehen und ordnungsgemäß verwendet werden können. Umgesetzt wird dieses Schutzziel bei Daten beispielsweise dadurch, dass Sicherheitskopien

angefertigt werden. Verfügbarkeit eines Systems bedeutet, dass bei einem Ausfall ein anderes System ersatzweise einspringen kann, bevorzugt ohne dass die Nutzenden von diesem Ersatz etwas bemerken. Organisatorisch lässt sich dieses Ziel umsetzen, indem man beispielsweise Reparaturstrategien einrichtet oder indem für ausfallende Mitarbeiterinnen und Mitarbeiter Vertretungsregeln bestehen.

Integrität

Das Schutzziel Integrität bezeichnet die Anforderung, dass ein System ausschließlich seine zweckbestimmte Funktion verlässlich und erwartungsgemäß erfüllt. Etwaige Nebenwirkungen müssen dabei möglichst ausgeschlossen und verbleibende Risiken berücksichtigt sein. Daten müssen während der Verarbeitung unversehrt, vollständig und aktuell bleiben. Umgesetzt wird dieses Schutzziel dadurch, dass von gespeicherten oder versendeten Daten Prüfsummen – sogenannte → *Hash*werte – vor und nach einer Aktion erzeugt und miteinander verglichen werden. Wenn die Prüfsummen nach einem Vergleich übereinstimmen, darf man sichergehen, dass die Daten in der Zwischenzeit nicht verändert wurden. Die Integrität technischer oder organisatorischer Prozesse und Systeme überprüft man dadurch, dass man die Ist-Werte eines Prozesses misst und diese mit den vorher festgelegten Soll-Werten eines Prozesses vergleicht. Wenn die Ist-Werte innerhalb der oberen und unteren Soll-Werte liegen, funktioniert ein Prozess so, wie er funktionieren soll.

Vertraulichkeit

Das Schutzziel Vertraulichkeit bezeichnet die Anforderung, dass nicht zuständige, unbeteiligte Dritte keine Möglichkeit haben, von Daten unbefugt Kenntnis zu bekommen oder ein System einzusehen und Betroffene identifizieren zu können. Umgesetzt wird dieses Schutzziel in Bezug auf Daten durch Verschlüsselung von gespeicherten oder transferierten Daten. In Bezug auf Prozesse und IT-Systeme sorgt vor allen Dingen eine Abschottung von Räumen oder Netzbereichen voneinander dafür, dass niemand unerlaubt Zugriff auf andere Prozesse und Systeme nehmen kann.

Transparenz

Das Schutzziel Transparenz bezeichnet die Anforderung, dass in einem unterschiedlichen Maße sowohl Betroffene als auch Betreiber von Systemen

sowie zuständige Kontrollinstanzen erkennen können, welche Daten für welchen Zweck erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wem die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung gehören. Der Eigentümer von Daten, Prozessen oder Systemen ist verantwortlich für die korrekte Datenverarbeitung. Durch Transparenz der gesamten Datenverarbeitung werden oftmals Regelungslücken deutlich. Transparenz ist auch für die Beobachtung und Steuerung von Daten, Prozessen und Systemen von ihrer Entstehung bis zu ihrer Löschung erforderlich als Voraussetzung dafür, dass eine Datenverarbeitung rechtskonform betrieben und in die von Betroffenen eingewilligt werden kann. Umgesetzt wird dieses Schutzziel durch das weitgehend automatisierte Kontrollieren von Systemen durch → *Monitoring*-Systeme, durch Protokollierungen sowie durch die Dokumentation der Daten, der Datenflüsse und der gesamten technischen und organisatorischen Systeme und Prozesse.

Intervenierbarkeit

Das Schutzziel Intervenierbarkeit bezeichnet die Anforderung, dass sowohl Betroffene als auch Betreiber von Systemen jederzeit in der Lage sind, die Datenverarbeitung – vom Erheben bis zum Löschen von Daten – ändern zu können. Schon bei der Gestaltung eines neuen Datenverarbeitungsverfahrens muss für die Umsetzung dieses Schutzes gesorgt werden. Umgesetzt wird dieses Schutzziel, indem für Betroffene und Betreiber an Systemen Vorrichtungen installiert sind, mit denen Systeme verändert und gestoppt werden können. Eine solche technische Vorrichtung, die im Wesentlichen mit der Funktionalität eines An-/Aus-Knopfs vergleichbar ist, entspricht auf der rechtlichen Ebene der Einwilligung, die erteilt oder verweigert werden kann.

Nichtverkettbarkeit

Das Schutzziel Nichtverkettbarkeit bezeichnet die Anforderung, für Prozesse und Systeme sicherzustellen, dass deren Daten nur für den Zweck verarbeitet und ausgewertet werden, für den sie erhoben werden. Zu bedenken ist, dass generell große Datenbestände Begehrlichkeiten mit ganz anderen Interessen an diesen Daten wecken können. Dies lässt sich mit dem Schlagwort → Vorratsdatenspeicherung kennzeichnen. Umgesetzt wird dieses Schutzziel bei personenbezogenen Daten durch die Begründung der Erforderlichkeit von Daten, durch Datensparsamkeit sowie die Nutzung von

Anonymisierungsservern oder →Pseudonymen, wie sie von nutzerkontrollierten Identitätsmanagement-Applikationen unterstützt werden.[6] Es empfiehlt sich, System(-teile) voneinander zu separieren, damit sich beispielsweise Fehler in einem System nicht in einem anderen System fortpflanzen (Funktion einer Brandmauer). Die Nichtverkettbarkeit ist der technische Ausdruck der Anforderung an Zweckbindung und Zwecktrennungen, die als Funktionstrennungen einen wesentlichen Mechanismus zur Umsetzung von *Checks & Balances* – der informationellen Gewaltenteilung in einem modernen Rechtsstaat – darstellen.[7]

Die Funktion der Schutzziele besteht darin, eine vertrauenswürdige Beziehung zwischen einer Organisation – gleichgültig ob es sich hierbei um eine öffentliche Verwaltung, ein privates Unternehmen, ein Forschungsinstitut oder auch eine Arztpraxis handelt – und einer Person zustande kommen zu lassen. Eine vertrauenswürdige Beziehung ist regelmäßig für alle Beteiligten besonderes effektiv. Die Beachtung der Schutzziele und deren Umsetzung durch Schutzmaßnahmen tragen dazu bei, dass Organisationen nachweisen können, dass sie ihre Prozesse und Systeme beherrschen und dabei an Fairness orientiert sind, weil sie sich an die Regeln halten.

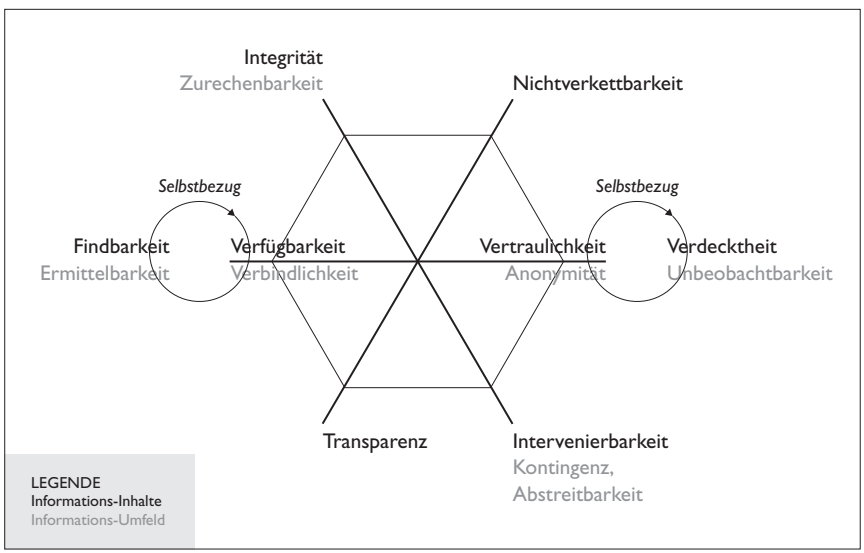
2 Warum gerade diese Schutzziele?

Datenschutz nimmt die Kommunikationsbeziehungen und die Informationsverarbeitung von staatlichen Verwaltungen sowie Bürgerinnen und Bürgern, von Unternehmen sowie Kundinnen und Kunden, von Instituten und Patienten, Mandanten, Klienten etc. kritisch in den Blick. Anhand der Vorgaben der Datenschutzgesetze wird überprüft, ob diese Beziehungen fair gestaltet sind. So sollen die Bürgerinnen und Bürger in einem Rechtsstaat in der Lage sein, sich auch gegen die notorisch mächtigeren Organisationen wehren zu können. Grundrechte gelten vor allem als Abwehrrechte der Bürgerinnen und Bürger gegen den Staat. Wie müssen nun die IT-Systeme der Organisationen und gesellschaftsweit genutzte Infrastrukturtechniken ausgelegt sein, damit niemand – weder Organisationen noch Personen – technisch bevor- oder benachteiligt sind? Die Lösung besteht darin, dass man verallgemeinerungsfähige, vernünftige (Schutz-)Ziele formuliert, mit deren Umsetzung diese Infrastrukturen dann allseits vertrauenswürdig genutzt werden können.

In einer Gesamtbetrachtung der Schutzziele stellt man fest, dass diese in einem Spannungsverhältnis zueinander stehen. Dabei gibt es drei Schutz-

ziel-Paare, die besonders herauszuheben sind, weil jeweils zwei Schutzziele zueinander sowohl komplementär als auch widersprüchlich (»dual«) sind. Werden beispielsweise Verfügbarkeit und Vertraulichkeit gemeinsam betrachtet, stellt man fest, dass beide zusammen nicht im gleichen Maße zur gleichen Zeit realisiert werden können. Man kann von ein und demselben Datum nicht fordern, dass es für einen Empfänger zugleich verfügbar als auch ihm gegenüber vertraulich sein soll. Auch das Verhältnis von Integrität und Intervenierbarkeit ist dual. Die Integrität eines Datums oder eines Prozesses oder Systems soll einerseits kontrolliert, korrekt und dauerhaft stabil gegen mögliche Störungen von außen funktionieren; das Funktionieren muss andererseits aber auch durchbrochen werden können, weil dies eine wesentliche Eigenschaft ist, um Daten und Systeme verwalten und ändern zu können. Und auch Transparenz und Nichtverkettbarkeit stehen dual zueinander: Ein Datum, das transparent ist, kann grundsätzlich mit anderen Daten verkettet werden. Erst eine Grenze verhindert, dass Daten miteinander verarbeitet werden, und sorgt insofern für Intransparenz auf der anderen Seite einer Grenze (Prinzip Burgtor).

Abb: 1: Die Systematik der Datenschutzziele



Quelle: Martin Rost/Kirsten Bock, *Privacy by Design* und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen, in: Datenschutz und Datensicherheit (DuD), 35. Jahrgang, Heft 1/Januar 2011, S. 32.

Aus den sechs elementaren Schutzzielen lassen sich weitere ableiten. Wenn man einerseits Schutzziele für Nachrichteninhalte (sowie Prozesse und Systeme) und andererseits für den Kontext von Inhalten unterscheidet, sowie methodisch Selbstbezüge zulässt – indem man beispielsweise auch für Vertraulichkeit noch Vertraulichkeit sichert –, dann ergibt sich eine Systematik der wesentlichen Schutzziele, die in Abbildung 1 dargestellt ist.

Die Spannungsverhältnisse der Schutzziele untereinander müssen bei der Beurteilung einer Datenverarbeitung durch Abwägung zunächst in ein rechtlich ausgewogenes Verhältnis zueinander gebracht werden. Ist diese Abwägung erfolgt und ein Lösungsraum gefunden, dann sind anschließend die technischen und prozessualen Maßnahmen zu treffen, mit denen die Schutzziele umsetzbar sind.

3 *Facebook* und die Schutzziele – ein Anwendungsbeispiel

Zum Schluss soll die Nützlichkeit der elementaren sechs Schutzziele zur Analyse der Angebote von *Facebook* aus Sicht des Datenschutzes dargestellt werden. Wie erwähnt, muss aus Datenschutzsicht methodisch vornehmlich die Organisation – hier *Facebook* – als mögliche Angreiferin auf die Schutzinteressen einer Person gelten.

Facebook macht gegenüber seinen Nutzenden keine Zusagen darüber, wie verlässlich der Dienst zur Verfügung steht. Dass *Facebook* auch morgen noch zugänglich sein wird, ist zwar sehr wahrscheinlich, denn das →soziale Netzwerk will weiterhin Geld mit der Auswertung personenbezogener Daten der Nutzenden verdienen. Aber diese haben nichts in der Hand, wenn sie morgen nicht mehr in das Netzwerk hineinkommen. Macht *Facebook* Zusagen darüber, dass die Nutzerdaten gegen Verfälschungen gesichert sind? Dass also niemandem ein Nutzerprofil untergeschoben werden kann (was etwa den Betroffenen bei polizeilichen Ermittlungen in große Schwierigkeiten bringen könnte)? Bei *Facebook* ist es ganz leicht, andere Teilnehmerinnen und Teilnehmer in Gruppen mit problematischen Inhalten hineinzuziehen, von deren Existenz und Mitgliedschaft diese gar nichts wissen. *Facebook* legt zudem Nutzenden schon bei der Anmeldung nahe, das Passwort eines *E-Mail-Accounts* zu verraten, damit die Firma daraus neue Kontaktdaten gewinnen kann. *Facebook* weist in seinen Datenschutzerklärungen darauf hin, dass es die Nachrichten zwischen den Nutzenden untereinander mitliest, es gilt also kein Briefgeheimnis. Dass eine bei *Facebook* registrierte Person die Daten ihres *Accounts* nicht löschen oder korrigieren kann, ist inzwischen hinlänglich bekannt. Auch beim Löschen

eines *Facebook-Accounts* werden dessen Daten nicht wirklich gelöscht, sondern es wird nur der Zugang gesperrt. Schließlich bleibt unklar, welche Daten zu welchen Zwecken ausgewertet werden, und in welchem Ausmaß Strafverfolgungs- und Sicherheitsbehörden – sowohl nationale als auch ausländische wie etwa der amerikanische Geheimdienst *Central Intelligence Agency (CIA)* – die Nutzenden durchleuchten.[8] *Facebook* ist die perfekte, privat organisierte Vorratsdatenspeicherung.

Im Ergebnis werden sämtliche elementaren Datenschutz-Schutzziele von *Facebook* missachtet. Es bleibt die Frage, was aus einer solchen Analyse folgt. Eine Diagnose ist noch keine Therapie, aber das wäre ein anderes Thema.

Anmerkungen

1 Dt: Technologien zur Verbesserung der Privatsphäre. Mittlerweile lassen sich Phasen der Entwicklung von PET ausweisen: Auf die Phase, in der die technische Unterstützung der Datenminimierung im Zentrum der Bemühungen stand, folgte die Phase der Nutzerkontrolle. Als dritte Phase könnte jetzt die technische Unterstützung der Sicherung der *Integrität des Kontextes*, in dem Daten erhoben oder verarbeitet werden, folgen (vgl. Katrin Borcea-Pfitzmann/Andreas Pfitzmann/Manuela Berg, Privacy 3.0 := Data Minimization + User Control + Contextual Integrity; in: Information Technology, Heft 1/2011).

2 Die sechs elementaren Schutzziele sind seit Januar 2012 Bestandteil des §5 Landesdatenschutzgesetz von Schleswig-Holstein. Zur Kritik am BDSG vgl. Andreas Pfitzmann/Hansjürgen Garstka/Alexander Roßnagel, Modernisierung des Datenschutzrechts. Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2000, im Internet unter http://www.lda.brandenburg.de/sixcms/media.php/2473/dsmodern.pdf.

3 Vgl. Hannes Fedderath/Andreas Pfitzmann, Gliederung und Systematisierung von Schutzzielen in IT-Systemen, in: Datenschutz und Datensicherheit (DuD), Bd. 34 (12/2000), S. 704-710.

4 Vgl. Bundesverfassungsgericht, Urteil vom 27.2.2008, BVerfGE 120, 274 (303 ff.), Urteil vom 27. Februar 2008 – Az. 1 BvR 370/07 und 1 BvR 595/07, im Internet unter http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html.

5 Vgl. als zentralen theoretischen Artikel zu den neuen Schutzzielen: Martin Rost/Andreas Pfitzmann, Datenschutz-Schutzziele – revisited, in: DuD, Bd. 33 (Heft 6/2009), S. 353-358. Zur Beziehung zwischen *Privacy by Design* und den neuen Schutzzielen s. Martin Rost/Kirsten Bock, *Privacy by Design* und die neuen Schutzziele – Grundsätze, Ziele und Anforderungen; in: DuD, Bd. 35 (Heft 1/2011), S. 30-35.

6 Vgl. Marit Hansen/Sebastian Meissner (Hrsg.), Verkettung digitaler Identitäten, Kiel 2007, sowie die Informationen des Forschungsprojekts PRIME/FIDIS –

Privacy and Identity Management for Europe, im Internet unter https://www.datenschutzzentrum.de/projekte/idmanage.

7 Vgl. Martin Rost, Gegen große Feuer helfen große Gegenfeuer, Datenschutz als Wächter funktionaler Differenzierung, in: vorgänge Nr. 184 (Heft 4/2008), S. 15–25.

8 Vgl. Sascha Adamek, Die *Facebook*-Falle – Wie das soziale Netzwerk unser Leben verkauft, München 2011.

Peter Schaar

Systemdatenschutz – Datenschutz durch Technik oder warum wir eine Datenschutztechnologie brauchen

Der technologische Wandel beeinflusst in vielerlei Hinsicht unser Zusammenleben, unsere Vorstellungen von Privatheit und Öffentlichkeit. So ist es nicht verwunderlich, dass auf technologische Entwicklungen in der Vergangenheit häufig mit neuen rechtlichen Ge- und Verboten reagiert wurde: Es waren die Herausforderungen des Fotojournalismus, die die amerikanischen Juristen Warren und Brandeis im Jahr 1890 in ihrem berühmten Aufsatz »The Right to Privacy« (siehe auch die Literaturhinweise im Anhang dieses Bandes, S. 444 ff.) zu der Forderung nach einem Recht veranlassten, »in Ruhe gelassen zu werden«.

Auch die Grundzüge des heutigen Konzepts des Datenschutzes gehen auf einen technologischen Wandel zurück – die in den 1960er Jahren einsetzende »elektronische Datenverarbeitung« (EDV), wie die maschinelle Informationsverarbeitung damals hieß. Die Menschen sollten vor einem »Missbrauch« ihrer personenbezogenen Daten geschützt werden (siehe auch den Beitrag von Lewinski in diesem Band, S. 23 ff.).

Schließlich entwickelte das Bundesverfassungsgericht auf dieser Basis im Volkszählungsurteil 1983[1] seine Lehre vom Datenschutz als »Grundrecht auf informationelle Selbstbestimmung« (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.). Zur Absicherung des Grundrechts auf informationelle Selbstbestimmung müssen die datenverarbeitenden Stellen technische und organisatorische Maßnahmen treffen, welche den rechtmäßigen Umgang mit den Daten gewährleisten und einen Missbrauch verhindern. Insofern überschneidet sich das traditionelle Konzept des technischen Datenschutzes mit der »IT-Sicherheit«, das heißt mit der Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten und informationstechnischen Systemen.

1 Grundrechtskonforme Datenschutztechnologie wird immer wichtiger

Rechtliche Definitionen allein gewährleisten heutzutage aber längst nicht mehr die Datenhoheit des Einzelnen. Immer deutlicher wird: Es kann nicht bloß um die Vermeidung von Nebenwirkungen, um die organisatorischen und technischen Rahmenbedingungen der Informationstechnik gehen. Vielmehr muss die Gestaltung der IT-Systeme selbst in den Vordergrund gerückt werden. Die Forderung nach einer grundrechtskonformen Technikgestaltung, einer »Datenschutztechnologie«, erhob bereits 1995 der von der damaligen Bundesregierung eingesetzte »Rat für Forschung, Technologie und Innovation«.[2]

Datenvermeidung und *Datensparsamkeit* sind Kernforderungen dieser »Datenschutztechnologie«. Nicht zuletzt vor dem Eindruck der wiederkehrenden Datenschutzskandale wird ein »Systemdatenschutz« wichtiger denn je:

- Die *Miniaturisierung der Informationstechnik* und der damit verbundene Einsatz immer kleinerer und leistungsfähigerer informationstechnischer Systeme führen zu einer allgegenwärtigen Datenverarbeitung (→ *Ubiquitous Computing*). Die Speicher- und Verarbeitungskapazitäten heutiger Westentaschencomputer mit Telefonfunktion (→ *Smartphones*) ist bisweilen größer als diejenige von Großrechnern in den 1960er Jahren. Ohne Systemdatenschutz sind derartige Geräte in der Lage, vielfältige Daten der Nutzerinnen und Nutzer (etwa Standorte oder Kontaktdaten) – auch ohne deren Einwilligung – zu übermitteln. Dies führte in der Vergangenheit schon dazu, dass Patienteninformationen ungewollt bei *Facebook* veröffentlicht wurden. Die *Facebook*-Funktion »Freunde finden« hatte die auf den PCs oder *Smartphones* gespeicherten Adressbücher der Ärzte ohne deren gezielte Einwilligung übertragen.
- Mit der Vernetzung im Nahbereich (zum Beispiel mit Hilfe der → *Bluetooth*- oder → RFID-Technologie) oder über Telekommunikationsnetze werden IT-Systeme zu umfassenden Verbundsystemen. Derartige Systeme aus miteinander vernetzten *Smartphones*, *Notebooks*, Arbeitsplatzcomputern und Großrechnern lassen sich immer weniger mit der klassischen datenschutzrechtlichen Rollenverteilung (verantwortliche Stelle, Auftragnehmer und Betroffene) beschreiben. Die Nutzerinnen und Nutzer solcher vernetzten Gegenstände haben heute kaum noch einen Überblick über Art und Umfang der erhobenen Daten, Speicherort und -dauer sowie die Verwendung ihrer Daten. Ein Alltagsbeispiel für die Vernetzung im Nahbereich und den damit verbundenen Kontrollverlust der Nutzenden sind die in Kleidungsstücken eingewebten

→RFID-Chips: Über die RFID-Chips in den gekauften Kleidungsstücken lassen sich Produktinformationen (von der Herstellung bis zur Entsorgung) und Konsumgewohnheiten (wann und wo gekauft, wie lang getragen etc.) erfassen und mit Hilfe einer Kundenkarte zu detaillierten personenbeziehbaren Kundenprofilen verdichten. Bereits in der Entwurfsphase solcher Vernetzungstechniken wäre festzulegen, welche Daten von wem erhoben, verwendet und gespeichert werden dürfen, um unkontrollierbaren Datenaustausch zu vermeiden und das Recht auf informationelle Selbstbestimmung zu wahren.

- Durch die Globalität der Informationstechnologie, die spätestens mit dem Siegeszug des Internet für jedefrau und jedermann sichtbar geworden ist, stoßen die rechtlichen Steuerungsmöglichkeiten, vor allem im Hinblick auf das nationale Recht, im wahrsten Sinne des Wortes an ihre Grenzen. In der Praxis wird das bei den sogenannten → *Cloud Computing*-Diensten anschaulich. Die Nutzenden eines *Online*-Angebotes wissen häufig nicht, auf welchem Server in welchem Land ihre Daten verarbeitet werden. Oftmals stehen die Server in Staaten mit einem niedrigen Datenschutzniveau. Wo Gesetze nicht weiterhelfen, kann eine datenschutzgerechte Technikgestaltung grenzüberschreitend dazu beitragen, die Persönlichkeitsrechte der Betroffenen zu wahren und ihnen ein möglichst hohes Maß an Kontrolle über ihre Daten zu erhalten.

Einen wirksamen Schutz der personenbezogenen Daten und damit der Persönlichkeitsrechte gewährleistet heutzutage also nur eine Allianz von Recht und Technik. Systeme müssen mit einem »eingebauten Datenschutz« entwickelt werden. Dieser gestalterische Ansatz wird auch als *Privacy by Design* bezeichnet.

2 Datenschutz durch Gestaltung von Produkten, Dienstleistungen und Verfahren

Die Grundlagen einer datenschutzfreundlichen Gestaltung finden sich bereits in den rechtlichen Normen des Datenschutzes:

Schon die europäische Datenschutzrichtlinie von 1995 (RL 95/46/EG) enthält den Grundsatz, dass eine Verarbeitung personenbezogener Daten nur stattfinden darf, soweit sie im Hinblick auf bestimmte, festgelegte Zwecke notwendig ist. Sie geht auch von dem Prinzip aus, dass Privatsphäre und informationelle Selbstbestimmung dann am wirksamsten

geschützt sind, wenn möglichst keine personenbezogenen Daten erhoben werden. Im Hinblick auf die Umsetzung dieses Grundsatzes fördert die Europäische Kommission die Entwicklung und Anwendung datenschutzfreundlicher Technologien insbesondere im Rahmen des elektronischen Handels (Stichworte sind hier der →anonyme Zugang zu Netzen und anonyme Zahlungsweisen).

Datenvermeidung und Datensparsamkeit sind wichtige Systemkomponenten

Schließlich haben die Grundsätze der Datenvermeidung und Datensparsamkeit im Jahr 2001 auch Eingang in das Bundesdatenschutzgesetz gefunden (§ 3a BDSG). Danach haben sich die »Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen (…) an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.«

Letztlich geht es bei Datenvermeidung und Datensparsamkeit um die Übersetzung des datenschutzrechtlichen Grundsatzes der Erforderlichkeit in die Technik: Für einen Informationsdienst dürfen nur jene Daten erhoben werden, die zu seiner Bereitstellung erforderlich sind. Oder anders: Daten, die für das Funktionieren eines Dienstes nicht benötigt werden, sollten gar nicht erst erhoben werden. Insofern handelt es sich bei »*Privacy by Design*« um keine völlig neue Erfindung, sondern um die technische Implementierung eines traditionellen Datenschutzprinzips in neue Informationssysteme.

Die rasante Ausbreitung neuer Informationssysteme in den vergangenen Jahren stellt den Datenschutz vor neue Herausforderungen: Beim Einkaufen, Zahlen, Buchen und Reservieren mittels bequemer Chip- oder Magnetstreifenkarten, bei der Kommunikation in digitalen Netzen, bei Arztbesuchen mit Krankenversicherten- oder Gesundheitskarte, durch die Teilnahme an *Online*diensten, →sozialen Netzwerken etc. fallen eine Fülle von Einzeldaten über die Nutzerinnen und Nutzer an. Der Schutz der Privatsphäre wird bei vielen Systemen bisher vorwiegend dadurch angestrebt, dass der Zugang zu den personenbezogenen Daten mittels technischer und organisatorischer Maßnahmen beschränkt wird. Der Datenschutz hängt – nach dieser Systemlogik – lediglich von der Wirksamkeit der implemen-

tierten Sicherheitsmaßnahmen und der Gewissenhaftigkeit ab, mit der sie angewandt werden. Mit solchen zugangsbeschränkenden Sicherheitsmaßnahmen werden aber nur die klassischen Schutzziele (Integrität, Vertraulichkeit, Verfügbarkeit und Zurechenbarkeit der gespeicherten Daten) angesprochen, weitergehende Datenschutzanforderungen können nicht erfüllt werden (siehe auch den Beitrag von Rost in diesem Band, S. 353 ff.).

Ein effizienter, zeitgemäßer Datenschutz verlangt jedoch mehr! Es wächst die Erkenntnis, dass der zunehmenden Gefährdung der Privatheit des Einzelnen nur durch eine weitgehende Reduzierung der Menge der gespeicherten Daten wirksam begegnet werden kann. Datenvermeidung ist also nach wie vor das A und O datenschutzfreundlicher Technikgestaltung.

Bei genauer Betrachtung zeigt sich, dass eine Vielzahl von Prozessen, die heute direkt oder indirekt auf einzelne Personen zurückzuführen sind und insofern einem erhöhten Missbrauchsrisiko unterliegen, auch anonym oder zumindest unter einem → Pseudonym abgewickelt werden können. So ist es zum Beispiel völlig überflüssig, dass ein Anbieter eines kostenlosen Informationsportals im Internet dessen Nutzung von einer persönlichen Registrierung der Nutzenden und damit einer Erhebung personenbezogener Daten abhängig macht. Selbst bei der Bereitstellung kostenpflichtiger Internetdienste gibt es bewährte Geschäftsmodelle, die ohne direkten Personenbezug auskommen, weil die Zahlungsvorgänge über Dritte abgewickelt werden können. Umgekehrt müssen die Anbieter der Zahlungsdienste nicht Detailwissen aufbauen, in welcher Weise die bezahlten Dienste jeweils genutzt werden. Dieses Beispiel macht deutlich, dass Datenvermeidung nicht nur den Aspekt der technologischen Gestaltung einzelner Systemkomponenten umfasst, sondern auch die Organisation und das Zusammenwirken unterschiedlicher Systemfunktionen.

Anonymisierung und Pseudonymisierung sind zwei wesentliche Bausteine in der datenschutzfreundlichen Gestaltung von Produkten, Dienstleistungen und Verfahren.

3 Anonymisierung

Bereits 1983 hat das Bundesverfassungsgericht im Volkszählungsurteil – am Beispiel der Statistik – den Anspruch auf Anonymisierung anerkannt: »Für den Schutz des Rechts auf informationelle Selbstbestimmung ist – und zwar auch schon für das Erhebungsverfahren – (…) die Einhaltung des

Gebots einer möglichst frühzeitigen faktischen Anonymisierung unverzichtbar, verbunden mit Vorkehrungen gegen die Deanonymisierung«[3].

In der Rechtsprechung zum Medienrecht ist das Recht auf Anonymität ebenfalls seit Längerem als besondere Ausprägung des Persönlichkeitsrechts anerkannt, beispielsweise vom Bundesgerichtshof: »Das Recht auf informationelle Selbstbestimmung schützt (…) davor, aus dem Bereich der Anonymität in den einer persönlichen Bekanntheit gerückt zu werden«[4].

Sofern eine Wahlmöglichkeit besteht, gilt aus Sicht der Nutzerinnen und Nutzer, dass jene Verfahren den Vorrang verdienen, die den Betroffenen ein Höchstmaß an Anonymität gegenüber Netzbetreibern und Dienstleistungsanbietern sichern. Dieser Grundsatz der Datenvermeidung ist zum Beispiel im Telemediengesetz enthalten. Danach haben Anbieter von Telemediendiensten den Nutzenden die Inanspruchnahme und Bezahlung entweder vollständig anonym oder unter Verwendung eines Pseudonyms (dazu unten ausführlich) zu ermöglichen, soweit dies technisch möglich und zumutbar ist.

Anonymisierung – so die Definition in § 3 Absatz 6 BDSG – ist eine Veränderung personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

Im Unterschied zu einer pseudonymen Nutzung bedeutet Anonymisierung, dass die Daten zumindest für eine »logische Sekunde« personenbezogen sind, aber im System sofort so geändert werden, dass eine Zuordnung zu den konkreten Personen danach nicht mehr möglich ist. Verfahren zur Anonymisierung von Daten werden beispielsweise in Statistik und Forschung angewandt

Die Qualität einer Anonymisierungsprozedur hängt von verschiedenen Einflussfaktoren ab. Entscheidend hierfür sind der Zeitpunkt der Anonymisierung, die Rücknahmefestigkeit der Anonymisierungsprozedur, die Mächtigkeit der Menge, in der sich der Betroffene verbirgt, und die Verkettungsmöglichkeit von einzelnen Transaktionen desselben Betroffenen. Auch die Anzahl und die statistische Verteilung der konkreten Einzelangaben in den Datensätzen/Transaktionen sind für die Qualität der Anonymisierungsprozedur von Bedeutung. Sie bestimmen die Mächtigkeit der Menge, in der sich die Daten des einzelnen Betroffenen verbergen lassen. Sind in den Daten singuläre Werte vorhanden (Beispiel: Beruf/Amt = Bundeskanzlerin), müssen diese mit anderen zusammengefasst werden, um die Anonymität nicht zu gefährden (etwa: Beruf/Amt = Mitglied der Bundesregierung). Ist eine solche Aggregation der

Daten aus technischen oder inhaltlichen Gründen nicht möglich, kann keine Anonymität erreicht werden.

Grundsätzlich gilt aber auch hier: Ein Höchstmaß an Anonymität wird dann erreicht, wenn personenbezogene Daten gar nicht erst entstehen. Gelungene Beispiele anonym nutzbarer Dienste sind Telefonkarten und anonyme Zahlkarten im öffentlichen Personennahverkehr.

4 Pseudonymisierung

Pseudonymisieren ist das Ersetzen des Namens oder anderer Identifikationsmerkmale durch ein Kennzeichen. Durch Pseudonyme soll die Identifikation der Betroffenen ausgeschlossen oder wesentlich erschwert werden (§ 3 Absatz 6a BDSG).

Dazu werden beispielsweise die Identifikationsdaten durch eine Abbildungsvorschrift in ein willkürlich gewähltes Kennzeichen (das Pseudonym) überführt. Ziel eines solchen Verfahrens ist es, nur bei Bedarf und unter Einhaltung vorher definierter Rahmenbedingungen den Personenbezug wieder herstellen zu können. Je nach Verknüpfbarkeit und dem Geheimnisträger des Pseudonyms kann der Personenbezug

- lediglich vom Betroffenen (selbstgenerierte Pseudonyme),
- nur über eine Referenzliste (Referenz-Pseudonyme) oder
- nur unter Verwendung einer sogenannten Einweg-Funktion mit geheimen Parametern (Einweg-Pseudonyme)

wiederhergestellt werden.

Im Unterschied zu anonymen Daten sind Daten, die unter Pseudonym gespeichert werden, in vielen Fällen noch einzelnen Personen zuzuordnen. Ja, es ist geradezu der Zweck einer pseudonymen Speicherung, die Zuordnung bestimmter persönlicher Einzelangaben zu einem Datenbestand zu ermöglichen, ohne dass die reale Identität des Betroffenen dabei selbst gespeichert wird. Mit Pseudonymen versehene Daten sind deshalb grundsätzlich als personenbezogene Daten anzusehen.

Unter gleichen Bedingungen ist die Anonymisierung datenschutzfreundlicher als die Pseudonymisierung. Wo Anonymisierungen nicht möglich sind, sollten daher Pseudonyme eingesetzt werden. So ist es in vielen Forschungsvorhaben ohne Belang, welche Person sich hinter einem bestimmten Wert (Einkommen, Alter, Gesundheitszustand) verbirgt. Gleichwohl muss sichergestellt werden, dass insbesondere bei Langzeitstudien oder der Zusammenführung von Daten aus unterschiedlichen

Quellen eine korrekte Zuordnung erfolgt. Die Verwendung von Pseudonymen ist hier das Mittel der Wahl.

Die Qualität der Pseudonymisierungsprozedur hängt von den gleichen Einflussfaktoren ab wie die Stärke der Anonymisierungsprozedur – nämlich vom Zeitpunkt der Pseudonymisierung, von ihrer Rücknahmefestigkeit und von der Verkettungsmöglichkeit von einzelnen Transaktionen/Datensätzen desselben Betroffenen. Da in pseudonymen Daten die verschiedenen Transaktionen/Datensätze einer Person, die unter demselben Pseudonym gespeichert wurden, miteinander verkettet werden, ist die Gefahr einer Deanonymisierung hier ungleich größer. (Im oben gewählten Beispiel: Unter den Mitgliedern der Bundesregierung gibt es nur eine Person, die 1973 ihr Abitur in Templin absolvierte – die Verknüpfung der beiden Daten würde Frau Merkel identifizierbar machen.)

Sichere Pseudonyme ermöglichen es, die Identität einer Person zuverlässig zu verdecken und nur in den vorab bestimmten Einzelfällen erkennbar zu machen. Pseudonyme sollen zufällig und nicht vorhersagbar gewählt werden. Die Menge der möglichen Pseudonyme soll so mächtig sein, dass bei zufälliger Auswahl nicht zweimal das gleiche Pseudonym generiert wird. Ist eine hohe Sicherheit erforderlich, muss die Menge der Pseudonymkandidaten mindestens so mächtig sein wie der Wertebereich sicherer kryptographischer Kodierungsfunktionen (auch → *Hash*funktionen genannt).[5]

5 Perspektiven und Stellschrauben einer datenschutzfreundlichen Technikentwicklung

Für die Akzeptanz von neuen Multimedia-Techniken und *Online*diensten wird die Sicherstellung des Datenschutzes und der Privatheit der einzelnen Person von entscheidender Bedeutung sein. Studien belegen immer wieder: Die Nutzerinnen und Nutzer sorgen sich um den Schutz ihrer persönlichen Daten. Datensicherheit und Datenhoheit wird in diesen Studien eine hohe Bedeutung eingeräumt. Gleichwohl gestaltet sich die Umsetzung datenschutzfreundlicher Techniken in IT-Verfahren schwierig, weil die Anbieter bei konsequenter Einhaltung der Datensparsamkeit und Datenvermeidung keine Daten von ihren Nutzerinnen und Nutzern bekommen, die sie »wiederverwerten« können. Datenschutzfreundliche Technikgestaltung läuft also dort ins Leere, wo die geschäftlichen Interessen der Diensteanbieter konträr zum Schutzanspruch der Nutzenden stehen. Hier sind dann gesetzliche Regelungen gefragt, die die Anbieter auf datensparsame Techniken verpflichten.

Darüber hinaus haben es die Anwenderinnen und Anwender selbst in der Hand: Wenn datenschutzkonforme Produkte besser angenommen werden als »datenschutzunfreundliche« Produkte, wird Datensparsamkeit zum Wettbewerbsfaktor und die Menge der personenbezogenen Daten unweigerlich reduziert.

Nach wie vor fehlen aber vielfach praktikable Verfahren, die von den Nutzerinnen und Nutzern auf einfache Weise bedient werden können. Die heute verfügbaren Verfahren zur Anonymisierung oder Pseudonymisierung sind zum Teil sehr komplex, aufwendig und unflexibel. Hier bedarf es noch umfassender Forschung und Entwicklung, um die Verfahren so zu gestalten, dass sie auch von »Laien« problemlos eingesetzt werden können.

Die Zukunft des Datenschutzes hängt insofern entscheidend davon ab, ob es gelingt, einfach zu handhabende datenschutzfreundliche Produkte und Dienstleistungen auf dem Markt zu etablieren, die genauso komfortabel und leistungsfähig sind wie die heute verfügbaren datenintensiven Anwendungen. Unabhängige Zertifizierungen von informationstechnischen Produkten und Dienstleistungen (Datenschutzaudit) können hier eine Entscheidungshilfe für die Nutzerinnen und Nutzer geben (siehe auch den Beitrag von Bock in diesem Band, S. 310 ff.).

Anmerkungen

1 BVerfGE 65,1; Az. 1 BvR 209/83 u. a.
2 Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie (Hrsg.), Informationsgesellschaft – Chancen, Innovationen, Herausforderungen – Feststellungen und Empfehlungen, Bonn 1995.
3 BVerfGE 65,1; Az. 1 BvR 209/83 u. a., Rn. 49.
4 BGH, AfP, in: Zeitschrift für Medien und Kommunikationsrecht, Jg. 1994, S. 306–307.
5 Die Mächtigkeit einer mathematischen Funktion bzw. Menge wird durch die Anzahl ihrer Elemente bestimmt. Bei einer Kodierungsfunktion geht es dabei um die Anzahl der möglichen Lösungen (Passwörter oder Pseudonyme) – je mehr davon existieren, umso mächtiger und zugleich sicherer ist die Funktion.

Martin Schallbruch

Hilfen für Sicherheit im Internet

Das Internet ist ein selbstverständlicher Teil unseres Lebens geworden. Ob beim Abholen der Post, beim Einkaufen oder Kommunizieren – längst sind virtuelle und reale Welt eng verknüpft. Die zunehmende Vernetzung aller Lebens-, Wirtschafts- und Verwaltungsbereiche über das Internet ist positiv und chancenreich, sie hat aber auch ihre Schattenseiten. Der seriösen Nutzung und Anwendung steht eine starke international tätige Organisierte Kriminalität im Internet gegenüber.

1 Identitätsdiebstahl und Identitätsmissbrauch

Viele Dienste und Anwendungen im Internet werden personalisiert angeboten. Dafür stellen wir Identitätsdaten bereit, die von den Anbietern gespeichert werden. Digitale Identitätsdaten rücken deshalb zunehmend in den Mittelpunkt des Interesses Krimineller. Das betrifft Zugänge zum *Online-Banking, E-Mail-Accounts* ebenso wie Zugangsdaten für DHL-Packstationen, *Onlineshops* oder →soziale Netzwerke wie zum Beispiel *Facebook*. Sind solche Identitätsdaten erst einmal erbeutet, können sie missbräuchlich genutzt und für betrügerische Zwecke verwendet werden.

Für die Sicherheit im Internet wird der Schutz der eigenen Identitätsdaten, der »elektronischen Identität«, immer wichtiger. Im Vergleich zur analogen Welt fehlt vielen Internetanwendern jedoch ein Bewusstsein der Sicherheitsrisiken. Niemand würde seine Kreditkarte bei einem Warenhaus für einen späteren Einkauf hinterlegen. Selbstverständlich tun wir dies aber bei *Online*-Einkaufsportalen. Auch seine Urlaubsbilder hängt kaum ein Mensch außen an seine Wohnungstür. In der Digitalsphäre ist es jedoch für viele Nutzerinnen und Nutzer normal, ihre privaten Bilder bei *Online*-Portalen hochzuladen und zur Schau zu stellen.

2 Wirksamer Schutz vor Angriffen

Private Identitätsdaten werden heute überwiegend durch Angriffe auf die Rechner der Benutzer erbeutet, bei denen Schadprogramme (zum Bei-

spiel »Trojanische Pferde«) eingesetzt werden. →»Trojaner« verdanken ihren Namen dem Heldenepos über den Kampf um Troja: Mit einem Geschenk, dem Trojanischen Pferd, schleusten die Griechen ihre darin versteckten Soldaten in die Stadt Troja ein und konnten so den Krieg für sich entscheiden. Digitale »Trojaner« arbeiten ähnlich: Hinter einer scheinbar nützlichen Software oder Datei verbirgt sich ein tückisches Schadprogramm, das unbemerkt Eingaben (etwa Passwörter) protokolliert und an fremde Rechner übermittelt.

Trojaner nutzen Schwachstellen in der Software oder im Betriebssystem der Computer aus. Den besten Schutz bieten nach wie vor die Standardsicherheitsmaßnahmen wie Virenschutzprogramme, → *Firewalls* sowie regelmäßige Updates von Betriebssystemen und Anwendungssoftware. Keine dieser Sicherheitsmaßnahmen bietet jedoch einhundertprozentigen Schutz.

Weil ein perfekter Schutz nicht möglich ist, sollten Nutzerinnen und Nutzer immer überlegen, welche ihrer persönlichen Daten im Internet gut aufgehoben sind. Vieles erscheint praktisch, wie die hinterlegte Kreditkartennummer bei Einkaufsportalen, erleichtert jedoch auch den Missbrauch. Müssen die letzten Urlaubsbilder im Netz für jede und jeden sichtbar sein? Inzwischen bieten die meisten *Online*-Portale Einstellmöglichkeiten, bei denen persönliche Daten nur für festgelegte Personenkreise zugänglich sind. Datenschutz fängt bei der individuellen Entscheidung jedes Einzelnen an und muss mehr denn je die Privatsphäre anderer achten.

Schon mit einfachen Regeln kann der Schutz der persönlichen Daten im Internet erhöht werden:

- Nur Webseiten aufrufen, denen ein Mindestmaß an Vertrauen entgegengebracht wird. Schadsoftware kann auch bereits durch das schlichte Ansurfen von Webseiten, ohne ausdrückliches Ausführen von Programmen, auf den Rechner des Benutzers geladen werden.
- Bei sozialen Netzwerken ein den eigenen Bedürfnissen passendes, also altersgerechtes Netzwerk suchen.
- Vor der Eingabe persönlicher Daten im Internet lohnt sich die Frage, ob man diesen Dienst nur ausprobieren oder tatsächlich längerfristig nutzen will. Sollte ersteres der Fall sein, reicht vielleicht eine Anmeldung mit →anonymen oder →pseudonymen Identitätsdaten aus, um sich ein Bild von dem Angebot zu machen. Bei der Angabe persönlicher Daten reicht es, zunächst nur die Pflichtfelder auszufüllen – weitere Angaben lassen sich immer nachtragen, einmal freigegebene Daten dagegen schwer wieder zurückholen.

- Persönliche Daten sollten nur auf Webseiten eingegeben werden, über die mit einer →SSL-gesicherten Verbindung kommuniziert wird. Wenn eine solche Sicherung fehlt, könnten die Daten während der Übertragung zum Server abgefangen werden.
- Bilder mit niedriger Auflösung hochladen und kompromittierende Fotos vermeiden.
- Datenschutzfreundliche Einstellungen verwenden. Browser können etwa auch ohne Speicherung von Verlauf und →*Cookies* genutzt werden. In sozialen Netzwerken sollten die Standardeinstellungen so geändert werden, dass persönliche Daten nur für ausgewählte Freunde und nicht für jede beliebige Person sichtbar sind.
- Für unterschiedliche Netzwerke verschiedene →Pseudonyme und E-Mail-Adressen verwenden. Auch bei *Onlineshops* und anderen Diensten sollten nie die gleichen Benutzernamen/Passwörter verwendet werden. Die Passwörter sollten außerdem regelmäßig geändert werden.
- Bei Nutzung von Internetcafés oder fremdadministrierten Netzen (ungesicherte Rechner) möglichst keine vertraulichen Daten oder Passwörter angeben.
- Wird ein soziales Netzwerk nicht mehr genutzt, sollten die Mitgliedschaft beendet und die Daten gelöscht werden.

Maßstab für alle Sicherheitsbemühungen sollte der Vergleich zur realen Welt sein: Würde ich diesem Anbieter oder diesem Personenkreis tatsächlich meine Daten, Fotos etc. verfügbar machen?

3 Bekämpfung von Botnetzen – eine neue Herausforderung

Eine große Herausforderung für die Sicherheit im Internet ist die Bekämpfung von →Botnetzen. Für den Aufbau eines Botnetzes werden zunächst tausende von Rechnern mit Schadprogrammen (meist »Trojanern«) infiziert. Die infizierten Rechner der meist ahnungslosen Nutzenden führen dann Befehle der Betreiber dieses Botnetzes aus, sie lassen sich fernsteuern. Derart »gekaperte« PCs werden für eine Vielzahl von Angriffen genutzt. Dazu gehören insbesondere der massenhafte Versand von Spam-Nachrichten, der Diebstahl von Bankzugangsdaten (→*Phishing*), sonstiger Datendiebstahl und Erpressung.

In großen Botnetzen können hunderttausende dieser gekaperten PCs zusammengeschaltet werden. Diese verfügen dank Breitband-Anschlüssen und Internet-Flatrates über enorme Übertragungskapazitäten, die

von Kriminellen zum Beispiel für *Distributed Denial of Service-Angriffe (DDoS)* genutzt werden. Bei einem solchen Angriff senden alle Rechner eines Botnetzes gleichzeitig Anfragen oder Daten an einen Zielserver und zwingen ihn dadurch in die Knie. DDoS-Attacken auf gewerbliche Webangebote sind oft mit einer Erpressung der entsprechenden Anbieter verbunden.

Deutschland rangiert derzeit unter den TOP 10 der Länder hinsichtlich der infizierten und Spam-versendenden Rechner. Ein besserer Schutz der Computernutzer und mehr Hilfen für die Anwender sind daher notwendig.

Mit der »Anti-Botnet-Initiative« des Verbands der Deutschen Internetwirtschaft *eco* werden Kunden, deren PC infiziert worden ist, von ihrem Provider darüber informiert. Ihnen wird zugleich kompetente Unterstützung bei der Beseitigung der Schadsoftware angeboten. In einem ersten Schritt erhalten die Betroffenen auf der Internetseite *www.botfrei.de* Informationen und Hilfen zur Selbsthilfe, insbesondere Programme zur automatischen Entfernung dieser Schadprogramme. Sollte dies nicht ausreichen, hilft ein anbieterübergreifendes Beratungszentrum telefonisch weiter. Es werden die notwendigen Schritte zur Beseitigung der Schadsoftware und zur Absicherung des PCs vor einem erneuten Befall erläutert.

Auch private PC-Nutzende stehen in der Verantwortung. Die Angebote der Anti-Botnet-Initiative werden bislang – im Vergleich zur Zahl der infizierten Rechner – nur recht wenig in Anspruch genommen. Versierte sind sicherlich in der Lage, ihren PC selbst wieder von einem Schadprogramm zu bereinigen. Doch ist zu befürchten, dass viele eine mögliche Infizierung ihres Rechners ignorieren, so lange die Schadprogramme sie nicht unmittelbar bei ihrer Arbeit stören – beispielsweise durch Rechnerabstürze oder langsame Datenverbindungen. Das haben inzwischen auch die Entwickler dieser Schadprogramme erkannt: Aktuelle Versionen sind meist so programmiert, dass ihr »Wirt« möglichst wenig von ihnen mitbekommt. Inzwischen geht dies so weit, dass neuere Versionen sogar ältere Schadprogramme entfernen, damit sie nicht aufgrund von Performance-Einbußen entdeckt werden.

Nutzende, die nichts gegen eine solche Infektion ihres Rechners unternehmen, müssen selber mit rechtlichen Konsequenzen rechnen. Im besten Fall sperrt ihnen ihr Provider wegen eines Verstoßes gegen dessen Allgemeine Geschäftsbedingungen (AGB) den Internetzugang, bis der Rechner wieder bereinigt ist. Im schlimmsten Fall steht irgendwann die Polizei vor der Tür und beschlagnahmt den Rechner, weil von diesem immer wieder Angriffe auf andere Rechner im Internet festgestellt wurden.

4 Sichere Kommunikation mit De-Mail

Heute werden immer noch weniger als fünf Prozent der E-Mails verschlüsselt und signiert. Über 95 Prozent aller E-Mails können also auf ihrem Weg durch das Internet abgefangen, wie Postkarten mitgelesen und in ihrem Inhalt verändert werden. Absender und Empfänger können nie vollständig sicher sein, mit wem sie gerade kommunizieren und ob die gesendete E-Mail tatsächlich beim Empfänger angekommen ist. Wenn es um vertrauliche Kommunikation geht, die Identität der Kommunikationspartner sicher gestellt sein muss oder auf den Nachweis des Empfangs einer Nachricht beim Empfänger (elektronisches Einschreiben) ankommt, können solche Nachrichten deshalb nicht mit einer einfachen E-Mail verschickt werden – sie sollten es zumindest nicht.

Am Markt existieren zahlreiche Lösungen für mehr Sicherheit bei E-Mails (siehe auch den Beitrag von Thomsen in diesem Band, S. 381 ff.). Diese haben sich jedoch nicht in der Fläche durchsetzen können, da sie häufig zusätzliche Soft- und Hardware auf den Rechnern der Nutzer erfordern (etwa Zertifikate und Kartenlesegeräte) und teilweise nur über unhandliche Benutzeroberflächen zugänglich sind.

→De-Mail soll eine sichere Mailkommunikation für breite Anwenderkreise zugänglich machen. Im einfachsten Fall melden sich Anwender über Benutzername und Passwort an der Weboberfläche ihres De-Mail-Providers an und können sichere De-Mails empfangen und verschicken. Bei De-Mails werden Verschlüsselung, sichere Identität der Kommunikationspartner und Nachweisbarkeit der Zustellung gewährleistet. Die Einstiegshürde soll für diese grundlegenden Sicherheitsfunktionen möglichst niedrig sein, um Sicherheit endlich mehr in die breite Nutzung zu bringen. Weitergehende Sicherheitsniveaus, etwa die Anmeldung am De-Mail-Konto mit dem neuen Personalausweis (nPA) oder anderen Identifikationsverfahren, eine →Ende-zu-Ende-Verschlüsselung oder qualifizierte elektronische Signaturen sind möglich, aber nicht obligatorisch vorgeschrieben.

Wer De-Mail-Dienste anbietet, muss künftig hohe Anforderungen an Interoperabilität[1], IT-Sicherheit und die Funktionsweise seines Dienstes erfüllen. Die Anforderungen hat der Bund gemeinsam mit der Wirtschaft entwickelt und in Form von technischen Richtlinien festgeschrieben. Darüber hinaus muss jeder De-Mail-Anbieter strenge Anforderungen an den Datenschutz erfüllen, etwa Kopplungsverbote, Datensicherheitsvorschriften oder Protokollierungspflichten.

Der zugrunde liegende Kriterienkatalog ist vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) im Internet

unter *www.bfdi.bund.de* veröffentlicht. Auf dieser Grundlage vergibt der BfDI einen Datenschutznachweis. Nur wenn die Einhaltung aller Anforderungen aus den technischen Richtlinien und dem Datenschutzkatalog nachgewiesen wird, werden De-Mail-Provider durch das Bundesamt für Sicherheit in der Informationstechnik (BSI; siehe dazu weiter unten Abschnitt 6 dieses Artikels) akkreditiert und können De-Mail-Dienste am Markt anbieten.

Die Deutsche Telekom AG, T-Systems und die Mentana-Claimsoft GmbH wurden bereits vom BSI als erste De-Mail-Anbieter in Deutschland zugelassen. United Internet (mit den Marken GMX, WEB.DE und 1&1) befindet sich derzeit noch im Zulassungsverfahren (Stand: Juli 2012). Weitere Informationen zu De-Mail sind zu finden auf *www.de-mail.de*.

5 Der neue Personalausweis

Der neue Ausweis hat das praktische Format einer Kreditkarte und bietet viele Einsatzmöglichkeiten in der digitalen Welt, die man vom »Perso« bislang nicht kannte. Ein Chip im Inneren der Ausweiskarte schafft die Voraussetzung für eine »*Online*-Ausweisfunktion«. Mit ihr kann eine Person – analog zur realen Welt – ihre Identität sicher und zuverlässig nachweisen. Das Identifikationsverfahren erlaubt es den Anwenderinnen und Anwendern gleichzeitig auch, die Identität ihres Gegenübers zweifelsfrei zu bestimmen, denn alle Diensteanbieter, die das Verfahren nutzen wollen, müssen zuvor eine Berechtigung beantragen. Dadurch können noch mehr Dinge bequem, zeit- und geldsparend vom PC aus getätigt werden.

Der neue Personalausweis bietet nicht nur ein Höchstniveau an technischer Sicherheit, sondern berücksichtigt die wichtigsten Prinzipien des Datenschutzes, nämlich Datensparsamkeit, Erforderlichkeit und Zweckbindung. Dies geschieht zum einen durch staatliche Berechtigungszertifikate, die regeln, welche Ausweisdaten für die Abwicklung der verschiedenen *Online*-Services auf Anbieterseite überhaupt erforderlich sind. Zum anderen haben Nutzende die volle Kontrolle über ihre persönlichen Daten, da sie in jedem Einzelfall selbst entscheiden, ob und welche Informationen sie dem Anbieter preisgeben möchten.

So etwa bei der Altersbestätigung, die zur Nutzung von bestimmten Angeboten im Internet oder an Automaten notwendig ist: Anstelle des vollständigen Geburtsdatums erhält der Anbieter nur die Information, ob das angefragte Alter erreicht oder unterschritten ist. Die Funktion des pseudonymen Zugangs, die etwa für das Anmelden bei *Chat-Rooms*

gedacht ist, geht sogar noch einen Schritt weiter: Hierbei wird überhaupt keine personenbezogene Information übermittelt. Dennoch kann sich der Nutzer oder die Nutzerin mit dem Ausweis bei jeder erneuten Anmeldung auf der Seite als ein und dieselbe Person identifizieren. Diese beiden Beispiele zeigen, dass dem neuen Personalausweis ein konsequent datenschutzfreundliches Konzept zugrunde liegt.

Die Nutzung von Basislesern, das heißt Lesegeräten ohne eigenem PIN-Pad, hat zu einiger Kritik am Gesamtsystem des neuen Personalausweises geführt. Werden diese Lesegeräte für die *Online*-Ausweisfunktion eingesetzt, so kann über entsprechende Schadprogramme – beispielsweise *Key-Logger* – die PIN der Nutzenden ausgespäht werden. Für die Nutzung der *Online*-Ausweisfunktion wird aber neben der PIN immer der Ausweis benötigt, allein durch die Kenntnis der PIN können also keine Identitäten gefälscht werden.

Der Personalausweis erhöht die Sicherheit des Handels im Internet. Es bleibt aber gleichwohl eine Verantwortung bei den Nutzerinnen und Nutzern. So sollte der Ausweisinhaber mit seinem Ausweis genauso sorgsam umgehen wie mit seinen EC- und Kreditkarten, das heißt der Ausweis sollte immer sicher aufbewahrt werden, die PIN für die Nutzung der *Online*-Ausweisfunktion muss sorgsam ausgewählt werden und darf nicht an Dritte weitergegeben oder zusammen mit dem Ausweis aufbewahrt werden. Verloren gegangene oder gestohlene Ausweise müssen unverzüglich gesperrt werden. Zusätzlich sollten auf dem genutzten Rechner jeweils aktuelle Antivirensoftware, eine *Firewall* und das aktuelle Betriebssystem installiert sein. Weitere Informationen dazu gibt es im Internet unter *www.personalausweisportal.de*.

6 Informationsangebote zum Thema Computersicherheit

Die wichtigste staatliche Informations- und Anlaufstelle zu Fragen der IT-Sicherheit ist das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit Sitz in Bonn. Zu seinen Aufgaben gehört die Aufklärung über IT-Sicherheitsfragen. Mit seinem Angebot unter *www.bsi-fuer-buerger.de* geht das BSI speziell auf die Bedürfnisse von Privatnutzenden ein. Einsteiger und Fortgeschrittene finden auf diesen Seiten Informationen und Tipps rund um das Internet und den PC. Auch unter der dort zu findenden BSI-Hotline erhalten Nutzende persönlichen Rat. Ein vierzehntägig erscheinender Newsletter »Sicher informiert« sowie Extraausgaben dieses Dienstes bei zeitkritischen Sicherheitsvorfällen können über

die Plattform *www.buerger-cert.de* abonniert werden. Neben diesen Angeboten stellt das BSI zahlreiche Informationsmaterialien wie Broschüren, Flyer oder CDs bereit. Unter *www.bsi.bund.de* finden Nutzerinnen und Nutzer zudem die zehn wichtigsten Tipps im Umgang mit sozialen Netzwerken.

Das Bundesministerium des Innern arbeitet auch mit dem Verein »Deutschland sicher im Netz (DsiN) e. V.« eng zusammen. Der Verein hat das Ziel, bei Verbraucherinnen und Verbrauchern sowie in Unternehmen ein Bewusstsein für einen sicheren Umgang mit Internet und IT zu fördern. Seine Mitglieder, zu denen führende Unternehmen der IT-Branche gehören, stellen verschiedene Service-Angebote zur Sicherheit im Netz zur Verfügung (»Handlungsversprechen«) und kooperieren dabei eng mit dem BSI. Die Angebote werden unter *www.sicher-im-netz.de* vorgestellt.

Mit dem Portal *www.internauten.de* spricht »Deutschland sicher im Netz« (DsiN) gemeinsam mit seinen Partnern Kinder zwischen acht und dreizehn Jahren an. Ein Medienkoffer begleitet die Internautenserie. Er enthält vier Unterrichtseinheiten und wird zurzeit in Grundschulen in Rheinland-Pfalz, dem Saarland und Berlin eingesetzt.

7 Wenn doch etwas passiert – Tipps für den Ernstfall

Wer man trotz aller Vorsichtsmaßnahmen Opfer einer Internetstraftat geworden ist, sollte prinzipiell dieselben Schritte wie bei einer Straftat im »realen« Leben unternehmen. Dabei ist Folgendes zu tun:

- Es ist zu verhindern, dass der bereits eingetretene Schaden noch größer wird. Karten sollten gesperrt werden, Nutzerkennungen und Passwörter sind möglichst schnell zu ändern.
- Alle Informationen, die zur Aufklärung der Straftat beitragen können, sind zu sichern (Bildschirmfotos, Ausdrucke).
- Der Vorfall ist bei der Polizei zur Anzeige zu bringen.

Besteht beispielsweise der Verdacht, Opfer einer → *Phishing*-Attacke geworden zu sein, ist schnelles Handeln angezeigt:

- Sperren Sie sofort den *Online*zugang für das betroffene Konto bei Ihrem Kreditinstitut.
- Prüfen Sie, ob auf dem Konto Verfügungen vorgenommen wurden, die nicht von Ihnen stammen.
- Sichern Sie betrügerische E-Mails, die Sie erhalten haben.
- Erstatten Sie Anzeige bei der Polizei.

Eine Reihe von Polizeidienststellen bieten mittlerweile die Möglichkeit einer *Online*-Anzeige. Wie eine solche Anzeigenerstattung aussieht, kann man sich beispielsweise auf der Homepage der nordrhein-westfälischen Polizei anschauen: *https://service.polizei.nrw.de/egovernment/service/anzeige.html*. Weiterführende Informationen mit Links zu den Polizeien anderer Bundesländer enthält die Webseite der Internetwache der Berliner Polizei: *https://www.berlin.de/polizei/internetwache/indexmitc.php*.

Anmerkung

1 Interoperabilität meint die Anschlussfähigkeit von (Software-)Systemen, damit zwischen ihnen Daten ausgetauscht und im Idealfall die Systeme gegeneinander ausgetauscht werden können.

Sven Thomsen

Verschlüsselung – Nutzen und Hindernisse in der Praxis

Kryptografie, also das technische Verschlüsseln von digitalen Informationen, ist kein Selbstzweck. Wer den Einsatz von Kryptografie plant, verfolgt hiermit normalerweise einen konkreten Zweck. Dabei lassen sich drei grundlegende Ziele unterscheiden:

- Daten sollen vor unberechtigter Einsichtnahme geschützt werden: In einer Arztpraxis werden Patientendaten in einem Computer gespeichert. Falls in die Praxis eingebrochen und der Computer entwendet wird, sollen die sensiblen Daten geschützt sein.
- Eine Datenverarbeitung soll nur für bestimmte Personen oder Maschinen zugänglich sein: Eine Bürgerin will ihre Steuererklärung gern elektronisch abgeben. Dabei soll sicher gestellt sein, dass die Daten bei der Übertragung zum Finanzamt nicht von anderen abgefangen werden.
- Die Identität einer Person oder Organisation soll bestätigt werden: Eine Kundin erhält die Rechnung eines Versandhauses elektronisch zugeschickt. Sie möchte gern prüfen, ob die Rechnung wirklich von dem Versandhandel ausgestellt wurde, bei dem sie kurz zuvor *online* eingekauft hatte.

Aus diesen Zielen ergeben sich die verschiedenen Anforderungen an kryptografische Verfahren. Alle drei Forderungen lassen sich unter Einsatz solcher Verfahren heute mit ökonomisch vertretbarem Aufwand umsetzen.

1 Lösungsansätze für sichere Kommunikation

Will man eine sichere Kommunikation zwischen zwei oder mehr Teilnehmenden herstellen, so könnte man als erste Idee versuchen, alle Komponenten des Kommunikationssystems abzusichern: Jeder Sender und Empfänger, alle Leitungen, Schaltstellen etc. des Systems müssten vor der eigentlichen Kommunikation geprüft werden. Sind die Systeme korrekt und sicher konfiguriert? Ist die Leitung wirklich abhörsicher? Wer hat Zugriff auf die beteiligten Komponenten? In der Praxis heutiger, weltweit vernetzter Kommunikationssysteme können die Kommunikations-

partner diese Sicherheit selbst kaum noch beurteilen. Allein am Austausch einer einzelnen E-Mail etwa mit einem Freund in Amerika sind schnell 10 bis zwanzig Rechner beteiligt, von den tausenden Kilometern Datenleitung ganz zu schweigen. Wie sollte man eventuelle Sicherheitslücken oder Angriffe in dieser Übertragungskette erkennen? In der Praxis wäre eine Absicherung des gesamten Kommunikationssystems deshalb nur mit hohem personellen und technischen Aufwand zu erreichen. Es müssten rund um die Uhr Sicherheitsüberprüfungen und Fehlerbehebungen durchgeführt werden, und selbst dann wäre nur ein labiles Sicherheitsniveau erreicht: Bereits eine einzige unerkannte Sicherheitslücke würde die Gesamtsicherheit des Systems stark beeinträchtigen. Bei dieser Art der Absicherung müssten die Kommunikationspartner auf die Angemessenheit und Wirksamkeit der technischen und organisatorischen Maßnahmen der Anbieter und Hersteller blind vertrauen.

Kryptografische Verfahren erlauben demgegenüber die sichere Kommunikation in grundsätzlich schlecht kontrollierbaren, unsicheren Umgebungen. Das Konzept der sogenannten →Ende-zu-Ende-Verschlüsselung beruht darauf, sensible Daten vor ihrer Übertragung zu verschlüsseln und sie erst bei den Empfängern wieder zu entschlüsseln. Dieses Verfahren kann für beliebige Kommunikationsformen angewandt werden, etwa den Versand von E-Mails, das sichere Einkaufen über das Internet oder abhörsichere Telefonate. Dadurch können die Teilnehmenden das Sicherheitsniveau selbst bestimmen und die korrekte Umsetzung kontrollieren. Zugleich sind sie nicht vom Mitwirken Dritter (insbesondere den Betreibern der Datenleitungen) abhängig. Eine vollständige Ende-zu-Ende-Verschlüsselung gewährleistet vertrauliche Kommunikation auch auf unsicheren Übertragungskanälen, da die übertragenen Daten von Dritten nicht dechiffriert, das heißt entschlüsselt werden können – so zumindest die Theorie. In der Praxis werden diese Ziele jedoch in den wenigsten Verfahren wirklich zufriedenstellend erreicht.

In aktuellen kryptografischen Verfahren werden zur Verschlüsselung der Informationen mathematische Funktionen genutzt, die durch ihre Eigenheiten einen Angriff sehr aufwändig machen. Entscheidend für die Sicherheit eines solchen Verfahrens ist der Aufwand, den mögliche Angreifer haben, wenn sie beispielsweise eine verschlüsselte E-Mail vorliegen haben und daraus den unverschlüsselten Text berechnen möchten.

Wohlgemerkt: Kein Verfahren ist absolut sicher. Ein zumindest in der Theorie immer erfolgreicher Angriff besteht darin, einfach alle möglichen Schlüssel- oder Passwortkombinationen systematisch durchzuprobieren (*brute force*). Die Güte eines kryptografischen Verfahrens lässt sich daran messen,

wie hoch der Aufwand für einen solchen Angriff ist. Häufig ist die Anzahl der Schlüssel, die man durchprobieren müsste, so hoch, dass es selbst mit einer großen Anzahl an Rechnern mehrere hundert Jahre dauerte, bis die richtige Kombination gefunden wäre. Ein solcher Angriff wäre somit nicht wirtschaftlich, und der verschlüsselte Text wäre längst nicht mehr aktuell.

2 Überprüfbarkeit kryptografischer Verfahren als Sicherheitskriterium

Die Entwicklung kryptografischer Verfahren ist sehr aufwändig. Sie ist von zahlreichen Faktoren abhängig, allen voran von der Güte der verwendeten mathematischen Funktionen und Eigenschaften (zum Beispiel Zufallsgeneratoren oder extrem große Primzahlen), aber auch von der Qualität ihrer Software-Umsetzung – ob also Fehler in der Programmierung der kryptografischen Programme das Verfahren anfällig machen. Aufgrund der vielen denkbaren Fehlerquellen kann letztlich nicht auf formalem Weg (das heißt mit »absoluter« Sicherheit) bewiesen werden, dass ein bestimmtes Verfahren sicher ist. Aus diesem Grund wird häufig auf das Wissen der Vielen gesetzt: Kryptografische Verfahren werden veröffentlicht, damit die führenden Spezialisten ihre Zuverlässigkeit prüfen können. Sie prüfen, ob und wie ein erfolgreicher Angriff aussehen könnte. Die Sicherheit eines Verfahrens wird dann durch die Anzahl und das Ansehen der damit beschäftigen Fachleute und den Zeitablauf entschieden: Wenn anerkannte Experten über einen Zeitraum von mehreren Jahren keine für Angriffe nutzbaren Fehler im Verfahren finden, wird ihm eine ausreichende, stabile Sicherheit zugeschrieben.

Dieses Vorgehen zeigt, dass vertrauenswürdige Verfahren sich vor allem durch maximale Transparenz und Offenheit auszeichnen. Das Herstellen von Sicherheit durch die Geheimhaltung oder das Verschweigen wesentlicher Details (*Security by Obscurity*), ist im Bereich der kryptografischen Verfahren kein akzeptiertes Sicherheitskonzept. Intransparente kryptografische Verfahren werden als Sicherheitsrisiko betrachtet. Diese Verfahren enthalten möglicherweise (unerkannte) Schwächen, beruhen auf dem (blinden) Vertrauen in die Anbietenden und offerieren deshalb nur labile Sicherheit – sie sollten gemieden werden. Eine erste, auch von Laien durchzuführende Kontrolle der Verlässlichkeit kryptografischer Verfahren besteht schlicht darin zu prüfen, ob das Verfahren offengelegt wurde.

Zusätzlich bietet jedes kryptografische Verfahren nur für eine gewisse Zeit einen angemessenen Schutz. Durch technische Fortentwicklungen oder neue mathematische Erkenntnisse kann der Aufwand für einen

Angreifer erheblich sinken. Es ist deshalb wichtig, die eingesetzten Verfahren regelmäßig zu prüfen, zu modernisieren oder durch neue, bessere Vorgehensweisen abzulösen.

Kryptografische Verfahren lassen sich grundsätzlich in zwei Klassen einteilen, die im Folgenden beschrieben werden.

3 Symmetrische und asymmetrische Verfahren

Symmetrische Verfahren benutzen zum Verschlüsseln und Entschlüsseln denselben geheimen Schlüssel. Hierzu ist es notwendig, dass sich die Teilnehmenden eines solchen Verfahrens auf einen gemeinsamen Schlüssel einigen, den sie dann über einen sicheren Weg austauschen müssen. Die Sicherheit des Verfahrens wird hierbei direkt von der Komplexität des vereinbarten Schlüssels beeinflusst, zum Beispiel von der Länge des gemeinsamen Kennworts. Je einfacher das Kennwort, desto leichter fällt es einem Angreifer, das Kennwort durch einfaches Durchprobieren zu erraten. Angreifer werden üblicherweise zunächst Kennworte mit einer hohen Trefferwahrscheinlichkeit ausprobieren, zum Beispiel Vor- und Nachnamen, Geburtsdaten oder naheliegende Kombinationen auf der Rechnertastatur wie »QWERT« oder »1234«.

Beim Einsatz von symmetrischen Verschlüsselungsverfahren müssen ausreichend komplexe Kennworte gewählt werden. Eine generelle Empfehlung ist schwierig zu treffen, weil die Umsetzung symmetrischer Verfahren sehr unterschiedlich ist. Generell sollten Kennworte jedoch nicht kürzer als zehn Zeichen sein und zumindest Zahlen, Groß- und Kleinbuchstaben sowie Sonderzeichen wie zum Beispiel ein Prozentzeichen oder ein Klammersymbol enthalten. Die Unsicherheit symmetrischer Verfahren nimmt mit der Zahl der beteiligten Kommunikationspartner zu – mit der Zahl der Beteiligten, die den gemeinsamen Schlüssel besitzen, steigt die Zahl der potentiellen Angriffspunkte des Kommunikationssystems.

Asymmetrische Verfahren verzichten auf den Austausch eines gemeinsamen Schlüssels. Stark vereinfacht gibt es in diesen Verfahren einen Schlüssel zum Verschlüsseln und einen Schlüssel zum Entschlüsseln. Der Schlüssel zum Entschlüsseln – »privater Schlüssel« genannt – verbleibt beim jeweiligen Besitzer. Der Schlüssel zum Verschlüsseln – »öffentlicher Schlüssel« genannt – kann frei verteilt werden.

Da es in der realen Welt kaum Beispiele für asymmetrisch verteilte Schlüssel und Schlösser gibt, fällt es vielen schwer, sich einen passenden Vergleich für dieses Verfahren vorzustellen. Vielleicht hilft folgende Ana-

logie: Man betrachte asymmetrische Verschlüsselung wie das Verteilen von Schatzkisten mit geöffneten Schnappschlössern. Die Schnappschlösser der Kisten lassen sich, wenn sie einmal geschlossen sind, nur mit dem Schlüssel wieder öffnen. Der Schlüssel zu den Schnappschlössern verbleibt jedoch beim Absender der Kisten (bzw. dem Empfänger der Nachrichten). Möchte nun jemand dem Absender der Schatzkisten eine geheime Nachricht zukommen lassen, so legt er diese in die Kiste und lässt das Schloss zuschnappen. Dann schickt er die Kiste zurück. Dieser Vergleich verdeutlicht das Prinzip asymmetrischer Verschlüsselung: »Einmal chiffrierte Nachrichten können nur mit dem privaten Schlüssel gelesen werden. Und der private Schlüssel verbleibt beim Absender.«

4 Verschlüsselung, Identifikation und Authentisierung

Bisher wurde der Einsatz kryptografischer Verfahren beim Ver- und Entschlüsseln von Nachrichten beschrieben. Wie oben bereits erwähnt, wird Kryptografie jedoch auch für andere Zwecke eingesetzt.

Kryptografische Verfahren dienen neben der Verschlüsselung vor allem zur Identifikation (von Benutzerinnen und Benutzern) oder Authentisierung (von Texten oder Daten). Ein Beispiel für den mehrfachen Nutzen eines kryptografischen Verfahrens ist des Protokoll für den verschlüsselten Zugriff auf Webseiten (→ *Secure Sockets Layer, SSL*). Dieses vielen Internetnutzenden über die »https«-Adressen bekannte Protokoll verschlüsselt in erster Linie die Daten bei der Übertragung zwischen Webserver und Internetnutzenden. Zusätzlich bietet es die Möglichkeit, die jeweiligen Kommunikationspartner zu authentifizieren. Im Normalfall weist der Anbieter einer Webseite seine Identität gegenüber den Benutzern nach (damit diese beispielsweise sicher gehen können, dass sie wirklich mit dem Webauftritt ihrer Bank kommunizieren und ihre PINs/TANs nicht anderen verraten). Aber auch der umgekehrte Fall, das Authentifizieren der Nutzerin oder des Nutzers gegenüber dem Webanbieter, ist möglich.

5 Voraussetzungen kryptografischer Verfahren

Für die meisten Verfahren ist eine Interaktion zwischen den Beteiligten notwendig, bevor der eigentliche Datenaustausch stattfinden kann. Entweder muss ein gemeinsames Geheimnis vereinbart werden, oder es müssen einzelne Teile des kryptografischen Verfahrens (zum Beispiel die

öffentlichen Schlüssel) ausgetauscht werden. Angriffe auf die Verschlüsselung richten sich aus diesem Grund häufig nicht gegen das kryptografische Verfahren selbst, sondern gegen die Begleitumstände des Verfahrens. Im einfachen Fall einer symmetrischen Verschlüsselung muss ein Angreifer dafür lediglich die Kommunikationspartner dazu bringen, ein auch ihm bekanntes Kennwort zu nutzen. Für symmetrische Verschlüsselungsverfahren war und ist dies der größte Angriffspunkt.

Asymmetrische Verfahren sind hier zunächst im Vorteil, weil der ausgetauschte öffentliche Schlüssel kein Geheimnis darstellt. Ein grundsätzliches Problem bleibt aber auch bei asymmetrischen Verfahren bestehen: Wie kann man sicherstellen, dass man wirklich den öffentlichen Schlüssel der Person besitzt, mit der man vertraulich kommunizieren möchte? Ist einem die Person seit langem persönlich bekannt, sollte man am besten den öffentlichen Schlüssel von Angesicht zu Angesicht austauschen. Ist dies nicht möglich, so müssen andere Wege gefunden werden, die Identität des Gegenübers sicherzustellen. In der fehlenden Authentisierung liegen aktuell die größten Defizite der gängigen Verfahren.

Dieses Angriffsszenario auf asymmetrische Verschlüsselungsverfahren soll an einem einfachen Beispiel verdeutlicht werden: Anton und Berta wollen ihre E-Mails in Zukunft vertraulich austauschen. Sie haben sich für die Software *Gnu Privacy Guard (GPG)* entschieden, ein quelloffenes, asymmetrisches Verfahren, das als relativ sicher gilt und für verschiedene Mailplattformen zur Verfügung steht. Damit Anton und Berta *GPG* nutzen können, müssen sie vorab ihre öffentlichen Schlüssel austauschen. Bei den Schlüsseldateien handelt es sich um kleine Textdateien – von denen die beiden annehmen, dass sie sich am einfachsten per E-Mail austauschen lassen, und sie verabreden, sich ihre Schlüsseldateien gegenseitig per E-Mail zuzusenden. Ein Angreifer Caesar, der möglicherweise von ihrem Vorhaben erfahren hat, könnte sich mit gefälschten E-Mails (Absendeadressen lassen sich problemlos ändern) gegenüber den beiden als der/die jeweils andere ausgeben und so an ihre öffentlichen Schlüssel gelangen. Zugleich würde er Anton einen anderen öffentlichen Schlüssel unterschieben, für den Caesar selbst das passende private Schlüsselpaar besitzt (und vice versa mit Berta). Hat er dies erreicht, so kann Caesar jede verschlüsselte Nachricht zwischen Anton und Berta entschlüsseln und dann (neu verschlüsselt) an den jeweiligen Empfänger weiterleiten, ohne dass die beiden etwas bemerken würden. Wie sich dieser Fehler in der Schlüsselverteilung vermeiden lässt, dazu gleich mehr.

6 Nutzen und Hindernisse

Für die symmetrische Verschlüsselung enthält zur Zeit fast jedes Programm im Bereich der automatisierten Datenverarbeitung mehr oder minder sichere Verfahren. Gängige Textverarbeitungsprogramme bieten die Möglichkeit, Texte mit einem Kennwort zu versehen. Viele Programme zum Verpacken und verlustfreien Verkleinern von Dateien – sogenannte Packer oder Entpacker – bieten die Möglichkeit, die beim Verpacken entstehenden Archive mit einem Kennwort zu versehen. Viele dieser Verfahren sind jedoch nicht im kryptografischen Sinne sicher. Es gibt bekannte Schwachstellen, die es einem Angreifer ermöglichen, das verwendete Kennwort zu entschlüsseln oder durch ein selbstgewähltes Kennwort zu ersetzen. Für den gelegentlichen Versand von Daten, die nicht einem erhöhten Schutzbedarf unterliegen, bietet jedoch beispielsweise der in einigen Packprogrammen verwendete Algorithmus namens *AES (Advanced Encryption Standard)* ein ausreichendes Schutzniveau, wenn ein hinreichend langes Kennwort genutzt wird.

Für Kommunikation mit erhöhtem Schutzbedarf haben sich die asymmetrischen Verfahren durchgesetzt. Wie das oben geschilderte Beispiel zeigt, beruhen deren Schwächen häufig nicht auf den zugrunde liegenden mathematischen Verfahren, sondern auf Fehlern, die vor der eigentlichen Anwendung des Verfahrens liegen, zum Beispiel bei der Schlüsselverteilung.

Für den Versand von E-Mails haben sich Verschlüsselungsverfahren wie *PGP (Pretty Good Privacy)*, *GPG* oder *OpenPGP* durchgesetzt. Sie bieten nach Ansicht der Entwickler »ziemlich gute Sicherheit« oder auf engl. »*pretty good privacy*«. Der wesentliche Erfolgsfaktor für den sicheren Einsatz ist hier wie bei allen asymmetrischen Verfahren der sichere Austausch der öffentlichen Schlüssel. Ein direkter Austausch, von Angesicht zu Angesicht, funktioniert nur mit einem begrenzten Personenkreis. Deshalb hat sich ein alternatives Modell für die Zuordnung von Personen zu öffentlichen Schlüsseln durchgesetzt: Dabei wird der öffentliche Schlüssel einer Person durch andere Personen kryptografisch unterschrieben (signiert). Als Grundregel gilt hier, dass man nur die öffentlichen Schlüssel von Personen unterschreibt, bei denen man sicher ist, dass diese wirklich der genannten Person gehören. Durch mehrere, sogar wechselseitige Unterschriften entsteht so ein »Netz des Vertrauens« oder (engl.) *web of trust*. Dieses Netzwerk versetzt den jeweiligen Absender in die Lage, aus der Anzahl der Unterschriften durch bereits vertraute Personen die Vertrauenswürdigkeit des öffentlichen Schlüssels eines neuen Adressaten nachzuvollziehen.

Für die sichere Identifikation von Webseitenbetreibern und anderen Internetanbietern haben sich Verfahren wie → *SSL* oder *TLS (Transport Layer Security)* durchgesetzt. Dabei geht es meist darum, die Identität eines Anbieters (etwa Mailprovider oder *Online*-Bank) nachprüfen zu können, damit sensible Daten nicht in falsche Hände gelangen. Das Vorgehen bei diesen Verfahren unterscheidet sich jedoch grundsätzlich vom *web-of-trust* bei *PGP*. Das »Unterschreiben« der Schlüssel erfolgt hier nicht durch eine Vielzahl unabhängiger Personen, sondern durch einige zentrale Stellen. Diese als besonders »vertrauenswürdig angesehenen Zertifizierungsstellen« (beispielsweise *Verisign, Comodo, StartCom, TC Trustcenter* und viele andere) bestätigen durch ihre mit kryptografischen Verfahren erstellten Zertifikate die korrekte Zuordnung eines öffentlichen Schlüssels zu einem Anbieter.

In der Praxis zeigt sich, dass die Identitätsprüfung im Internet auf wenige Stellen verlagert wurde, die sich der Kontrolle durch die Nutzerinnen und Nutzer größtenteils entziehen. Betrachtet man die in aktuellen Browsern bereits hinterlegten »vertrauenswürdigen Zertifizierungsstellen«, so stellt sich kritischen Anwendern durchaus die Frage, warum gerade diese Organisationen »vertrauenswürdig« sein sollen. Auch die Zertifizierungsstellen haben Sicherheitsprobleme durch technische Fehler oder fahrlässiges Verhalten. So wurde 2011 ein spektakulärer Einbruch in eine Zertifizierungsagentur bekannt, bei dem sich Angreifer bereits Wochen zuvor falsche Zertifikate für große Webdienstleister (unter anderem *Google-Mail*) beschafft und diese lange Zeit unbemerkt auf gefälschten Seiten eingesetzt hatten, bevor die Zertifikate öffentlich zurückgezogen wurden.[1]

Die Browser-Hersteller veröffentlichen zwar genaue Regeln, wann eine Organisation und deren Prozesse als vertrauenswürdig gelten und in die Software aufgenommen werden. Aber jede Nutzerin und jeder Nutzer muss sich darüber im Klaren sein, dass sich hier auch staatliche Zertifizierungsstellen wiederfinden, die bereits mehrfach durch massive Eingriffe in die Vertraulichkeit persönlicher Kommunikation aufgefallen sind. Ebenso kann für viele Zertifizierungsstellen nicht nachvollzogen werden, nach welchen Vorgaben und in welcher Güte die Identitätsprüfung durchgeführt wird. Vielfach reicht ein einfacher E-Mail-Kontakt aus. In Analysen über die ausgestellten Zertifikate wurden zahlreiche Fehler bei der Vergabe festgestellt. Mit wenig Aufwand kann es gelingen, durch das Vortäuschen einer falschen Identität unberechtigt ein Zertifikat zu erhalten und sich danach – von einer »vertrauenswürdigen Stelle« bestätigt – unter dieser falschen Identität auszuweisen.

In vielen aktuellen Browsern wird mit solchen Angriffen noch nicht korrekt umgegangen. So erkennen die Browser zum Beispiel nicht, dass sich ein Zertifikat geändert hat – und zeigen den Anwendern keine entsprechende Warnmeldung an. Gerade im Bereich des *Online-Bankings* und beim Kontakt mit Behörden sollte jede unangekündigte Änderung des Zertifikats misstrauisch betrachtet werden.

7 Sichere Identitätsbestimmung als Aufgabe künftiger kryptografischer Verfahren

Kryptografie ist eine der wesentlichen technischen Datenschutzmaßnahmen, um die Vertraulichkeit und Integrität von Kommunikation sicherzustellen. Die mathematischen Verfahren, die in den aktuellen Programmen genutzt werden, sind hinreichend sicher und können auch ein hohes Schutzniveau erreichen. Vielfach wird der Sicherheitsgewinn von Kryptografie jedoch durch schlechte Ausgangsvoraussetzungen, insbesondere eine mangelhafte Zuordnung der Schlüssel zu Kommunikationspartnern, unnötig verringert.

Nutzerinnen und Nutzer sollten deshalb bei sensiblen Daten die Verfahren mit Bedacht wählen und die Vertrauenswürdigkeit eines vorliegenden Schlüssels stets hinterfragen. Kommende Verfahren müssen für die Feststellung und Prüfung der Identität eines Schlüssel- bzw. Zertifikatsinhabers bessere Verfahren finden. Die Datenschutzbehörden des Bundes und der Länder sind im Zweifelsfall kompetente Ansprechpartner sowohl für Bürgerinnen und Bürger als auch für die öffentliche Verwaltung und die Privatwirtschaft, um das Schutzniveau eines Verschlüsselungsverfahrens und seiner Umsetzung zu bewerten.

Anmerkung

1 Ronald Eikenberg, Über 500 Zertifikate: Ausmaß des CA-Hacks schlimmer als erwartet, Heise Online vom 5.9.2011, im Internet unter http://heise.de/-1336603.

Angelika Martin

Datenschutzmanagement

Datenschutzmanagement ist eng mit der Art und Weise der technischen und organisatorischen Prozesse verknüpft, in der personenbezogene Daten auf informationstechnischen Systemen (IT-Systeme) verarbeitet werden. So wie sich die Systeme zur Speicherung, dem Transport und der Verarbeitung von Daten in den letzten dreißig Jahren verändert haben, ändern sich auch die Anforderungen an deren Verwaltung und an die Gestaltung von Datensicherheit. Wurden früher vornehmlich einzelne isolierte IT-Systeme verwaltet, sind heute größtenteils komplexe, heterogene und vernetzte IT-Systeme zu steuern und zu überwachen. Für einen reibungslosen Arbeitsablauf in Unternehmen und Behörden ist die fehlerfreie Funktion dieser Datenverarbeitungssysteme eine Grundvoraussetzung: Ohne funktionierende IT-Systeme sind viele Unternehmen und Behörden heutzutage nicht mehr handlungsfähig und ein größerer Systemausfall kann große finanzielle Schäden anrichten, im schlimmsten Fall kann er das Fortbestehen eines Unternehmens gefährden.

Aus diesem Grund entwickelte sich die eher maßnahmenorientierte Verwaltung einzelner Systeme zu einer prozessorientierten Verwaltung komplexer IT-Systeme. Die dafür international anerkannten und in der Praxis erprobten Vorgehensweisen werden als »IT-Management« bezeichnet. Werden dabei hauptsächlich die Risiken betrachtet, die für die IT-Systeme und durch die IT-Systeme entstehen, so spricht man vom »Informations-Sicherheits-Management« oder »IT-Sicherheits-Management«.

In der Anfangszeit war der betriebliche und behördliche Datenschutz von einzelfallbezogenen Stellungnahmen zu meist juristischen Fragen geprägt. Doch im Zuge der technischen Weiterentwicklung mussten sich Datenschützer immer stärker mit aufbau- und ablauforganisatorischen Organisationsstrukturen beschäftigen. Heutiger Datenschutz bedeutet, dass die Arbeitsabläufe zur Verarbeitung personenbezogener Daten auch im technisch-organisatorischen Umfeld aktiv mitgestaltet werden, um eine datenschutzkonforme Datenverarbeitung zu gewährleisten. Denn genauso wie IT-Systemausfälle für Unternehmen und Behörden zu einer existentiellen Bedrohung werden können, können auch Fehler und Versäumnisse bei der Verarbeitung personenbezogener Daten erhebliche Schäden hervorrufen.

Die Sensibilität der Bevölkerung ist in Bezug auf Themen des Datenschutzes und der Datensicherheit in den letzten Jahren gestiegen. Datenschutzverstöße können zu einem großen Verlust an Vertrauen und Ansehen führen, aber auch zu empfindlichen Geldstrafen. Die Einführung eines Datenschutzmanagements, das sich an den Prozessen zur Verarbeitung von personenbezogenen Daten orientiert, ist eine wesentliche Voraussetzung, um solchen Fällen vorzubeugen.

1 Was bedeutet Datenschutzmanagement?

In seinem Volkszählungsurteil vom 15. Dezember 1983 hat das Bundesverfassungsgericht ein Grundrecht auf informationelle Selbstbestimmung begründet (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.). Es gewährt das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Aufgabe des Datenschutzes ist es, die Rechte des Einzelnen bei der Verarbeitung seiner personenbezogenen Daten zu schützen.

Datenschutzmanagement betrachtet die Verarbeitung von personenbezogenen Daten in ihrem technischen und organisatorischen Zusammenhang. Es beschreibt einen Prozess des datenschutzkonformen Umgangs mit personenbezogenen Daten in Unternehmen und Behörden – ausgehend von der Zielbestimmung über die Durchsetzung und Problembehandlung bis hin zur Erfolgskontrolle. Das Ziel des Datenschutzmanagements besteht darin, datenschutzgerechte Verarbeitungsregeln nachhaltig in die bestehende Aufbau- und Ablauforganisation einzubinden. Datenschutzmanagement ist eine Leitungsaufgabe.

2 Die Einführung von Datenschutzmanagement – ein Praxisszenario

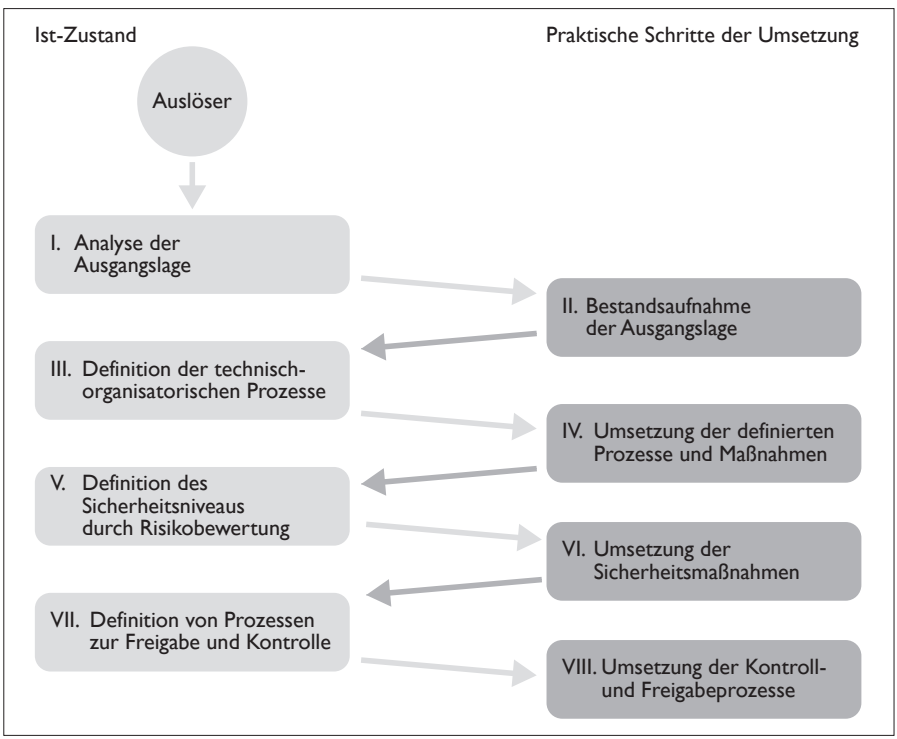
Es sind vielfache Szenarien denkbar, die das Einführen eines Datenschutzmanagements auslösen können. So kann es beispielsweise in einer Organisation zu einem Datenschutzvorfall kommen: Ein Mitarbeiter hat etwa Zugriff auf Personaldaten seiner Kollegen erhalten, da diese sensiblen Daten nicht ausreichend vor unberechtigten Zugriffen geschützt wurden. Die Vertraulichkeit dieser Daten ist nun nicht mehr gewährleistet.

Möchte diese Organisation oder Behörde nun Konzepte für ein effektives Datenschutzmanagement entwickeln, so muss sie die über die Zeit

gewachsene Technikausstattung und die bisherigen technisch-organisatorischen Abläufe berücksichtigen. Auch die vorhandenen Erfahrungswerte mit positiven oder negativen technisch-organisatorischen Regelungen beziehungsweise effektiven oder ineffektiven Arbeitsabläufen sollten für die weitere Planung berücksichtigt werden.

Die folgende Vorgehensweise beschreibt in acht Schritten die Einbindung von Datenschutzmanagement in ein bestehendes System. Nach dem Abarbeiten aller Schritte sind die technisch-organisatorischen Maßnahmen für eine datenschutzkonforme Datenverarbeitung in Form von definierten Arbeitsschritten in die Ablauforganisation eingebunden und dokumentiert. Die acht Schritte sind so gestaltet, dass nach deren Umsetzung eine datenschutzkonforme Dokumentation der eingesetzten IT-Systeme vorliegt, die dem Datenschutzmanagement als Grundlage dient.

Abb. 1: Gesamtprozess der Einführung von Datenschutzmanagement



Eigene Darstellung.

Die vier Schritte auf der linken Seite repräsentieren als *strategische Schritte* den Ist-Zustand des Datenschutzmanagements in der Organisation. In diesen Phasen wird analysiert, werden Strategien festgelegt und Entscheidungen getroffen. Die vier Schritte auf der rechten Seite repräsentieren als *praktische Schritte* die Umsetzung, das *Doing*. Die Ergebnisse jeder Phase werden dokumentiert und bilden die Grundlage für den jeweils nächsten Schritt. So wächst schrittweise eine Dokumentation heran, die den jeweiligen Stand des Datenschutzmanagements und den technisch-organisatorischen Status des IT-Systems wiedergibt.

Nachfolgend werden die strategischen Schritte zur Einführung eines Datenschutzmanagements vorgestellt; die praktischen Schritte ergeben sich aus den jeweils in ihnen erreichten Ergebnissen und Arbeitsaufträgen.

Analyse der Ausgangslage

Nachdem der Gesamtprozess zunächst durch ein bestimmtes Ereignis ausgelöst wird – etwa durch einen Datenschutzvorfall in der datenverarbeitenden Stelle –, werden im ersten Schritt zunächst der Auslöser und die Ausgangslage analysiert. Datenschutz ist eine Führungsaufgabe, daher sollte die erste richtungweisende Sitzung ebenso wie die weiteren strategischen Schritte durch die Leitung eines Unternehmens oder einer Behörde veranlasst werden. Datenschutz betrifft nicht nur die IT-Beschäftigten und den Datenschutzbeauftragten. Deshalb sind alle Verantwortlichen daran zu beteiligen, die mit Hilfe von IT-Systemen Daten verarbeiten. Das können beispielsweise die Verfahrensverantwortlichen sein, also diejenigen Personen, die etwa für die Verarbeitung von Personal- bzw. Finanzdaten verantwortlich sind. Datenschutzmanagement wird nicht nur von einzelnen Personen eingeführt, sondern durch ein Team von Mitarbeitenden, das das Unternehmen oder die Behörde repräsentiert.

Das Ziel des ersten Schrittes ist die gemeinsame Erfassung und Beschreibung der Aufgabe: Was bedeutet die Integration des Datenschutzmanagements in alle technischen und organisatorischen Arbeitsabläufe für unsere Organisation?

Als Vorbereitung für den nächsten Schritt werden Arbeitsaufträge zur Bestandsaufnahme sowohl der IT-Systeme, der Dokumentation als auch der technisch-organisatorischen Regelungen erstellt, schriftlich festgehalten, die ausführenden Personen benannt und ein Zeitpunkt für die nächste strategische Sitzung benannt, zu der die Ergebnisse der Bestandsaufnahme vorliegen sollen.

Definition der technisch-organisatorischen Prozesse

Die Ergebnisse der Bestandsaufnahme (Ist-Zustand) werden nun aufbau- und ablauforganisatorisch daraufhin analysiert, ob und in welchem Umfang datenschutzkonforme Maßnahmen berücksichtigt wurden.

Das Bundes- und die Landesdatenschutzgesetze verweisen auf die Gestaltung der innerbetrieblichen bzw. innerbehördlichen Organisation durch technische und organisatorische Maßnahmen, die geeignet sind, die Rechte des Einzelnen bei der Verarbeitung seiner personenbezogenen Daten zu schützen. An diesen Gestaltungsvorgaben muss sich ein effizientes Datenschutzmanagement messen lassen. So fordert beispielsweise §9 Satz 1 Bundesdatenschutzgesetz (BDSG) in Verbindung mit der Anlage zu §9 BDSG technische und organisatorische Maßnahmen zur Gewährleistung der

- Zutritts-, Zugangs- und Zugriffskontrolle: Nur berechtigte Personen dürfen die Räume mit den IT-Systemen betreten (Zutritt), die IT-Systeme verwenden (Zugang) und nur auf die für sie freigegebenen Daten auf den IT-Systemen zugreifen (Zugriff).
- Weitergabekontrolle: Daten, die an andere Stellen weitergegeben werden, dürfen auf ihrem Transport nicht unbefugt zur Kenntnis genommen bzw. verarbeitet werden.
- Eingabekontrolle: Es ist (auch nachträglich) nachvollziehbar, wer wann welche personenbezogenen Daten auf den IT-Systemen verarbeitet hat (zum Beispiel mit Hilfe von Protokollierungsfunktionen).
- Auftragskontrolle: Eine Datenverarbeitung im Auftrag wird nur entsprechend der Weisungen des Auftragsgebers durchgeführt.
- Verfügbarkeitskontrolle: Die personenbezogenen Daten sind gegen Verlust oder zufällige Zerstörung geschützt (zum Beispiel mit Hilfe einer geeigneten Datensicherung).
- Zwecktrennung: Personenbezogene Daten, die zu einem bestimmten Zweck gespeichert werden (etwa Mitarbeiterdaten zur Lohnabrechnung), dürfen nicht zu einem anderen Zweck verwendet werden.

Werden diese in der Anlage zu §9 BDSG aufgeführten Maßnahmen aus der Sicht des Datenschutzmanagements (mit Zielbeschreibung, Durchsetzung, Problembehandlung bis hin zur Erfolgskontrolle) betrachtet, dann müssen zusätzliche Maßnahmen berücksichtigt werden, die nicht explizit im Gesetz genannt sind, sich aber als Folgerung daraus ableiten lassen:

- Dokumentation: Die definierten technischen und organisatorischen Maßnahmen werden in Form einer Sicherheitsdokumentation schriftlich festgehalten. Diese definiert das Sicherheitsniveau der Organisation

oder Behörde und bildet als Soll-Zustand die Grundlage bei Datensicherheits- und Datenschutzüberprüfungen (Zielbeschreibung).
- Zuweisung von Verantwortlichkeiten: Für die IT-Systeme und IT-Verfahren werden Verantwortliche benannt, die sicherstellen, dass in ihrem Verantwortungsbereich die definierten Maßnahmen umgesetzt werden (Durchsetzung).
- Transparenz: Die Mitarbeiterinnen und Mitarbeiter werden in einer geeigneten Form (Betriebs-/Dienstanweisung, Schulung, Intranet usw.) über die Maßnahmen informiert und in Bezug auf ihren Anwendungsbereich sensibilisiert.
- Erfolgskontrolle: Die technischen und organisatorischen Maßnahmen werden regelmäßig daraufhin überprüft, ob sie eingehalten werden. Bei Problemen werden die Maßnahmen in Form einer Qualitätssicherung im technischen und/oder organisatorischen Bereich überarbeitet.

Das Land Schleswig-Holstein regelt beispielsweise in der Landesverordnung über die Sicherheit und Ordnungsmäßigkeit automatisierter Verarbeitung personenbezogener Daten (Datenschutzverordnung, DSVO) in Verbindung mit dem Landesdatenschutzgesetz Schleswig-Holstein (LDSG SH) die Dokumentation automatisierter Verfahren bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen. Sie beschreibt die Anforderungen an eine datenschutzkonforme Dokumentation anschaulich in drei Kapiteln: Verfahrensdokumentation, Dokumentation der Sicherheitsmaßnahmen sowie Dokumentation des Tests und der Freigabe. Das Datenschutzmanagement wird im § 4 Absatz 6 DSVO explizit erwähnt.

Auf Grundlage dieser Analyse kann ein Soll-Zustand in Bezug auf den Einsatz der IT-Technik und einer datenschutzkonformen Gestaltung der technisch-organisatorischen Prozesse definiert werden. Bei dieser Bewertung sollten nicht nur die einzelnen Komponenten für sich allein betrachtet werden. Vielmehr ist auch zu berücksichtigen, dass alle Maßnahmen im Resultat eine strukturierte und transparente Gesamtheit ergeben. So genügt es beispielsweise nicht, administrativen Mitarbeiterinnen und Mitarbeitern die Aufgabe zuzuweisen, Nutzungsberechtigungen innerhalb der IT-Systeme zu vergeben, wenn nicht der vorangehende Prozess geregelt ist. Dieser sollte beschreiben, wer dafür verantwortlich ist, Benutzerinnen und Benutzern die notwendigen Berechtigungen im System zu gewähren (zum Beispiel die Abteilungs- oder Referatsleitung), und auf welche Weise die Beschäftigten der IT-Administration die Anweisung zur Berechtigungsvergabe erhalten (etwa auf Papier oder in einem Ticketsystem).

Definition des Sicherheitsniveaus durch Risikobewertung

Im Anschluss daran wird auf der Grundlage des Soll-Zustands ein Sicherheitsniveau für das Unternehmen oder die Behörde definiert. Mit Hilfe einer Risikobewertung werden einzelne Risiken, die das entsprechende Sicherheitsniveau beeinträchtigen können, identifiziert, klassifiziert und geeignete Maßnahmen zur Vermeidung dieser Risiken erarbeitet. So bildet beispielsweise eine zu hohe Temperatur im Serverraum ein Risiko, das die Verfügbarkeit der Daten auf den Servern gefährden kann. Als technische Maßnahme könnte festgelegt werden, dass im Serverraum eine Klimaanlage zu installieren ist oder dass die Beschäftigten der IT-Administration mit Hilfe eines Temperatursensors über einen eventuellen Temperaturanstieg informiert werden und dadurch in der Lage sind, das Problem durch kontrolliertes Herunterfahren der Server zu lösen (organisatorische Maßnahme).

Manchen Risiken lässt sich nicht mit angemessenen technischen oder organisatorischen Maßnahmen begegnen. Da auch in diesem Fall das Sicherheitsniveau nicht aufrechterhalten werden kann, werden diese Risiken in einer Restrisikobeschreibung aufgeführt. So wird beispielsweise ein Rohrbruch der Wasserleitung, die durch den Serverraum führt, die Verfügbarkeit der Daten auf den Servern gefährden. Es kann jedoch keine Maßnahme erarbeitet werden, die geeignet ist, umfassende Sicherheit in diesem Bereich zu gewährleisten. Dieser Umstand wird daher als Restrisiko schriftlich in der Restrisikobeschreibung festgehalten.

Für das Datenschutzmanagement ist es wichtig, dass nicht nur die Risiken im Voraus betrachtet, sondern dass auch Prozesse entwickelt werden, die dann zum Einsatz kommen, wenn es zu unvorhergesehenen »Notfällen« kommt – mit welchen Maßnahmen beispielsweise einem »Hackerangriff« entgegenwirkt werden soll. Für den Fall, dass tatsächlich der Verdacht besteht, angegriffen zu werden, ist ein Notfallprozess definiert, der beschreibt, wer wie zu benachrichtigen ist und welche Maßnahmen in welcher Reihenfolge abgearbeitet werden sollen. Somit sollte jedes Risiko, das im Rahmen der Risikobewertung betrachtet wird, daraufhin überprüft werden, inwieweit ein Notfallprozess für diesen Bereich sinnvoll ist.

Definition von Prozessen zur Freigabe und Kontrolle

Die Ergebnisse aus den vorhergehenden Schritten liefern den dokumentierten Soll-Zustand der IT-Technik, die datenschutzkonformen technisch-organisatorischen Prozesse und das definierte Sicherheitsniveau mit den entsprechenden Maßnahmen.

Was jetzt noch fehlt und in diesem Schritt erarbeitet wird, sind die Prozeduren, wie dieses System und diese Maßnahmen auf ihre Wirksamkeit getestet werden können, wer für die Freigabe des IT-Systems mit den Datenschutzmanagement-Komponenten verantwortlich ist, in welchen Zeitintervallen die Prozesse und Maßnahmen überprüft werden und welche Auslöser eine Überprüfung von Datenschutzmanagement-Prozessen bewirken. So kann beispielsweise festgelegt werden, dass einmal jährlich die bestehende Dokumentation auf ihre Transparenz und Aktualität überprüft wird oder dass Notfallprozesse in gewissen Zeitabständen geübt werden. Ziel ist es dabei, das Datenschutzmanagement nachhaltig in die Arbeitsabläufe zu integrieren.

Sind all diese Aufgaben abgearbeitet und dokumentiert, können das Gesamtsystem und die Datenschutzmanagement-Prozesse durch die verantwortliche Person freigegeben werden.

3 Lebendiges Datenschutzmanagement

Bei der Betrachtung der oben genannten Schritte und Fragestellungen sollte das Ziel des Datenschutzmanagements im Auge behalten werden: den Prozess zum datenschutzkonformen Umgang mit personenbezogenen Daten in Unternehmen und Behörden nachhaltig in die bestehende Aufbau- und Ablauforganisation zu integrieren.

Es genügt nicht, den Prozess zur Einführung von Datenschutzmanagement einmalig zu durchlaufen, um danach in die »alten« Arbeitsabläufe zurückzufallen und die neu definierten Prozesse zu vernachlässigen. Wichtig ist, dass die Datenschutzmanagement-Prozesse zur Gewohnheit und von allen Beschäftigten unterstützt werden. Dazu ist es notwendig, dass die Mitarbeiterinnen und Mitarbeiter von Anfang an über das Datenschutzmanagement informiert sind und an dem Entstehungsprozess beteiligt werden. Bei ihnen sollte nicht das Gefühl entstehen, dass über ihre Köpfe hinweg entschieden wird. Wenn die Mitarbeiterinnen und Mitarbeiter das Datenschutzmanagement »von unten« unterlaufen, da sie den Nutzen der Maßnahmen nicht nachvollziehen können, wird das Datenschutzmanagement als Ganzes nicht erfolgreich sein. Notfallprozesse können beispielsweise nur dann abgearbeitet werden, wenn die Beschäftigten diesen »Notfall« erkennen, ihn entsprechend bewerten und die definierten Maßnahmen ergreifen.

Auch wenn es wichtig ist, dass bei der Einführung von Datenschutzmanagement ein Mitarbeiterteam bei der Gestaltung der Prozesse und

Maßnahmen beteiligt wird, so ist es notwendig, dass es eine verantwortliche Person gibt. Sie koordiniert den Datenschutzmanagement-Prozess, gibt ihm eine einheitliche Richtung, informiert die Beschäftigten über die Fortschritte, steht nach Einführung als Ansprechperson sowohl den Beschäftigten als auch der Leitung zur Verfügung und sollte daher über die geeignete Fachkunde und Zuverlässigkeit verfügen.

4 Datenschutzmanagement nach nationalen und internationalen Standards

Die Weiterentwicklung des betrieblichen oder behördlichen Datenschutzes zum Datenschutzmanagement ist keine rein deutsche oder europäische Angelegenheit. Nach vielen nationalen und internationalen Standards zur Informationssicherheit finden sich konkrete Anforderungen und Vorgaben für die Einrichtung eines Datenschutzmanagements. Der von der Internationalen Organisation für Normung (*International Organization for Standardization,* →ISO) veröffentlichte Standard für das Informations-Sicherheits-Management (ISO 27 001) enthält zahlreiche Datenschutzvorgaben (siehe auch den Beitrag von Körner in diesem Band, S. 426 ff.).

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein mit den internationalen Vorgaben der ISO 27 001 vergleichbares Vorgehen unter dem Namen »IT-Grundschutz« entwickelt. Auch hier finden sich in vielen Maßnahmen direkte Anforderungen zum Datenschutz.

Beispielsweise formuliert die Maßnahme Nummer 2 110 Anforderungen an den Umgang mit Protokolldaten und die Einbettung in die betriebliche oder behördliche Mitbestimmung: »Personal- bzw. Betriebsräte sollten bei der Erarbeitung des Revisionskonzeptes und bei der Festlegung der Auswertungsmöglichkeiten der Protokolle beteiligt werden.«

Die Landesbeauftragten und der Bundesbeauftragte für den Datenschutz bieten eine für den Bereich des Bundesdatenschutzgesetzes anwendbare Sammlung von Prozess- und Maßnahmenvorgaben für den Aufbau eines Datenschutzmanagements innerhalb der Vorgehensweise des BSI an. Der sogenannte »Baustein Datenschutz« kann auf den Webseiten des BSI heruntergeladen werden.

5 Datenschutz als Gestaltungsaufgabe

Datenschutzmanagement bedeutet mehr als das reine Abarbeiten von Checklisten, denn es begreift Datenschutz als eine Gestaltungsaufgabe. Datenschutzmanagement bedeutet, die Prozesse zur Verarbeitung personenbezogener Daten rechtskonform zu gestalten und die Transparenz und Nachvollziehbarkeit für die Betroffenen bei der Verarbeitung ihrer Daten sicherzustellen. Die Leitung eines Unternehmens und einer Behörde muss hierfür die Initiative ergreifen und die Verantwortung übernehmen. Betriebliche und behördliche Datenschutzbeauftragte müssen an der Ausgestaltung aufbau- und ablauforganisatorischer Prozesse frühzeitig beteiligt werden und aktiv an der Verbesserung des Datenschutzniveaus mitwirken. Erst durch regelmäßige und anlassbezogene Kontrollen und festgelegte Vorgehensweisen im Fall von Datenschutzvorfällen entfaltet Datenschutz die notwendige »Tiefenwirkung«.

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.

Hielke Hijmans / Owe Langfeldt

Datenschutz in der Europäischen Union

Dieser Beitrag gibt einen Überblick über die Entwicklung und den aktuellen Stand des Datenschutzes auf europäischer Ebene.[1] Außerdem wird die aktuelle Diskussion um eine Überarbeitung des europäischen Rechtsrahmens für den Datenschutz vorgestellt.

1 Die Entwicklung des Europäischen Datenschutzes: Vom Ursprung bis zum Vertrag von Lissabon

Der Ursprung: Übereinkommen Nr. 108 des Europarats im Jahr 1981

Der Ursprung des Europäischen Datenschutzes liegt beim Europarat, nicht bei der Europäischen Union (EU). Der Europarat ist eine europaweite zwischenstaatliche Organisation mit Sitz in Straßburg. Ihm gehören 47 Mitglieder an, darunter Russland und die Türkei. Die im Europarat entwickelten Datenschutz-Grundsätze wurden später auf die EU übertragen.

Das Übereinkommen Nr. 108 des Europarats »zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten« vom 28. Januar 1981 ist die primäre Quelle des Datenschutzes in der EU. Es gilt als allgemein anerkannter Mindeststandard für den europäischen Datenschutz und regelt die Datenspeicherung und -verarbeitung im öffentlichen wie im privaten Bereich. Das Übereinkommen wurde 2001 mit einem Zusatzprotokoll zu Kontrollstellen und zum grenzüberschreitenden Datenaustausch ergänzt. Zusätzlich wurden Empfehlungen zu Fragen der polizeilichen Nutzung persönlicher Daten (1987) ausgearbeitet. Als sich die EU eigene Rechtsvorschriften zum Datenschutz gab, bezog sie sich hauptsächlich auf dieses Übereinkommen.

Eine weitere Quelle des EU-Datenschutzes ist die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte zu Artikel 8 der Europäischen Menschenrechtskonvention (EMRK), der das Privatleben schützt. Das Gericht gab mit seinen Entscheidungen wichtige Impulse für die Entwicklung europäischer Datenschutzstandards, unter anderem mit der Feststellung, dass auch öffentliche und frei zugängliche Daten bei systematischer Sammlung und Speicherung unzulässig in die Persönlichkeitsrechte

eingreifen können[2] oder dem Verbot einer Speicherung biometrischer Merkmale von Freigesprochenen.[3]

Beginn des EU-Datenschutzes: Die Richtlinie 95/46/EG aus dem Jahr 1995 und der Binnenmarkt

Die EU führte Mitte der 1990er Jahre einen Rechtsrahmen für den Datenschutz ein. Die Richtlinie 95/46/EG »zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr« vom 24. Oktober 1995 ist bis heute das zentrale Element der Datenschutzvorschriften auf Unionsebene und bildet das Fundament des Datenschutzrechts in den 27 Mitgliedstaaten der EU.

Die EU-Datenschutzrichtlinie verfolgt zwei Ziele: Sie soll im Rahmen des gemeinsamen Binnenmarktes den freien Datenverkehr innerhalb der EU gewährleisten und dabei zugleich die Grundrechte der Bürgerinnen und Bürger wahren. Für den Grundrechtsschutz baut die Richtlinie auf den Standards des oben beschriebenen Europarats-Übereinkommens Nr. 108 auf. Ihr Geltungsbereich hat jedoch zwei wesentliche Einschränkungen: Die Datenschutz-Richtlinie gilt nicht für den Polizei- und Justizbereich sowie die Gemeinsame Außen- und Sicherheitspolitik der Union. Außerdem gilt sie nicht für ausschließlich persönliche und familiäre Tätigkeiten. Die Reichweite dieser Ausnahmen ist nicht immer offensichtlich. Mit Verweis auf die erste Einschränkung hat der Europäische Gerichtshof entschieden, dass die Datenschutz-Richtlinie nicht auf die Übermittlung personenbezogener Fluggastdaten (*Passenger Name Record, PNR*) durch Fluggesellschaften an die Vereinigten Staaten anwendbar ist.[4] Diese Daten seien dem Bereich der polizeilichen Zusammenarbeit zuzuordnen, auch wenn sie von privaten Unternehmen im Rahmen ihrer Dienstleistungen erhoben wurden.

Generell hat das EU-System des Datenschutzes nach Auslegung des Gerichtshofs einen weiten Anwendungsbereich: Es ist auch anzuwenden, wenn nicht-sensible Daten verarbeitet werden und die betroffene Person tatsächlich nicht geschädigt wird. Trotz des ursprünglichen Binnenmarktbezugs ist es auch auf nicht-kommerzielle Aktivitäten anwendbar. Es ist ein ausgewogenes System, das die Verarbeitung personenbezogener Daten nicht verbietet, sondern unter bestimmten Voraussetzungen und Schutzmaßnahmen zulässt.

Die Richtlinie richtete mit der → Artikel-29-Gruppe eine Arbeitsgruppe der Datenschutzbehörden der Mitgliedsstaaten ein, der inzwischen auch der Europäische Datenschutzbeauftragte (EDSB) angehört. Diese Gruppe koordiniert die Aktivitäten ihrer Mitglieder, um ein einheitlich hohes Schutzniveau zu gewährleisten, und berät die Europäische Kommission.

Neben der allgemeinen Datenschutzrichtlinie gibt es spezielle Regelungen für den Bereich der Telekommunikation (2002/58/EG). Die im November 2009 überarbeitete Datenschutzrichtlinie für elektronische Kommunikation konkretisiert die Regeln in Bereichen der Sicherheit und Vertraulichkeit der Kommunikation, der Speicherung von Verkehrs- und Standortdaten sowie Spam (RL 2009/136/EG). Sie sieht beispielsweise vor, dass Verletzungen des Schutzes personenbezogener Daten gemeldet werden müssen.

Als Ausnahme zu der dort festgeschriebenen Verpflichtung, Verkehrs- und Standortdaten zu löschen, sieht die Richtlinie über die → Vorratsspeicherung von Daten der elektronischen Kommunikation (RL 2006/24/EG) vor, dass gewisse Verbindungsdaten gespeichert werden müssen, damit sie zum Zwecke der Ermittlung, Feststellung und Verfolgung von schweren Straftaten zur Verfügung stehen. In mehreren Mitgliedsstaaten wurden die Gesetze, die diese heftig kritisierte Richtlinie umsetzten, von den Verfassungsgerichten verworfen, so auch in Deutschland (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.).

Datenschutz innerhalb der EU-Organe: Verordnung (EG) Nr. 45/2001

Die Richtlinie 95/46/EG richtet sich an die Mitgliedsstaaten. Sie kann auf die Organe der EU selbst – wie die Kommission, den Ministerrat und das Europäische Parlament – nicht angewendet werden. Für eine Datenschutzkontrolle dieser Organe war eine andere Rechtsgrundlage erforderlich. Diese wurde mit dem 1997 unterzeichneten Vertrag von Amsterdam geschaffen, der 1999 in Kraft trat (Artikel 286 EG-Vertrag). Der neue Vertrag sah zusätzlich die Errichtung einer unabhängigen Europäischen Behörde für den Datenschutz vor. Auf seiner Grundlage wurde im Jahr 2000 die Verordnung (EG) Nr. 45/2001[5] erlassen, die Datenschutzvorschriften für die Organe selbst schuf und den Europäischen Datenschutzbeauftragten (EDSB) einführte. Die Bereiche Polizei und Justiz waren bis zum Inkrafttreten des Vertrags von Lissabon am 1. Dezember 2009 von ihrem Geltungsbereich ausgenommen.

Der EDSB nahm seine Arbeit 2004 auf. Er ist für die Aufsicht über die Verarbeitung personenbezogener Daten durch Organe und Einrichtungen der EU zuständig und berät die Kommission bei neuen Vorschlägen mit Auswirkungen auf den Datenschutz. Außerdem koordiniert er seine Arbeit mit den nationalen Datenschutzbehörden, unter anderem in der oben erwähnten Artikel-29-Gruppe, um ein einheitliches Schutzniveau zu gewährleisten.

Polizei- und Justizkooperation: Ein nur teilweise harmonisierter Flickenteppich

Im Bereich der polizeilichen und justiziellen Zusammenarbeit (der früheren »Dritten Säule« des EU-Vertrags) ähnelt der Datenschutz in der EU einem Flickenteppich: Es gibt verschiedene Rechtsakte und nicht in allen Mitgliedstaaten gelten dieselben Rechtsvorschriften; in einigen Fällen ist nicht klar, welches Datenschutzsystem anzuwenden ist, so dass die Rechtssicherheit nicht umfassend gewährleistet ist.

Alle Mitgliedstaaten sind an das Übereinkommen Nr. 108 des Europarats gebunden, wonach sie zu Datenschutzvorschriften für den Polizei- und Justizbereich verpflichtet werden. Viele Mitgliedsstaaten haben sich dafür entschieden, den Geltungsbereich ihres nationalen Rechts, mit dem sie die Richtlinie 95/46/EG umsetzen, so zu erweitern, dass es den Polizei- und Justizbereich einschließt. Andere Mitgliedstaaten haben spezielle Rechtsvorschriften für diesen Bereich geschaffen.

Zusätzlich mussten die EU-Mitgliedsstaaten bis zum 27. November 2010 den Rahmenbeschluss 2008/977/JI des Rates, den ersten allgemeinen EU-Rechtsakt in diesem Bereich, umsetzen. Er beschränkt sich allerdings auf den Informationsaustausch zwischen den Mitgliedstaaten, gilt also weder für die innerstaatliche Datenverarbeitung noch für die Verarbeitung durch →Europol und Eurojust.[6] Schließlich gewährleistet er ein geringeres Schutzniveau als die Richtlinie 95/46/EG.

Daneben gibt es spezielle Bestimmungen zum Datenschutz in Rechtsakten, deren Hauptzweck ein anderer ist. Zum Beispiel enthält das – ursprünglich außerhalb des EU-Rechts stehende – Schengener Durchführungsübereinkommen von 1990 ein entsprechendes Kapitel, das auf den Bestimmungen des Übereinkommens Nr. 108 aufbaut. Europol (gegründet 1995) und Eurojust (gegründet 2002) haben ebenfalls eigene Regelungen zum Datenschutz. In diesen drei Fällen wurden sogenannte gemeinsame Kontrollinstanzen geschaffen, in denen die Verarbeitung personenbezogener Daten auf europäischer Ebene gemeinsam durch unabhängige einzelstaatliche Behörden überwacht wird.

Weiterhin gibt es neue spezielle Formen der polizeilichen Kooperation, die den Datenaustausch zwischen den Behörden der Mitgliedstaaten ohne ein Zentralsystem oder eine Zentralstelle auf europäischer Ebene regeln. Ein Beispiel hierfür ist der »Prümer Beschluss«[7], der den Austausch von →DNA-Profilen, Fingerabdrücken und Fahrzeugregisterdaten erlaubt.

2 Datenschutz als Grundrecht in der EU

Entwicklung zu einem allgemeinen Anliegen

Im Laufe der Jahre wurde der Datenschutz zunehmend als allgemeines Anliegen der EU anerkannt. Er ist kein reines Binnenmarktthema mehr, wie die – wenn auch nicht ausreichenden – Regeln im Bereich der Polizei- und Justizkooperation zeigen. Selbst in der Gemeinsamen Außen- und Sicherheitspolitik spielt der Datenschutz eine Rolle. Dort gibt es zwar keine Rechtsvorschriften, Fragen der Verarbeitung personenbezogener Daten wurden aber in mehreren Urteilen des Europäischen Gerichtshofs zu Terroristenlisten angesprochen.

Artikel 8 (»Schutz personenbezogener Daten«) der im Jahr 2000 verabschiedeten Charta der Grundrechte der Europäischen Union führt die Grundprinzipien des Datenschutzes auf:

- Personenbezogene Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke verarbeitet werden.
- Grundlage der Verarbeitung muss die Einwilligung der betroffenen Person oder eine sonstige gesetzlich geregelte legitime Grundlage sein.
- Die betroffene Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
- Eine unabhängige Stelle soll die Einhaltung dieser Vorschriften überwachen.

Dieser Artikel ist das sichtbarste Beispiel für die Rolle des Datenschutzes als Grundrecht in der EU.

Der Vertrag von Lissabon 2009: Bestätigung und Stärkung des allgemeinen Anliegens

Der am 1. Dezember 2009 in Kraft getretene Vertrag von Lissabon brachte bedeutende Änderungen für den Datenschutz. Am wichtigsten sind die drei folgenden:

- Die Charta der Grundrechte der EU, die vorher nur deklaratorischen Charakter hatte, ist jetzt rechtlich bindend sowohl für die EU selbst als auch für die Mitgliedsstaaten. Dies stärkt den Datenschutz als Grundrecht. Der Vertrag sieht außerdem vor, dass die EU der EMRK beitreten soll, was allerdings noch einige Zeit dauern wird.
- Er schafft die »Säulenstruktur« des bisherigen EU-Vertrags, das heißt die Aufteilung in verschiedene Rechtsgrundlagen für die verschie-

denen Politikbereiche (Binnenmarkt, Außen- und Sicherheitspolitik, Justiz und Innen) ab. Diese Struktur funktionierte nicht und führte immer wieder zu Problemen, etwa bei der oben erwähnten Nutzung der Datenbestände von Privatunternehmen für Zwecke der Strafverfolgung. Zudem hatte das Europäische Parlament in der Säulenstruktur im Bereich der justiziellen und polizeilichen Zusammenarbeit nur eine beratende Funktion, was zu intransparenten und demokratisch nicht ausreichend legitimierten Entscheidungsprozessen führte.

- Der neue Vertrag führt mit Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) eine allgemeine Bestimmung zum Datenschutz ein. Dieser als zentrale Rechtsgrundlage des Datenschutzes in der EU gedachte Artikel sieht vor, dass das Europäische Parlament und der Rat Vorschriften über den Datenschutz erlassen müssen. Er hat allgemeine Geltung: sowohl im privaten als auch im öffentlichen Sektor (polizeiliche und justizielle Zusammenarbeit eingeschlossen). Artikel 16 AEUV bestätigt, dass der Datenschutz jetzt ein allgemeines Anliegen ist. Zusätzlich gibt er jeder natürlichen Person ein subjektives Recht auf Datenschutz. Es ist allerdings noch nicht geklärt, ob Personen direkt unter Berufung auf dieses Recht vor Gericht gehen können, oder ob sie sich auf die Rechtsvorschriften verlassen müssen, mit denen dieses Recht umgesetzt wird.

In der Praxis sind die Folgen der mit dem Vertrag von Lissabon eingeleiteten Reform der EU ziemlich kompliziert. Trotz der Abschaffung der Säulenstruktur gilt die Richtlinie 95/46/EG beispielsweise nicht automatisch für den Bereich Polizei und Justiz. Ihr Geltungsbereich wird nämlich durch Artikel 3 Absatz 2 der Richtlinie beschränkt, der unter anderem die Tätigkeiten des Staates im Bereich des Strafrechts ausschließt.

Eine weitere Komplikation ergibt sich aus den Übergangsbestimmungen des Vertrags von Lissabon. Alle Rechtsakte, die vor seinem Inkrafttreten angenommen wurden, bleiben solange gültig, bis sie aufgehoben, für nichtig erklärt oder geändert werden. Alte Rechtsvorschriften gelten also weiterhin, auch wenn sie die Kriterien des Artikels 16 AEUV gegebenenfalls nicht erfüllen. Ein Beispiel hierfür ist der Rahmenbeschluss 2008/977/JI, der vom Rat allein angenommen wurde und nicht auf die Datenverarbeitung innerhalb der Mitgliedsstaaten anwendbar ist.

3 Auf dem Weg zu einem umfassenden Rechtsrahmen

Ein neuer, umfassender Rechtsrahmen für den Datenschutz innerhalb der EU ist also dringend nötig. Erste Schritte in diese Richtung hat die Kommission bereits vor dem Inkrafttreten des Vertrags von Lissabon mit einer offenen Konsultation zur Überarbeitung der Datenschutzrichtlinie unternommen.[8] Zu ihr haben die europäischen Datenschutzbehörden eine Stellungnahme mit dem Titel »Die Zukunft des Datenschutzes«[9] abgegeben. Sie stellen klar, dass die wichtigsten Grundsätze des Datenschutzes ungeachtet neuer Technologien und der Globalisierung weiterhin gelten werden. Ihre Stellungnahme enthält zudem eine Wunschliste für die Zukunft, in der unter anderem die Einführung neuer Grundsätze – etwa technisch »eingebauter Datenschutz« (siehe auch den Beitrag von Schaar in diesem Band, S. 363 ff.) und »Rechenschaftspflicht« –, eine Begrenzung des bürokratischen Aufwands und die Schaffung eines wirklich umfassenden Rechtsrahmens für den Datenschutz gefordert werden.

Die Kommission hat im November 2010 eine Mitteilung über das Gesamtkonzept für den Datenschutz in der EU veröffentlicht[10], in der sie mehrere Anregungen der Datenschutzbehörden – etwa zum »eingebauten Datenschutz« – übernommen hat. Weitere Hauptpunkte sind eine weitere Harmonisierung der Datenschutzgesetze in den Mitgliedsstaaten, ein »Recht auf Vergessen«, eine Stärkung der Unabhängigkeit der Datenschutzbehörden, bessere Regelungen für Datentransfers in Drittstaaten und schließlich die Prüfung der Aufnahme der Polizei- und Justizkooperation in den allgemeinen Rahmen.

Im Januar 2012 hat die Kommission ihr Paket zur Reform des EU-Datenschutzrahmens vorgestellt. Dieses Paket beinhaltet Vorschläge für eine Datenschutzgrundverordnung[11] und für eine Richtlinie für den Bereich der Strafverfolgung.[12] Mittels der Rechtsform einer direkt anwendbaren Verordnung würde dieser erste Vorschlag einen europaweit einheitlichen Rahmen für die Privatwirtschaft und weite Teile des öffentlichen Sektors schaffen. Der Vorschlag für eine Richtlinie blieb hingegen hinter den in ihn gesetzten Erwartungen zurück. Sowohl der EDSB[13], als auch die Artikel-29-Gruppe[14] und mehrere nationale Datenschutzbehörden haben umfangreiche Stellungnahmen zu diesen Vorschlägen abgegeben.

In der weiteren Diskussion stellen sich noch zahlreiche wichtige Fragen, zum Beispiel: Wie kann in einer globalisierten Welt mit starken Akteuren, die ihre Basis außerhalb der EU haben, ein wirksamer Datenschutz gewährleistet werden? Welche Regeln sollen für die Nutzung der Daten-

bestände von Privatunternehmen zu Zwecken der Strafverfolgung gelten, etwa bei der Nutzung von Fluggastdaten? Wie kann eine einheitliche Auslegung des Rechtsrahmens mit der Unabhängigkeit der Datenschutzbehörden vereinbart werden? Wie kann das Verhältnis zwischen einer EU-Verordnung und dem in föderalen Mitgliedsstaaten auf verschiedenen Ebenen bestehenden Datenschutzrecht geregelt werden?

Anmerkungen

1 Einen Überblick über und Zugang zu allen genannten Rechtsgrundlagen des europäischen Datenschutzes bietet die Webseite des Europäischen Datenschutzbeauftragten, im Internet unter http://www.edps.europa.eu/EDPSWEB/edps/cache/off/lang/de/EDPS/Dataprotection/Legislation.

2 Europäischer Gerichtshof für Menschenrechte, Fall »Rotaru vs. Rumänien«. Urteil vom 4.5.2000 (28341/95).

3 Europäischer Gerichtshof für Menschenrechte, Fall »S. und Marper vs. Vereinigtes Königreich«, Urteil vom 4.12.2008 (30562/04 u. 30566/04).

4 Europäischer Gerichtshof, Fall »Europäisches Parlament vs. Rat der Europäischen Union«, Urteil vom 30.5.2006 (C-317/04 u. C-318/04), im Internet unter http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=DE&Submit=rechercher&numaff=C-317/04.

5 Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr.

6 Europäische Einheit für justizielle Zusammenarbeit, eine Justizbehörde der Europäischen Union mit Sitz in Den Haag. Sie wurde 2002 aufgrund eines Beschlusses des Rates der EU begründet und soll den Informationsaustausch zwischen den Justizbehörden der Mitgliedsstaaten erleichtern sowie grenzüberschreitende Strafverfahren im Bereich der organisierten Kriminalität (z. B. Terrorismus, Waffenhandel, Drogenhandel, Menschenhandel und Geldwäsche) koordinieren.

7 Rat der Europäischen Union, Beschluss 2008/615/JI des Rates vom 23.6.2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, im Internet unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:210:0001:0011:de:PDF.

8 European Commission: Review of the data protection legal framework, im Internet unter http://ec.europa.eu/justice/newsroom/data-protection/opinion/090501_en.htm.

9 Artikel-29-Datenschutzgruppe/Arbeitsgruppe Polizei und Justiz, Die Zukunft des Datenschutzes. Gemeinsamer Beitrag zu der Konsultation der Europäischen Kom-

mission zu dem Rechtsrahmen für das Grundrecht auf den Schutz personenbezogener Daten vom 1.12.2009 (WP 168), im Internet unter http://www.bfdi.bund.de/SharedDocs/Publikationen/Art29Gruppe/WP168_de.pdf.

10 Europäische Kommission, Gesamtkonzept für den Datenschutz in der Europäischen Union. Mitteilung vom 4.11.2010 – KOM(2010) 609 endgültig, im Internet unter http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_de.pdf.

11 Vorschlag für Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM 2012(11) endgültig, im Internet unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:HTML.

12 Vorschlag für Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, KOM 2012(10) endgültig, im Internet unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:DE:HTML.

13 Stellungnahme des Europäischen Datenschutzbeauftragten zu dem Paket von Vorschlägen für eine Datenschutzreform, im Internet unter http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_DE.pdf.

14 Artikel-29-Gruppe, Opinion 01/2012 on the data protection reform proposals, WP191, im Internet unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf.

Lars Reppesgaard

Global Players: Die großen Internetunternehmen betrachten den Datenschutz eher als Geschäftshindernis

Für Marc Zuckerberg, den Gründer des →sozialen Netzwerks *Facebook*, ist das, was seine Firma tut, völlig harmlos. Er bietet seiner Ansicht nach nur eine technische Plattform für das an, was die Menschen ohnehin tun: Sie wollen Informationen austauschen – offen und ohne alle Grenzen. »Die soziale Norm ist einfach etwas, das sich über die Jahre verändert hat. Wir sehen es als unsere Aufgabe im System an, fortwährend innovativ zu sein und darüber zu informieren, was unser System ist, um widerzuspiegeln, welches die aktuellen sozialen Normen sind«, erklärte er im Rahmen einer Technologiekonferenz im Januar 2010. »Die Leute finden es angenehm, nicht nur Informationen und andere Dinge zu teilen, sondern dies auch stärker öffentlich und mit einer größeren Anzahl von Menschen zu tun.«[1]

Die Aussage, dass *Facebook* lediglich auf einer technischen Ebene gesellschaftliche Veränderungen nachvollzieht, blieb nicht lange unwidersprochen. »Ich kaufe Zuckerberg das Argument nicht ab, dass *Facebook* nun lediglich die Veränderungen widerspiegelt, die die Gesellschaft durchgemacht hat«, antwortete etwa der Technologiejournalist Marshall Kirkpatrick. »Ich denke, *Facebook* selbst ist eine wesentliche Ursache sozialer Veränderungen.«[2]

1 Wie die globalen *Player* die Welt prägen

Dass eine Netzplattform wie *Facebook*, über die weltweit 901 Millionen aktive Nutzerinnen und Nutzer (Stand: März 2012[3]) Informationen und Bilder austauschen, das Kommunikationsverhalten ganzer Generationen prägt, ist unter Fachleuten in der Tat unstrittig. Eine ähnliche Wirkungsmacht haben auch andere globale *Player*, die das Geschäft mit der Vernetzung und der Digitalisierung dominieren: der Suchmaschinenriese *Google*, dessen Netzdienste jeden Tag milliardenfach genutzt werden; *Microsoft*, dessen Software auf mehreren hundert Millionen Computern der Welt läuft; *Apple* mit seinen Lifestyle-Produkten, aber

auch der Internetbuchhandel *Amazon*. Sie alle prägen das Leben in der *Offline*-Welt.

»Wie und was Menschen kommunizieren, wer wen wann erreichen kann, wann und wo konsumiert wird und – im kritischen Fall – wer Stimmen zensieren kann – all das hängt davon ab, wie die dominanten Internetkonzerne ihre Verantwortung begreifen« schreibt der Journalist Johannes Boie. »Was eine Firma wie *Google* heute beschließt, wird tags darauf zum gesellschaftlichen Parameter.«[4]

Die große Frage ist dabei: Versuchen die globalen Player auch aktiv, zu beeinflussen, was die Nutzer als normal empfinden? Versuchen sie, Standards, etwa im Bereich des Datenschutzes und der Privatsphäre, zu Ungunsten der Benutzer ihrer Dienste zu beeinflussen? Vieles deutet darauf hin.

2 Warum die globalen *Player* den Mythos vom Ende der Privatsphäre verbreiten

Dass Zuckerberg die eigene Rolle bei weltweiten Veränderungsprozessen herunter spielt, ist kein Zufall, sondern gehört zur Kommunikationsstrategie. Auch die führenden Köpfe in Unternehmen wie *Google, Apple, Microsoft* oder *Amazon* reden regelmäßig die Einflussmöglichkeiten ihrer eigenen Unternehmen klein – unter anderem, um zu verhindern, dass Regulierungsbehörden sich ihr Treiben genauer ansehen und womöglich eingreifen. Vor allem wenn es um Themen wie Datenschutz und Privatsphäre geht, tun die mächtigsten Akteure in der Technologiewelt außerdem so, als bliebe ihnen keine andere Wahl, als einer Entwicklung zu folgen, von der sie behaupten, dass sie natürlich sei.

Scott McNealy, der damalige Chef des Konzerns *Sun Microsystems*, wurde etwa schon im Jahr 2000 mit der Aussage zitiert: »Die Privatsphäre ist tot. Kommen Sie darüber hinweg.«[5] Larry Ellison, Gründer des Softwareunternehmens *Oracle*, erklärte wenig später: »Die Privatsphäre, über die Sie sich Sorgen machen, ist größtenteils Illusion. Alles, was sie tun müssen, ist, Ihre Illusion aufzugeben.«[6]

Datenschutz wird in der Regel wahlweise innovationshemmend, überflüssig, als Konzept von gestern oder gar als Zensurwerkzeug dargestellt. Als führende Köpfe der Industrie kommen die Manager von *Apple, Google, Facebook* und Co. regelmäßig öffentlich zu Wort – und prägen den Diskurs so in ihrem Sinne; etwa, indem sie permanent dafür werben, dass in diesem Bereich Selbstverpflichtungen sinnvoller als strikte gesetzliche Regelungen sind. *Google*-Chef Eric Schmidt beispielsweise betont, »dass

es wichtig ist, dass wir neue Regeln für die Privatsphäre entwickeln, um die zunehmend transparente Welt, die heute *online* entsteht, zu verwalten.« Im gleichen Atemzug ergänzt er aber: »Mit neuen Regeln meine ich nicht neue Gesetze.«[7]

Ein kleiner Kreis von Technologie-Entscheidern möchte am liebsten im Alleingang für den Rest der Welt definieren, wie man die Technologie, die sie in die Welt gesetzt haben, zu benutzen hat. Schließlich zahlt es sich für die Vertreter der globalen *Player* aus, wenn die Nutzenden der Dienste glauben, dass es sich ohnehin nicht mehr lohnt, sich über Datenschutz und Privatsphäre Gedanken zu machen. »Informationen stellen den eigentlichen Wert des Internets dar, man muss sich nur geschickt in die Datenströme des Internets einklinken, um mit den Informationen Anderer Milliardenumsätze zu machen«, erklärt der Buchautor und Internet-Unternehmer Ibrahim Evsan.[8]

Das Prinzip gilt für die Buch-, Musik- und Filmvorlieben der *Facebook*-Nutzenden, die das Unternehmen an die Werbeindustrie verkauft, ebenso wie für *Amazons* Buchempfehlungsfunktion, die darauf beruht, dass vergangene Käufe ausgewertet werden, oder für *Googles* profitable *Online*-Werbedienste, die nur funktionieren, weil das Unternehmen jedem Surfer bei jedem Klick genau über die Schulter schaut und sie aufzeichnet. »Im Spiel der Internetgiganten ist der Anwender nicht mehr als Manövriermasse. Er ist Lieferant der Daten, mit denen die Anbieter heute und in Zukunft ihre Geschäfte machen«, schreibt der Wirtschaftsinformatiker und Berater Thomas R. Köhler.[9]

3 Wie mit *Privacy Policies* gespielt wird

Doch globale *Player* wie *Facebook* belassen es nicht nur dabei, das Geschäft mit den Daten verbal voran zu bringen. Vor allem über ihre *Privacy Policies* – die Regelwerke, in denen Firmen darlegen, welche Daten sie sammeln und wie sie mit ihnen umgehen – treiben viele Netzunternehmen den Wandel voran: weg von einer Gesellschaft, in der informationelle Selbstbestimmung die Norm ist, hin zu einer, in der es Menschen als normal empfinden, dass ihre Daten und Informationen über sie nach Gutdünken ökonomisch verwertet werden. Abgesehen davon, dass viele Nutzungsbedingungen (englisch: *Policies*) unverständlich formuliert sind und nicht über wesentliche Aspekte der Datensammlung und -verarbeitung informieren,[10] werden die Regelwerke regelmäßig überarbeitet – und zwar oft nicht im Sinne des Datenschutzes. »Betrachtet man die Entwick-

lung der vergangenen Jahre, so kann man festhalten, dass sich bezogen auf den Umgang mit Nutzerdaten immer die gleichen Muster wiederholen: Man versucht erst einmal relativ freizügig mit den Angaben umzugehen oder gerne auch mal neue Tatsachen zu schaffen«, schreibt Köhler. »Dies geschieht entweder ganz simpel durch technische Maßnahmen oder durch neue Nutzungsbedingungen. Wer liest denn schon das Kleingedruckte?«[11]

Wer verfolgt, wie sich das Kleingedruckte verändert hat, auf das sich etwa *Facebook* beim Umgang mit den Nutzerdaten verpflichtet, erkennt, wie radikal sich die Geschäftsgrundlage verändert hat, auf die sich die Netznutzenden bei der erstmaligen Nutzung eines Dienstes verlassen haben. Binnen fünf Jahren wurden die Aussagen der *Privacy Policy* völlig umgekehrt. 2005 hieß es noch, dass »keinerlei persönliche Daten«, die nicht zu einer selbst in den *Privacy Settings* definierten Gruppe gehören, allgemein zugänglich veröffentlicht werden. 2006 wurden die Standardeinstellungen dahingehend verändert, dass sich »die Informationen, die angezeigt werden, auf deine Schule, deinen von dir spezifizierten Ort und andere angemessene Begrenzungen der Gemeinschaft, die *wir* (Hervorhebung des Autors) dir mitteilen« begrenzen. Binnen eines Jahres hatte *Facebook* die Kontrolle darüber übernommen, was Nutzende als normal und angemessen im Umgang mit ihren Daten zu halten haben.

2007 gab es eine neue *Policy*, laut der »Dein Name, der Name Deiner Schule und Dein Profilbild« im Rahmen der Suchfunktion im gesamten *Facebook*-Netzwerk auffindbar waren, »es sei denn, Du änderst Deine *Privacy Settings*.« Im Dezember 2009 teilte *Facebook* mit: »Bestimmte Kategorien von Informationen, wie zum Beispiel Dein Name, Dein Profilfoto, Deine Freundeliste und Seiten, von denen Du Fan bist, Geschlecht, Herkunftsregion und Netzwerke, zu denen Du gehörst, werden als öffentliche Informationen für jedermann – dies schließt *Facebook* ergänzende Applikationen ein – betrachtet und haben daher keine *Privacy Settings*.«

Manuell ließen und lassen sich die *Settings* zwar bearbeiten, doch es ist angesichts der zeitweise mehr als 170 Einstellungsmöglichkeiten, die die *New York Times* im Mai 2010 zählte,[12] unwahrscheinlich, dass viele Nutzende die Dienste optimal in ihrem Sinne einstellen. Faktisch definierte *Facebook* in den letzten Jahren so nach Gutdünken, in welcher Weise Millionen von Nutzenden persönliche Informationen anderen zugänglich machen.

Damit das Geschäft mit den Nutzerdaten geschmiert läuft, hat *Facebook* die Grenze dessen, was das Unternehmen als die Norm in Sachen Datenschutz und Privatsphäre betrachtet, bewusst und aktiv in den letzten Jahren verschoben. Den gleichen Trend hat Professor Hendrik Speck von der Fachhochschule Kaiserslautern auch bei vielen anderen Netzunternehmen beob-

achtet. »Plattformen setzen dabei auf die Trägheit und auf die Unkenntnis der Nutzer, um ohne explizite Zustimmung, quasi durch die Hintertür, erweiterte Vermarktungsrechte durchzuführen. Plattformen führen dabei einseitig neue Verwertungsformen ein und verweisen auf die in diversen Menüs versteckten Ab-/Einstellmöglichkeiten für die Nutzer, in Wirklichkeit geht es jedoch um eine zielgerichtete Aushöhlung eines Grundpfeilers der informationellen Selbstbestimmung. Dieser Trend steht somit dem klassischen Verständnis des Datenschutzes diametral entgegen.«[13]

4 Warum der Datenschutz trotzdem Chancen hat

Wenn staatliche Stellen versuchen, bei den Netzriesen zu intervenieren, stoßen sie oft auf zähen Widerstand. Die Europäische Union drängt etwa seit Jahren darauf, dass Suchmaschinen ihren Datenhunger ein wenig zügeln. Die → Artikel-29-Gruppe, in der Datenschutzbeauftragte aus 27 europäischen Ländern zusammengeschlossen sind und die Datenschutzregelungen für die EU erarbeitet (siehe auch den Beitrag von Hijmans/Langfeldt in diesem Band, S. 403 ff.), rang 2007 *Google* das Zugeständnis ab, → *Cookies* nur noch zwei Jahre zu speichern und nicht mehr wie bis dato pauschal bis zum Jahr 2038. 2008 forderten sie *Google, Microsoft* und *Yahoo!* auf, spätestens nach sechs Monaten die Informationen der Nutzenden, die bei der Websuche anfallen – inklusive der → IP-Adressen – kompromisslos zu löschen. Bis 2008 speicherte *Google* alle gesammelten Daten zwei Jahre lang. Nach dem Druck der Datenschützer erklärte sich das Unternehmen bereit, Daten nach neun Monaten zu anonymisieren. Gelöscht werden sie nach wie vor nicht. *Google* erklärt, dass es ansonsten nicht möglich wäre, weiterhin gute Suchergebnisse zu liefern und andere Dienste weiterzuentwickeln. *Yahoo!* weigert sich mit ähnlichen Begründungen ebenfalls, die Auflagen zu erfüllen. 2010 mahnten die Datenschützer die Suchmaschinenbetreiber erneut ab.[14]

Microsoft hat als Betreiber der Suchmaschine *Bing* dagegen angekündigt, den Vorgaben Folge zu leisten. »Wir werden sämtliche Internet-Protokoll-Adressen, die mit Suchanfragen in Verbindung stehen, nun nach sechs Monaten löschen – und nicht länger nach 18 Monaten«, schrieb *Microsofts* Datenschutzmann Peter Cullen im Firmenblog.[15]

Zwei Entwicklungen, die *Microsoft* zu diesem Schritt bewegt haben, zeigen Perspektiven auf, wie globale Player trotz aller Widerstände dazu gebracht werden können, wenigstens ein Mindestmaß an Datenschutz-Regelungen zu akzeptieren. Zum einen bietet eine proaktive datenschutz-

freundliche Unternehmenspolitik inzwischen wegen der größeren öffentlichen Sensibilität gegenüber Datenschutzfragen oft eine Chance, sich positiv von Wettbewerbern abzuheben. Zum anderen verriet ein *Microsoft*-Manager gegenüber der *New York Times*, was der Konzern am meisten fürchtet: eine gesetzliche Regulierung der Datenspeicherung durch die EU.[16] Gesetzlichen Maßnahmen wollte *Microsoft* auf jeden Fall zuvorkommen.

Die Kombination aus einer wachen Netznutzer-Gemeinschaft, die sich nicht alles gefallen lässt, und Datenschutzinstitutionen sowie politischen Entscheidern, die notfalls die Daumenschrauben anziehen, könnte eine Formel sein, die selbst hartgesottene Technikvisionäre bei den *global Players* nachdenklich machen könnte.

Anmerkungen

1 Marshall Kirkpatrick, *Facebook's* Zuckerberg Says The Age of Privacy is Over, ReadWriteWeb vom 9.1.2010, im Internet unter http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php.
2 S. Anm. 1, a. a. O.
3 Quelle: *Facebook* Unternehmensseite, im Internet abrufbar unter http://newsroom.fb.com/content/default.aspx?NewsAreaId=22.
4 Johannes Boie, Die Menschenfischer, in: Süddeutsche Zeitung vom 13.2.2010, im Internet unter http://www.sueddeutsche.de/digital/facebook-und-google-die-menschenfischer-1.54914.
5 Zitiert nach Brock N. Meeks, Is privacy possible in the digital age? MSNBC vom 7.12.2000, im Internet unter http://www.msnbc.msn.com/id/3078854/.
6 Jane Black, Don't Make Privacy the Next Victim of Terror, Business week v. 4.10.2001, im Internet unter http://www.businessweek.com/bwdaily/dnflash/oct2001/nf2001104_7412.htm.
7 Lars Reppesgaard, Das *Google*-Imperium, Hamburg 2010, S. 148.
8 Ibrahim Evsan, Der Fixierungscode, München 2009, S. 104.
9 Thomas R. Köhler. Die Internetfalle: Was wir online unbewusst über uns preisgeben und wie wir das WorldWideWeb für uns nutzen können, Frankfurt/M. 2010, S. 141.
10 Alastair R. Beresford/Dorothea Kübler/Sören Preibusch, Unwillingness to Pay for Privacy, A Field Experiment, Discussion Paper Nr. 5017, Institut zur Zukunft der Arbeit (IZA), Berlin, Juni 2010.
11 Köhler 2010 (Anm. 9), S. 140f.
12 Guilbert Gates, *Facebook* Privacy, A Bewildering Tangle of Options, New York Times vom 12.5.2010, im Internet unter http://www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html.
13 Hendrik Speck, Mehr Profildaten verfügbar als zu Stasi-Zeiten (Gastbeitrag), deutsche-startups.de vom 27.2.2008, im Internet unter http://www.deutsche-startups.

de/2008/02/27/gastbeitrag-von-prof-hendrik-speck-mehr-profildaten-verfuegbar-als-zustasi-zeiten/.

14 Article 29 Data Protection Working Party, »EU data protection group says *Google*, Microsoft and Yahoo! do not comply with data protection rules«, Pressemitteilung der Artikel-29-Gruppe vom 26.5.2010, Brüssel.

15 Peter Cullen, Microsoft Advances Search Privacy with Bing, Microsoft on the Issues vom 19.1.2010, im Internet unter http://blogs.technet.com/b/microsoft_on_the_issues/archive/2010/01/19/microsoft-advances-search-privacy-with-bing.aspx.

16 Kevin J. O'Brien, Microsoft Puts a Time Limit on Bing Data, New York Times vom 19.1.2010, im Internet unter http://www.nytimes.com/2010/01/20/technology/companies/20search.html.

Thilo Weichert

Datenschutz und Überwachung in ausgewählten Staaten

Für die Europäische Union (EU) setzt die europäische Datenschutzrichtlinie Mindeststandards. Innerhalb der EU besteht nach der Anpassung des nationalen Rechts an diese Richtlinie ein in vieler Hinsicht übereinstimmendes Datenschutzniveau. Auch in einigen außereuropäischen Staaten besteht ein solches Schutzniveau, zum Beispiel in Kanada oder in Australien. Dies gilt aber nicht für den größten Teil der Welt, insbesondere nicht für die Vereinigten Staaten von Amerika (USA). Mit den USA praktiziert Europa einen regen Austausch personenbezogener Daten, etwa im Rahmen von Wirtschaftsbeziehungen oder zum Zweck der Terrorismusbekämpfung.

Der weltweite Handel und die Kommunikation über das Internet eröffnen den Austausch mit allen Staaten in der Welt. Für einen effektiven Datenschutz ist daher von Bedeutung, wie der Schutz vor Überwachung bzw. die informationelle Selbstbestimmung in anderen Ländern gewährleistet werden.

Datenschutz ist im internationalen Recht bisher nur unzureichend verankert; die Datenschutzkonvention des Europarates von 1981 ist bisher die am weitesten gehende völkerrechtliche Regelung (siehe auch die Beiträge von Hijmans/Langfeldt, S. 403 ff. und Körner, S. 426 ff. in diesem Band). Die Konvention ratifizierten auch Staaten außerhalb Europas. Die USA, China und der Iran gehören jedoch nicht dazu. Deren Datenschutzregeln und -praxis sollen im Folgenden dargestellt werden, weil sie politisch wie ökonomisch bedeutsam sind und zudem unterschiedliche Kulturkreise repräsentieren.

1 Vereinigte Staaten von Amerika (USA)

Die USA sind das Beispiel einer exzessiven Überwachungsgesellschaft, die zugleich über eine hoch entwickelte Kultur der Meinungs- und Pressefreiheit verfügt. Ein Paradox? Informationelle Kontrolle über die eigenen Daten wird in diesem Land offiziell als nicht wesentlich zur Wahrnehmung der eigenen Freiheitsrechte angesehen. Andererseits gehört es zum amerikanischen Freiheitsverständnis, dass es weder eine staatliche Meldepflicht noch eine verpflichtende Identitätskarte gibt. In einer Daten-

schutzrangliste der Nichtregierungsorganisation → *Privacy International* im Jahr 2007 landeten die USA weit abgeschlagen im Feld der »endemischen[1] Überwachungsgesellschaften« in Nachbarschaft zu wenig demokratischen Staaten wie Russland oder Singapur.

Dabei wurden die Grundlagen des modernen Datenschutzes in den USA 1890 durch die beiden US-amerikanischen Juristen Samuel Warren und Louis Brandeis mit ihrem wegweisenden Artikel »Das Recht auf Privatheit« gelegt (siehe auch die Literaturhinweise im Anhang dieses Bandes, S. 444 ff.). 1967 entwickelte Alan F. Westin in seinem Buch »Privacy and Freedom« die später vom deutschen Bundesverfassungsgericht aufgegriffene Idee der »informationellen Selbstbestimmung«. Die rechtlichen Regelungen, die noch in den 1970er Jahren in den USA ähnliche Ansätze verfolgten wie in Europa, entwickelten sich danach massiv auseinander.

Ende der 1970er Jahre begann in den USA unter den Vorzeichen eines »Krieges gegen Drogen« der Abbau von informationellen Freiheitsrechten, der später mit dem »Krieg gegen Terrorismus« seine Fortsetzung und Verstärkung finden sollte. Zwar gab es vereinzelte rechtliche Restriktionen bei Eingriffen in die Privatsphäre, insbesondere durch staatliche Stellen und Behörden. Jedoch wurde daraus bis heute kein umfassendes, in sich stimmiges Datenschutzrecht entwickelt. Geschuldet ist dies nicht zuletzt der Rechtsprechung des Obersten Gerichtes (*Supreme Court*), das – anders als das deutsche Bundesverfassungsgericht – polizeilichen und sonstigen behördlichen Überwachungsmaßnahmen und Eingriffen stetig weniger enge Grenzen setzte.

Einen starken Schub hin zu mehr staatlicher Überwachung brachte die Reaktion auf die terroristischen Anschläge vom 11. September 2001. Deren Kernstück ist der *Patriot Act*, der Sicherheitsbehörden weitgehende Befugnisse zur heimlichen und anlasslosen Kontrolle von Menschen gibt, die in einen Zusammenhang mit dem Terrorismus gebracht werden. Die Kontrollmanie wurde mit dem Projekt der »*Total Information Awareness*« auf die Spitze getrieben. Das Projekt strebte eine nahezu vollständige informationelle Kontrolle der Gesellschaft an. Es wurde vor allem aus Kostengründen jedoch wieder aufgegeben. Dennoch wird eine →DNA-Datenbank mit vielen Millionen Einträgen immer weiter ausgebaut. In einer offiziellen Anti-Terror-Liste sind über 400 000 Personen gespeichert. Diese Liste ist Teil eines Datenbanksystems des *National Security Branch Analysis Center*[2] mit 1,5 Milliarden Einträgen. Im Januar 2008 hat die US-Bundespolizeibehörde FBI (*Federal Bureau of Investigation*) eine in zehn Jahren aufzubauende Biometrie-Datenbank in Auftrag gegeben, in der Fingerabdrücke und weitere körperliche Merkmale gespeichert werden sollen. Auch EU-Bürgerinnen und -Bürger sind beispielsweise durch die Sammlung von

Fluggastdaten (*Passenger Name Records*) oder die Kontrolle internationaler Bank-Transaktionsdaten des Dienstleisters → SWIFT (*Society for worldwide Interbank Telecommunication*) betroffen.

In Kontinentaleuropa schützt das Recht auf informationelle Selbstbestimmung nicht nur die Privat- und Intimsphäre, sondern auch die sogenannte Sozial- und Öffentlichkeitssphäre der Menschen vor den Folgen der elektronischen Datenverarbeitung. Das US-Recht kennt diesen Ansatz nicht. Danach ist personenbezogene Datenverarbeitung grundsätzlich erlaubt, nicht verboten. Persönliche Daten sind Gemeinschaftsgut, über das der Staat wie auch private Unternehmen verfügen können, wenn dies nicht im Einzelfall aus triftigem Grund untersagt wird. Das Verbergen von Persönlichem wird als unsozial und verdächtig angesehen. Ein generelles Verbot personenbezogener Datenverarbeitung würde als Eingriff in die staatliche Organisationshoheit bzw. in die wirtschaftliche Betätigungsfreiheit eines Unternehmens angesehen. Rechtliche Beschränkungen werden regelmäßig erst bei tatsächlichen Diskriminierungen eingeführt. Das die Freiheit gefährdende Potenzial von Überwachung (siehe auch den Beitrag von Papier in diesem Band, S. 67 ff.) findet nur wenig Aufmerksamkeit, selbst bei sehr persönlichen Angelegenheiten.

So sehr in den USA der Grundsatz der Informations- und Pressefreiheit, also der öffentlichen Transparenz anerkannt wird, so wenig gilt dies für die personenbezogene Datenverarbeitung. Für sie kennt das US-amerikanische Rechtssystem keine allgemeinen Auskunftsrechte, Intransparenz und Geheimhaltung sind bei der Datenverarbeitung in der Verwaltung wie in der Privatwirtschaft der Regelfall. So klagte die Bürgerrechtsorganisation *American Civil Liberties Union (ACLU)* im Namen von zehn offensichtlich völlig unschuldigen Personen gegen das Heimatschutzministerium, weil dieses Auskünfte darüber verweigerte, ob und wie Betroffene auf einer → *No-Fly*-Liste registriert sind. Der Staat gewährt Datenschutz allenfalls beschränkt als Verbraucherschutz, zum Beispiel durch die Verbraucherschutzbehörde *Federal Trade Commission*. Wie wenig dieses System funktioniert, zeigt das zwischen den USA und der EU verabredete → *Safe-Harbor*-Abkommen. Es bietet keine effektive Kontrolle des Datenschutzes in US-Unternehmen, die Daten aus der Europäischen Union verarbeiten.

Dennoch gibt es in den USA eine starke Bewegung für mehr Datenschutz. Diese hat ihren Ursprung in Bürgerrechtsorganisationen und wissenschaftlichen Kreisen. Inzwischen fordern selbst IT-Unternehmen bessere Datenschutzregeln im Interesse ihrer Kundschaft, erste Gesetzesinitiativen wurden auf den Weg gebracht. Die strukturellen Defizite des US-amerikanischen Datenschutzes werden jedoch nicht so schnell behoben sein.

2 China

China hat keinen modernen Datenschutz und erst recht keinen Schutz der Privatsphäre. Die chinesische Kultur, die Praxis von Wirtschaft, Verwaltung und Politik sind autoritär strukturiert und gewähren kaum individuelle Rechte. Die Privatsphäre wie politische Freiheiten, insbesondere die Meinungsfreiheit, werden massiv unterdrückt.

In China gibt es circa 400 Millionen Internetnutzende und damit weltweit die größte Internetgemeinschaft. Diese will die Regierung umfassend unter Kontrolle halten. Die Politik des Landes zielt darauf ab, die anonyme Netznutzung zurückzudrängen, alle Nutzerinnen und Nutzer zu identifizieren und ihre Aktivitäten im Netz zu überwachen. Datenschutz, verstanden als Bürgerschutz, scheint hinderlich.

Das öffentliche Zurschaustellen von mutmaßlichen oder verurteilten Kriminellen und Systemgegnern hat Tradition; derartige Demütigungen finden heute auch im Internet statt. Sie führen immer wieder dazu, dass Betroffene von einem aufgehetzten Mob verfolgt und verprügelt werden.

So wenig Urheberrechte in China ein Hindernis für Wirtschaftsspionage sind, so wenig besteht für den chinesischen Staat eine Hemmschwelle, in die Privatsphäre seiner Bürgerinnen und Bürger einzudringen. Zwar beteuert die chinesische Regierung immer wieder, jede Form des Internethacking und der Spionage abzulehnen. Die Hinweise dafür, dass von offiziellen Stellen Chinas Computerangriffe auf ausländische Rechner durchgeführt oder zumindest geduldet werden, sind aber eindeutig. Das betrifft sowohl die politische Opposition im Exil (beispielsweise die nach mehr Unabhängigkeit strebenden Tibeter, die Anhänger der 1999 verbotenen *Falun Gong*-Sekte oder Menschenrechtsaktivistinnen und -aktivisten), aber auch Behörden und Unternehmen in Deutschland und Europa müssen mit Angriffen auf ihre Computersysteme aus China rechnen.

Anfang 2010 wurde bekannt, dass im Rahmen einer Operation »Aurora« die Rechner von 30 Unternehmen, darunter *Google, Adobe, Yahoo!, Dow Chemical* und *Symantec* mit Spionagesoftware angegriffen und sensible Daten ausspioniert wurden. Daraufhin drohte *Google*, sich aus dem Land zurückzuziehen und verweigerte die weitere Kooperation bei Zensur und Kontrolle der Internetkommunikation. Die Regierung drohte ihrerseits damit, *Google* vom chinesischen Markt auszuschließen und die Datenverbindung zwischen China und Hongkong (wohin sich *Google* zurückgezogen hatte) zu kappen. Dies veranlasste *Google* letztlich, sich wieder den Überwachungsanforderungen der Regierung zu unterwerfen.

Doch gibt es auch gegenläufige Entwicklungen: So sollen zum Beispiel Informanten, die Fälle von Korruption anzeigen, besser geschützt werden, um sie vor Racheakten zu bewahren. Dagegen sind Dissidentinnen und Dissidenten im Land einer umfassenden Kontrolle durch die politische Polizei unterworfen, ausländische Kritiker werden als Staatsfeinde registriert und dürfen nicht ins Land einreisen. Es wird berichtet, dass von offizieller Seite eine »50-Cent-Armee« damit beschäftigt ist, regierungsfreundliche Informationen im Internet zu verbreiten. Während englischsprachige Angebote einer geringeren Zensur unterworfen sind, unterliegen chinesische Angebote mit regierungskritischen Inhalten einer dauernden Überwachung und werden umgehend gesperrt.

Unter besonderer Überwachung stehen die Medien. Die Zahl der inhaftierten Journalistinnen und Journalisten wird von »Reporter ohne Grenzen« mit über 100 angegeben. Darunter befindet sich der 43-jährige Journalist Shi Tao, der eine Zensuranweisung der staatlichen Behörden verbreitete, was der E-Mail-Dienstleister *Yahoo!* unter Druck den Behörden offenbarte. Shi Tao wurde deswegen zu einer zehnjährigen Gefängnisstrafe verurteilt. Die Medienkontrolle in China ist dabei kaum berechenbar. Phasen einer gewissen Liberalisierung folgen Phasen massiver Repression und Kontrolle. Diese Wechsel stehen thematisch, zeitlich und örtlich oft in Zusammenhang mit politischen oder sonstigen nationalen oder internationalen Ereignissen (zum Beispiel den Olympischen Spielen 2008 in Peking, der Expo 2010 in Shanghai).

3 Iran

Iran ist ein weiteres Beispiel für ein technisch hoch entwickeltes Land mit einer umfassenden Kontrolle der Bevölkerung und strenger Zensur. Die Nutzung des Internet stieg von einer Million im Jahr 2000 auf circa 32 Millionen Nutzerinnen und Nutzer in 2010 und erreicht damit knapp die Hälfte der Gesamtbevölkerung. Die Überwachung der Bevölkerung durch Polizei, Geheimdienste und halbstaatliche Milizen hat eine lange Tradition. Die staatliche Kontrolle des Internet startete 2001, als die kommerziellen *Internet Service Provider (ISP)* aufgefordert wurden, ihre Zugänge über die staatlich kontrollierte iranische Telekommunikationsgesellschaft zu schalten.

Die iranische Verfassung regelt, dass die Medien »streng Abstand nehmen müssen von der Verbreitung zerstörerischer und antiislamischer Praktiken«. Das Betreiben von Internet-Webseiten setzt den Erwerb einer staatlichen Lizenz voraus und wird laufend überwacht. Verboten sind die »Propaganda

gegen den Staat«, die »Beleidigung der Religion«, das Verursachen von »Angst und Unruhe in der öffentlichen Meinung«, das Verbreiten »falscher Gerüchte« oder »nicht zutreffender Handlungen« oder die Kritik an staatlichen Bediensteten. Die Umsetzung dieser Vorschriften war wegen der schwierigen Kontrollierbarkeit der Netztechnik und deren massenhafter Nutzung aber zunächst nur begrenzt erfolgreich. Deshalb nimmt ein Gesetz zur »Internetkriminalität« aus dem Jahr 2008 die *ISP* verstärkt in die Pflicht, dass »verbotene« Inhalte nicht dargestellt, die Aufsichtsbehörden unverzüglich über Verstöße unterrichtet und Inhalte für Beweiszwecke gespeichert werden. Bei Verstößen drohen Ordnungsstrafen sowie zeitweise oder dauerhafte Sperren.

Der Iran investiert viel, um die technischen Fähigkeiten zur umfassenden Überwachung seiner Bevölkerung auszubauen. Dem kommt die zentralisierte Architektur des iranischen Internet entgegen. Mit einem zentralisierten System sollen sämtliche Webseitenbesuche protokolliert und ausgewertet werden. Zur Kontrolle des Internet wurden im Iran zunächst Produkte aus westlichen Staaten eingesetzt, so zum Beispiel *Smart Filter*[3] der US-Firma *Secure Computing*. Im Jahr 2008 verkaufte die deutsch-finnische Anbietergemeinschaft *Nokia Siemens Networks* ein hochentwickeltes elektronisches System zur Internetüberwachung. Nach Kritik durch die US-Regierung und Einflussnahme durch das deutsche Bundeskanzleramt 2009 zog sich *Siemens* aus diesem Geschäft zurück. Zugleich versuchte die iranische Regierung, die Nutzung westlicher Überwachungstechnik und die damit verbundene Abhängigkeit abzubauen.

Die Kontrolle elektronischer Medien ist umfassend. Sie zielt gegen politisch abweichende, antiislamische und »unmoralische« Aktivitäten. Betroffen sind Minderheiten- und Menschenrechtsorganisationen, etwa die Frauenrechtsbewegung und regierungskritische Reformbestrebungen. Die Verhaftung von Menschen wird immer wieder mit Protokollen aus elektronischer Überwachung begründet. Diese Kontrollen sind gesellschaftlich nicht unumstritten. Als beispielsweise das konservative *Online*-Journal *Baztab.com* im Februar 2007 gesperrt wurde, erklärte der Oberste Gerichtshof dies für unrechtmäßig, was dazu führte, dass das Journal vorübergehend wieder zugänglich war. Die staatliche Kontroll- und Filterpraxis ist schwer einzuschätzen und offensichtlich von politischen Entwicklungen abhängig. 2010 erklärte das iranische Geheimdienst-Ministerium alle Kontakte zwischen iranischen Bürgerinnen und Bürgern und 60 nichtstaatlichen Organisationen sowie zahlreichen in persischer Sprache (Farsi) sendenden internationalen Medien für »illegal«.

Die elektronische Überwachung ist ein Baustein des umfassenderen repressiven Systems, in dem Demonstrierende und Oppositionelle verprü-

gelt, verhaftet, drangsaliert und bedroht werden. Folterungen und Vergewaltigungen, ja sogar Tötungen von Verhafteten sind Teil des Systems. Die hierfür durchgeführte Überwachung zielt gegen die Bevölkerung des Landes, gegen Journalistinnen und Journalisten, Unternehmen sowie ausländische Botschaften. Die Aktivitäten des iranischen Geheimdienstes reichen bis in die westlichen Länder, in denen vor allem die emigrierte iranische Opposition überwacht wird. Nach den Protesten im Zusammenhang mit den Präsidentschaftswahlen am 12. Juni 2009 und den Demonstrationen zum 31. Jahrestag der Revolution im Februar 2010 ist im Land weitgehend Friedhofsruhe eingekehrt.

4 Grenzüberschreitende Auswirkungen

Angesichts der weltweiten Vernetzung haben staatliche und private Überwachung andernorts auch direkte Auswirkungen auf Deutschland und Europa. Umgekehrt hat unsere Datenschutzpolitik Wirkungen auf die Staaten anderer Kontinente. Vor allem der immer noch weitgehend ungehindert stattfindende Export von Überwachungstechnik kann dramatische Konsequenzen in den Zielländern zur Folge haben. Käufer sind vor allem arabische und islamische Länder, die oft mit hohen Investitionen einen großen technischen Sprung hin zu mehr Überwachung ohne jede Sensibilität für digitalen Grundrechtsschutz vollziehen.

Anmerkungen

1 Von engl. *endemic*: vorherrschend, ausgeprägt.

2 Das *National Security Branch Analysis Center (NBA)* ist eine Querschnittsabteilung des FBI und wurde 2005 auf Erlass des amerikanischen Präsidenten begründet. Es soll die Erkenntnisse verschiedener Abteilungen des FBI bündeln, um Bedrohungen durch terroristische Organisationen, ausländische Geheimdienste, den Handel mit Massenvernichtungswaffen und organisierte Kriminalität vorzubeugen. Weitere Informationen zum NBA im Internet unter http://www.fbi.gov/about- us/nsb.

3 Mit der Anwendung *Smart Filter* kann laut Herstellerangaben der Zugriff auf das Internet beobachtet, analysiert, gefiltert und kontrolliert werden. Der Einsatz wird Unternehmen zur Kontrolle der Internetnutzung ihrer Beschäftigten empfohlen. Die Firma Secure Computing wurde mittlerweile vom Sicherheitsdienstleister McAfee aufgekauft. Weitere Informationen im Internet unter http://www.mcafee.com/us/resources/data-sheets/ds-smartfilter.pdf.

Marita Körner

Globaler Datenschutz

Schon seit Beginn der nationalen Datenschutzgesetzgebung in den 1970er Jahren war man sich des Problems bewusst, dass nationale Regelungen an den Landesgrenzen enden, die Datenverarbeitung jedoch längst über Ländergrenzen hinweg stattfindet. Diesem Umstand kann man mit bilateralen und internationalen Regelungen begegnen. Neben den Datenschutzregelungen der Europäischen Union kommen völkerrechtliche Verpflichtungen in Betracht, die regional begrenzt sein können (Europarat) oder global gelten (UNO). Dabei richten sich die internationalen Regeln durchweg an den öffentlichen wie den nicht-öffentlichen Bereich.

1 Europarat

Vor allem der Europarat hat den Datenschutz auf internationaler Ebene geprägt. Die seit 1949 bestehende internationale Organisation, der 47 europäische Staaten angehören, hat schon in den 1970er Jahren die Mitgliedstaaten aufgefordert, Schutzregelungen für die Verarbeitung personenbezogener Daten zu schaffen. 1981 verabschiedete der Europarat eine verbindliche internationale Regelung, die *Konvention zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten*.[1] Sie trat 1985 zunächst nur zwischen fünf Staaten, darunter Deutschland, in Kraft und bindet heute 44 europäische Staaten.

Es wurde allerdings schnell klar, dass die allgemeinen Regeln der Konvention nicht genügend Schutz bieten würden, sodass rasch eine Reihe von bereichsspezifischen Regelungen folgte, etwa 1989 mit der Empfehlung zum Schutz personenbezogener Daten für Beschäftigungszwecke.[2] Diese Regeln für den Arbeitnehmerdatenschutz entfalten jedoch keine bindende Wirkung für die Mitgliedsstaaten des Europarates.

Die Datenschutzkonvention von 1981 stellt Verarbeitungsgrundsätze auf (Artikel 5 ff.), die aus den schon existierenden nationalen Datenschutzregeln entnommen wurden. Danach sollen nur in angemessenem Umfang sachlich richtige und aktuelle Daten erhoben werden, die für den Verarbeitungszweck relevant und an einen festgelegten, rechtmäßigen Zweck gebunden sind. Einem besonderen Schutz sollen »sensitive« Daten unter-

liegen (Artikel 6). Diese als zusätzlicher Schutz gedachte Regel schwächte allerdings den Datenschutz letztlich, da der Begriff in jedem Land anders ausgelegt wird. Auch die Rechte des Betroffenen sind geregelt: neben Auskunfts-, Berichtigungs- und Löschungsrechten sollen die nationalen Rechte auch Rechtsmittel gegen unzulässige Datenerhebung vorsehen (Artikel 8 d). Schließlich ist in jedem Staat für eine Kontrollinstanz zu sorgen, die in »völliger Unabhängigkeit« arbeitet (Artikel 1 Nr. 3 des Zusatzprotokolls). In Deutschland ist das für die Datenschutzkontrolle im privaten Bereich nicht gewährleistet, wie der Europäische Gerichtshof (Gerichtshof der EU) in Auslegung der EU-Datenschutzrichtlinie von 1995[3] im Jahr 2010 gerügt hat.[4] Die EU-Datenschutzrichtlinie ist im Übrigen ein Grund für die abnehmende Bedeutung der Datenschutzkonvention des Europarates, die für die EU-Mitgliedstaaten seither nur noch eine Auffangfunktion hat.

In Artikel 12 spricht die Konvention auch den grenzüberschreitenden Datenschutz an, beschränkt sich aber auf den Datenaustausch zwischen Ländern, in denen die Konvention gilt und blendet so die größten Probleme beim internationalen Datentransfer aus.

Die rasante technische Entwicklung seit 1981, welche die Konvention nicht vorhersehen konnte, ist ein weiterer Grund, warum ihre praktische Bedeutung abnimmt. Allerdings wird das zum Teil vom Europäischen Gerichtshof für Menschenrechte (Gerichtshof des Europarates) kompensiert, der in Auslegung insbesondere von Artikel 8 EMRK (Europäische Menschenrechtskonvention), der das Recht auf Achtung des Privatlebens gewährt, die Erhebung und Verarbeitung von personenbezogenen Daten einschränkt.[5]

2 Normierungsbemühungen der UNO

Ähnlich wie der Europarat sahen die Vereinten Nationen in der automatisierten Datenverarbeitung schon früh eine Gefahr für die Menschenrechte. Entsprechend beschäftigte sich die Menschenrechtskommission mit der Materie und legte 1988 Vorschläge für Richtlinien zur Verarbeitung personenbezogener Daten in automatisierten Dateien vor, die 1990 von der Generalversammlung verabschiedet wurden. Diese UNO-Datenschutzrichtlinien[6] haben allerdings nur Empfehlungscharakter. Im Gegenzug richten sie sich aber nicht nur an die Mitgliedstaaten (Teil A), sondern zielen mit ihren Verarbeitungsgrundsätzen auch auf interne Regelungen für die internationalen Organisationen selbst (Teil B). Für Datensammlungen,

die der »humanitären Hilfe« oder dem »Schutz der Menschenrechte« dienen, sind jedoch Ausnahmen erlaubt. Das ist sinnvoll, wenn man bedenkt, dass zum Beispiel *Amnesty International* für die Erhebung von Opferdaten nicht zuvor deren Einwilligung einholen kann oder Tätern keine Auskunft zu den über sie gespeicherten Daten geben will.

Die Datenschutzgrundsätze selbst sind in den UNO-Richtlinien vergleichbar denen in der Datenschutzkonvention des Europarates geregelt. So soll, um nur zwei zentrale Grundsätze zu nennen, die Erhebung von personenbezogenen Daten nach Treu und Glauben erfolgen (Nr. 1) und die Zweckbindung der Daten garantiert werden (Nr. 3). Herausgehoben sind die UNO-Grundsätze insofern, als sie ganz ausdrücklich die Einrichtung einer unabhängigen Kontrollinstanz verlangen (Nr. 8). Darüber hinaus stellen sie auch Bedingungen für den grenzüberschreitenden Datenaustausch auf: er erfordert eine gleichwertige Datenschutzregelung im Empfängerstaat (Nr. 9). Bei dieser Aussage bleibt es aber. Weitere Voraussetzungen werden nicht angesprochen, sodass aus Nr. 9 nicht abgeleitet werden kann, dass es sich bei den Datenschutzregeln im Empfängerstaat um gesetzliche Regelungen handeln muss.

Die UNO beschäftigt sich auch im Rahmen des *Internet Governance Forum*[7] mit Datenschutz. Dessen Arbeitsgruppe *Internet Rights and Principles Coalition*[8] arbeitet an Grundregeln für die Rechte der Internetnutzenden. Sie betonen in Artikel 8 den Anspruch auf Privatsphäre, die informationelle Selbstbestimmung des Einzelnen sowie dessen Recht auf Anonymität. Darüber hinaus werden Grundsätze des Datenschutzes (wie Datensparsamkeit, Auskunftsrechte) sowie eine unabhängige Kontrollinstanz für den Datenschutz (Artikel 9 d) eingefordert.

3 Internationale Arbeitsorganisation

Auch die Internationale Arbeitsorganisation (ILO)[9] beschäftigt sich mit Datenschutz. Als Sonderorganisation der UNO, die für Arbeitsbedingungen zuständig ist, steht für sie der Arbeitnehmerdatenschutz im Mittelpunkt. Normalerweise verabschiedet die ILO nach langwierigen Abstimmungsprozessen die Staaten bindende Übereinkommen, deren Preis nicht selten inhaltliche Unbestimmtheit ist, um eine Mehrheit der Mitgliedstaaten zur Zustimmung zu animieren. Für den Arbeitnehmerdatenschutz hat die ILO daher einen anderen Weg gewählt und 1997 einen Verhaltenskodex verabschiedet.[10] Damit konnte sie vergleichsweise schnell eine Regelung vorlegen, die inhaltlich weiter geht als es

bei einer bindenden Regelung möglich gewesen wäre. Der Preis ist der reine Empfehlungscharakter dieser Vorgaben. Dafür allerdings enthält der Kodex relativ genaue Vorgaben.

Der Datenschutzkodex der ILO ist, anders als etwa das deutsche Bundesdatenschutzgesetz, skeptisch gegenüber der Einwilligung des Betroffenen als Rechtfertigungsgrund für Datenerhebung und -verarbeitung, da Zweifel bestehen, ob der abhängige Arbeitnehmer derartige Einwilligungen wirklich freiwillig erklärt. Bei sensiblen Daten, beispielsweise medizinischen (Nr. 6.7) oder genetischen (Nr. 6.12) Informationen, muss nach dem Kodex jedenfalls ein Gesetz die Datenerhebung und -verarbeitung regeln. Den Besonderheiten des Arbeitsrechts trägt auch die Regelung Rechnung, dass möglichst kollektivrechtliche Regelungen zum Arbeitnehmerdatenschutz abgeschlossen werden sollen (Nr. 12.2).

Obwohl nicht rechtsverbindlich, liefert der Kodex doch eine Interpretationshilfe für die allgemeinen Verarbeitungsbedingungen des BDSG, vor allem solange der Arbeitnehmerdatenschutz in Deutschland noch nicht bereichsspezifisch geregelt ist (siehe auch den Beitrag von Däubler in diesem Band, S. 188 ff.). Aber auch dann ist die deutsche Regelung vor dem Hintergrund der internationalen Standards auszulegen.

4 OECD

Auch die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung *(Organisation for Economic Cooperation and Development, OECD)*, der 33 Mitgliedstaaten angehören, hat sich schon in den 1970er Jahren mit Datenschutzproblemen beim grenzüberschreitenden Datenaustausch beschäftigt und 1980 nach jahrelangen Vorarbeiten Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten[11] verabschiedet.

Anders als bei der Datenschutzkonvention des Europarates stellen die Leitlinien keine völkerrechtlich verbindlichen Regelungen auf, sondern geben den Mitgliedstaaten Empfehlungen für entsprechende einzelstaatliche Regelungen. Die Perspektive der OECD ist dabei eine andere als die des Europarates. Steht für den Europarat die Garantie der Menschenrechte im Vordergrund, so sieht die OECD als Wirtschaftsorganisation in nationalen Datenschutzregeln auch die Gefahr von Handelshemmnissen. Sie will mit ihren Leitlinien auch die Freiheit des Informationsaustauschs gewährleisten. Daher nehmen die Leitlinien von vornherein personenbezogene Daten von ihrem Anwendungsbereich aus, für die »ganz

offensichtlich keine Gefahr der Verletzung der Privatsphäre und der Freiheit von Personen« besteht (Nr. 3 b). Wann das der Fall sein soll, wird nicht näher beschrieben. Vor allem wird nicht berücksichtigt, dass sich die Beeinträchtigung des Persönlichkeitsrechts in der Regel nicht aus den Daten selbst, sondern erst aus dem Zusammenhang ergibt, in dem diese verwendet werden.

Die Leitlinien enthalten in Nr. 7 bis 14 acht Verarbeitungsgrundsätze – von der rechtmäßigen Datenerhebung (Nr. 7) über die Zweckbindung (Nr. 9 und 10) bis zur transparenten Verarbeitung (Nr. 12). Auch die Rechte der Betroffenen werden angesprochen (Nr. 13) und umfassen Auskunfts-, Berichtigungs- und Löschungsansprüche. Das eigentliche Anliegen der OECD findet sich aber in Nr. 15 bis 18, wo Maßnahmen der Mitgliedstaaten zum freien grenzüberschreitenden Datenverkehr angemahnt werden. Die Mitgliedstaaten sollen die erforderlichen Schritte ergreifen, um bei grenzüberschreitendem Datentransfer »einen sicheren Datenverkehr ohne Unterbrechungen zu gewährleisten« (Nr. 16) und von Einschränkungen der grenzüberschreitenden Weitergabe personenbezogener Daten unter Mitgliedstaaten absehen (Nr. 17). Schließlich sollen Maßnahmen, die »über den erforderlichen Schutz von Personendaten hinausgehende Hemmnisse für den grenzüberschreitenden Verkehr personenbezogener Daten darstellen«, vermieden werden (Nr. 18).

Zu dieser den grenzüberschreitenden Datenaustausch fördernden Haltung passt es, dass die OECD für die Umsetzung ihrer Datenschutzrichtlinien keineswegs nur die nationalen Gesetzgeber im Auge hat (Nr. 19a), sondern die Selbstregulierung durch die Unternehmen gleichwertig daneben stellt (Nr. 19b). Für die Sicherung des Persönlichkeitsrechts der Betroffenen verlangen die OECD-Leitlinien also nicht notwendigerweise eine datenschutzgesetzliche Regelung in den Mitgliedstaaten. Ein vom Datenverarbeiter selbst entwickelter Datenschutz-Kodex soll ebenso ausreichen. Dieser Linie entspricht der seit 2000 bereitgestellte »Datenschutz-Generator«, der Hilfestellung zur Selbstregulierung bietet.[12]

5 Madrider Erklärung

Auch Nichtregierungsorganisationen beschäftigen sich mit Datenschutz. Mit der »Madrider Erklärung« vom Oktober 2009 forderten sie – aus Deutschland ist der Verbraucherzentrale-Bundesverband beteiligt – internationale Datenschutzabkommen (Nr. 10) und einen Stopp weiter Überwachungsmaßnahmen, wie zum Beispiel Körper-Scanning oder

→RFID-gestützte Kontrollsysteme (Nr. 9).[13] Auf der 31. Internationalen Datenschutzkonferenz[14] am 3. November 2009 in Madrid haben über einhundert Nichtregierungsorganisationen diese Erklärung unterzeichnet. Grundlage ihrer Erklärung ist die Forderung, dass vor dem Hintergrund einer »dramatischen Ausweitung geheimer und unkontrollierbarer Überwachung« internationale Regelungen dringend geboten sind. Inhaltlich besteht die »Madrider Erklärung« aus zehn Forderungen, die zum Teil bescheiden klingen, aber die Defizite der Datenschutzrealität abbilden. So wird zunächst die Einhaltung der bereits geltenden nationalen und internationalen Datenschutzregeln angemahnt (Nr. 6). Die Staaten werden aufgefordert, die Datenschutzkonvention des Europarats zu ratifizieren (Nr. 4). Wo es noch keine Datenschutzgesetzgebung gibt, möge diese so bald wie möglich verabschiedet werden (Nr. 5). Darüber hinaus wird die Bedeutung von unabhängiger Datenschutzkontrolle betont, die frei sein muss von politischer Einflussnahme oder wirtschaftlichen Interessen (Nr. 2). Es soll auch für datenschutzfreundliche Technologie gesorgt werden (Nr. 3) und sichergestellt werden, dass Datenbestände wirklich zuverlässig anonymisiert werden (Nr. 8). Schließlich ist den Betroffenen für den Fall rechtswidriger Datenverwendung ein Informationsrecht einzuräumen (Nr. 7).

Die »Madrider Erklärung« ist nicht die einzige internationale Initiative für einen besseren Datenschutz im globalen Rahmen. Bei der jährlichen internationalen Datenschutzkonferenz[15] ist die Forderung schon mehrfach erhoben worden. Auch die *Internet Rights and Principles Coalition*, eine Arbeitsgruppe des *Internet Governance* Forum der UNO, entwickelt dazu Ideen (siehe oben Abschnitt 2 dieses Beitrags).

6 Internationale Standardisierung über ISO/IEC

Einen anderen Ansatz verfolgen internationale Normen und Standards der internationalen Standardsetzungsorganisation ISO.[16] Hier geht es um Datenschutz bei Diensten und Geräten. Einerseits kann die Sicherheit von Software und Systemen zertifiziert werden, andererseits das Management von IT-Systemen. Vor allem die internationale Norm ISO/IEC 27001 zur Zertifizierung des Managements von IT-Sicherheit[17] verlangt auch die Einhaltung der rechtlichen Datenschutzregeln. Ohne deren Gewährleistung ist eine ISO/IEC 27001-Zertifizierung nicht möglich. Diese bestätigt in regelmäßigem Turnus, dass das IT-Management auch den datenschutzrechtlichen Anforderungen genügt. Bis zum Jahr 2010 gab es in Deutschland etwa 120 solcher Zertifizierungen.[18]

7 Auf dem Weg zu einem internationalen Rechtsrahmen

Die Entwicklung globaler Datenschutzstandards begann vor dreißig Jahren mit der Datenschutz-Konvention des Europarates. Seitdem wurden zahlreiche internationale Regelwerke auf europäischer und internationaler Ebene entwickelt. Dennoch fehlt bis heute (zumindest außerhalb des europäischen Wirtschaftsraumes) eine explizite, menschenrechtliche Verankerung des Datenschutzes. Die Diskussion um die internationale Angleichung von Schutzstandards und Rechtsansprüchen der Bürgerinnen und Bürger ist deshalb noch nicht abgeschlossen.

Angesichts zunehmender internationaler Handelsbeziehungen (inzwischen mit weltweiten Einkaufsmöglichkeiten für Endverbraucher) und globaler Kommunikationsdienste nimmt der Bedarf an solchen Regelungen zu. Mit dem Waren- und Kommunikationsaustausch steigt nicht nur der Umfang grenzüberschreitender Kriminalität, immer häufiger treffen dabei auch verschiedene Ansprüche an den Schutz der Privatsphäre aufeinander. Fehlende Löschmöglichkeiten für einmal erstellte Benutzerprofile, die automatisierte Gesichtserkennung von Bildern oder die Datenerhebung bei Nicht-Mitgliedern durch →soziale Netzwerke wie *Facebook* sind nur einige dieser Streitfragen, die sich heute kaum noch national regulieren lassen. Internetnutzerinnen und –nutzer in Deutschland genießen dabei den Vorteil, dass die deutschen und europäischen Datenschutzvorgaben selbst dann gelten, wenn eine Firma weder ihren Sitz oder eine Niederlassung in Deutschland hat. Die europäische Datenschutzrichtlinie bzw. das Bundesdatenschutz greifen auch dann, wenn ausländische Firmen ihr Angebot an deutsche bzw. europäische Nutzerinnen und Nutzer adressieren.[19] Für eine effektive Wahrnehmung und Durchsetzung solcher Rechtsansprüche wäre ein gemeinsamer, internationaler Rechtsrahmen absolut hilfreich.

Auch wenn die bisherigen Ergebnisse der globalen Datenschutzdiskussion (zumindest außerhalb Europas) noch nicht zu rechtlich verbindlichen Regelwerken geführt haben, ist ihr Beitrag zur Entwicklung der nationalen Datenschutzstandards nicht zu unterschätzen. Wie das Beispiel der ILO-Empfehlungen für einen guten Arbeitnehmerdatenschutz zeigt, kann auch der deutsche Datenschutz von derartigen Debatten profitieren (siehe auch die Beiträge von Wolf, S. 199 ff. und Perreng, S. 206 ff. in diesem Band).

Anmerkungen

1 Genauer zur Konvention: Herbert Burkert, Die Konvention des Europarats zum Datenschutz, in: Computer und Recht (CR) 1988, S. 751.
2 Empfehlung Nr. R (89) 2. Siehe dazu: Spiros Simitis, Verarbeitung von Arbeitnehmerdaten – Die Empfehlung des Europarates, in: CR 1991, S. 161.
3 Richtlinie 95/46/EG.
4 EuGH, Urteil vom 9.3.2010 – C-518/07 (Kommission/Deutschland), in: Neue Juristische Wochenschrift (NJW) 2010, S. 1265; siehe dazu auch den Beitrag von Kamp/Thomé in diesem Band, S. 298ff.
5 Z. B. EGMR, Copland./.UK, in: Multimedia und Recht (MMR) 2007, S. 431.
6 Die UNO-Datenschutzrichtlinien sind zu finden unter http://www.unhcr.org/refworld/publisher,UNGA,THEMGUIDE,,3ddcafaac,0.html.
7 http://www.intgovforum.org/cms/.
8 http://irpcharter.org/compain/.
9 Die International Labour Organization (ILO) wurde 1919 als Unterorganisation des Weltbundes (dem Vorläufer der heutigen UNO) gegründet. Seit 1946 ist sie eine Sonderorganisation der Vereinten Nationen und hat ihren Sitz in Genf. Zu ihrem Auftrag gehört die Förderung sozialer Gerechtigkeit sowie der Menschen- und Arbeitsrechte. Dazu handelt die ILO Empfehlungen sowie rechtlich verbindliche Konventionen aus, mit denen internationale Standards des Arbeitsrechts, Arbeitsschutzes und der Arbeitssicherheit festgeschrieben werden. Der ILO gehören 183 Mitgliedsstaaten an. Weitere Informationen im Internet unter http://www.ilo.org.
10 International Labour Office, Protection of workers personal data. An ILO code of practice, Genf 1997 (engl.), im Internet unter http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrument/wcms_107797.pdf.
11 Eine Kurzfassung der OECD-Richtlinien über Datenschutz in deutscher Sprache findet sich im Internet unter: http://www.oecdbookshop.org. Mit einer Überarbeitung der Richtlinien ist im Laufe des Jahres 2012 zu rechnen.
12 Im Internet unter http://www.oecd.org/document/39/0,2340,en_2649_201185_28863271_1_1_1_1,00.html. Weitere Informationen der OECD zum Thema Privacy finden sich auf der Webseite ihrer Abteilung Wissenschaft, Technik und Industrie unter http://www.oecd.org/department/0,3355,en_2649_34255_1_1_1_1_1,00.html.
13 Informationen zur Erklärung unter: http://www.thepublicvoice.org/madrid-declaration.
14 Die Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre (kurz: Datenschutzkonferenz) ist eine jährlich stattfindende internationale Konferenz, die sich mit Fragen des Datenschutzes beschäftigt.
15 Zuletzt fand die 33. Internationale Datenschutzkonferenz am 2. und 3.11.2011 in Mexico City statt, siehe http://www.privacyconference2011.org.
16 Die Internationale Organisation für Normung (International Organization for Standardization, ISO) wurde 1947 begründet und hat ihren Sitz in Genf. Als zwi-

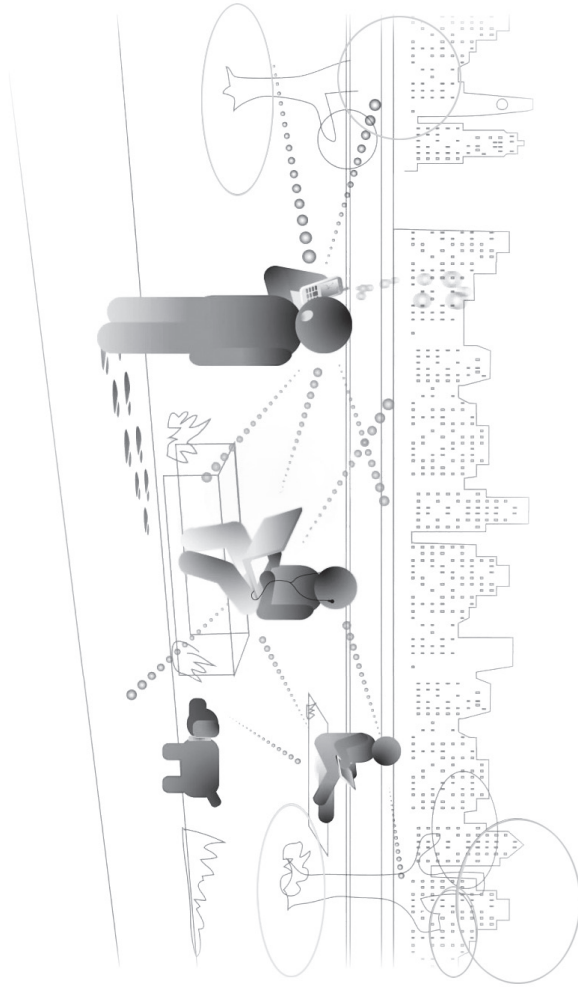
schenstaatliche Normungsorganisation erarbeitet sie technische, klassifikatorische und Verfahrensstandards für nahezu alle Bereiche des industriellen Lebens. Ausgenommen sind lediglich elektrische/elektronische Standards (dafür ist die Internationale elektrotechnische Kommission – IEC – zuständig) sowie technische Normen der Telekommunikation (dafür ist die Internationale Fernmeldeunion – ITU – zuständig). Der ISO gehören derzeit über 150 Mitgliedsstaaten an, für Deutschland ist seit 1951 das Deutsche Institut für Normung e. V. (DIN) Mitglied. Weitere Informationen im Internet unter http://www.iso.org; siehe auch Glossar →ISO.

17 http://www.iso.org/iso/catalogue_detail?csnumber=42103.

18 Gisela Quiring-Kock, Zertifizierung und ihre Bedeutung, in: Datenschutz und Datensicherheit (DuD) 2010, S. 178 ff.

19 Florian Jotzo: Gilt deutsches Datenschutzrecht auch für *Google*, *Facebook* & Co. bei grenzüberschreitendem Datenverkehr?, in: MMR 2009, S. 232 ff.

VI. Anhang



Ausschnitt aus dem Video zum Online-Spiel Data Dealer (http://www.datadealer.net)

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.

Literaturhinweise

Albers, Marion: Informationelle Selbstbestimmung, 2. Aufl. Baden-Baden 2012.

Grundlegende Auseinandersetzung mit dem Recht auf informationelle Selbstbestimmung und seiner verfassungsrechtlichen Verankerung.

Comans, Clemens David: Ein »modernes« europäisches Datenschutzrecht. Bestandsaufnahme und Analyse praktischer Probleme des europäischen Datenschutzes unter besonderer Berücksichtigung der Richtlinie zur Vorratsdatenspeicherung, Frankfurt/M. u. a. 2012.

Wissenschaftliche Darstellung zu den aktuellen Herausforderungen des Datenschutzrechts. Beinhaltet eine ausführliche Auseinandersetzung mit den Rechten der Betroffenen sowie deren Durchsetzungsmöglichkeiten.

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo: Bundesdatenschutzgesetz, Kompaktkommentar zum BDSG und anderen Gesetzen, 3. überarbeitete und erweiterte Auflage 2010.

Das Bundesdatenschutzgesetz (BDSG) ist durch drei Novellen im Juli 2009 in wichtigen Punkten geändert worden. Das in der neuen Auflage erscheinende, deutlich erweiterte Werk erläutert alle Vorschriften des BDSG und seine Neuregelungen kompetent, übersichtlich und gut verständlich.

Eifert, Martin / Hoffmann-Riem, Wolfgang (Hrsg.): Recht, Innovation und öffentliche Kommunikation, Recht und Innovation IV, Berlin 2011.

Sammelband der Projektgruppe »Innovation und Recht«, der Aufsätze zu aktuellen Fragestellungen im Zusammenhang mit kommunikationsrechtlichen Themen enthält (darunter auch die Beiträge von Alexander Roßnagel, Das Gebot der Datenvermeidung und -sparsamkeit als Ansatz wirksamen technikbasierten Persönlichkeitsschutzes?, und von Christoph Bieber, Wahlkampf als Onlinespiel? Die Piratenpartei als Innovationsträgerin im Bundestagswahlkampf 2009).

Elixmann, Robert: Datenschutz und Suchmaschinen – neue Impulse für einen Datenschutz im Internet, Berlin 2012.

Der Autor stellt die datenschutzrechtlichen Probleme dar, die bei der Protokollierung der Nutzeranfragen und bei der Veröffentlichung persönlicher Daten durch Suchmaschinenbetreiber entstehen.

Emmer, Martin/Vowe, Gerhard/Wolling, Jens: Bürger online. Die Entwicklung der politischen Online-Kommunikation in Deutschland, bpb-Schriftenreihe, Bonn 2011.

Das Internet hat zu einem grundlegenden Wandel gesellschaftlicher Kommunikation geführt. Die breit angelegte Studie analysiert, wie sich die politische Kommunikation der Bevölkerung in Deutschland durch die Nutzung des Internets innerhalb einer Dekade verändert hat.

Gaycken, Sandro/Kurz, Constanze (Hrsg.): 1984.exe, Münster 2008.

Sammelband zu Überwachung und Datenschutz mit akademischen und praxisbezogenen Beiträgen.

Hoeren, Thomas: Skript Internetrecht, Online-Buch – im Internet unter http://www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript%20Internetrecht_April_2011.pdf (Stand: Juli 2012).

Regelmäßig aktualisiertes Skript zu allen Bereichen des Onlinerechts. Eine allgemein verständliche Einführung in die rechtlichen Probleme der digitalen Welt.

Jarvis, Jeff: Was würde *Google* tun? Wie man von den Erfolgsstrategien des Internetgiganten profitiert, München 2009.

Positiv gestimmte Analyse des Internetkonzerns *Google*, in der die Erfolgsstrategie des Konzerns gepriesen wird und die kritischen Fragen aus dem Weg geht.

Kühling, Jürgen/Seidel, Christian/Sivridis, Anastasios: Datenschutzrecht, Heidelberg 2011.

Aktuelles Kurzlehrbuch zum Datenschutzrecht aus der Reihe »Start ins Rechtsgebiet«. Bietet einen guten Überblick über die nationalen und internationalen Vorgaben im Bereich des Datenschutzrechts und veranschaulicht die rechtlichen Probleme anhand kurzer Fallbeispiele und gut verständlicher Grafiken.

Kuner, Christopher: European Data Protection Law: Corporate Compliance and Regulation, Oxford 2007.

Umfassende Darstellung des europäischen Datenschutzrechts in englischer Sprache. Das Buch bietet einen guten Überblick über die Herausforderungen, denen sich das Datenschutzrecht auf internationaler Ebene stellen muss.

Kurz, Constanze/Rieger, Frank: Die Datenfresser. Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen. bpb-Schriftenreihe, Bonn 2011.

Aktuelle Diagnose zur informationellen Selbstbestimmung im Internet von zwei Mitgliedern des Chaos Computer Clubs. Angesichts der zahlreichen Datenspuren, die viele Tätigkeiten hinterlassen, trägt das Buch dazu bei, die digitale Welt besser zu verstehen, finanzielle Mechanismen zu durchschauen und die eigene Datensouveränität zurück zu erlangen.

Nissenbaum, Helen: Privacy in Context. Technology, Policy, and the Integrity of Social Life, Palo Alto 2010.

Soziale Netzwerke sind ein bestimmender Faktor in Teilen des gesellschaftlichen Lebens geworden. Das Buch thematisiert und analysiert unter Datenschutzgesichtspunkten die Reaktionen auf diese Entwicklung.

Quiring-Kock, Gisela: Zertifizierungen und ihre Bedeutung, Datenschutz und Datensicherheit (DuD) 2010, S. 178–181.

Darstellung unterschiedlicher Zertifizierungsverfahren sowie Beschreibung der jeweiligen Ziele und Anforderungen mit dem Praxisbeispiel »ELSTER«.

Reppesgaard, Lars: Das *Google*-Imperium. Hamburg 2008.

Journalistischer Einblick in Geschichte, Organisation und Strategien der Firma *Google*.

Rössler, Beate: Der Wert des Privaten, Berlin 2001,

Vor dem Hintergrund moderner, liberaler Gesellschaften wird eine normative Theorie des Privaten begründet. Probleme der Privatheit von Beziehungen kommen ebenso zur Sprache wie Fragen des Datenschutzes.

Roßnagel, Alexander/Pfitzmann, Andreas/Garstka, Hansjürgen: Modernisierung des Datenschutzrechts, Gutachten im Auftrag des BMI, Berlin 2001, im Internet unter http://www.lda.brandenburg.de/sixcms/media.php/2473/dsmodern.pdf.

Eine umfassende Bestandsaufnahme zur Entwicklung der Informationstechnologien und den daraus folgenden Notwendigkeiten für eine Modernisierung des Datenschutzrechtes in Deutschland.

Schaar, Peter: Das Ende der Privatsphäre. Der Weg in die Überwachungsgesellschaft. Gütersloh 2007

Umfassende und meinungsstarke Streitschrift des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

Schmidt, Jan-Hinrik: Das neue Netz. Merkmale, Praktiken und Folgen des Web 2.0, Konstanz 2011.

Die kommunikationssoziologische Studie untersucht Praktiken und gesellschaftliche Konsequenzen des Web 2.0, insbesondere die Veränderungen von Öffentlichkeit und – damit einhergehend – von Privatsphäre.

Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz, 7. Aufl., Baden-Baden 2011.

Juristischer Großkommentar zum Datenschutzrecht, der die datenschutzrechtlichen Probleme jeweils sehr umfassend aus wissenschaftlicher Sicht beleuchtet. Zusätzlich zu den Kommentierungen der Normen gibt es eine ausführliche Einleitung.

Simon, Anne-Catherine/Simon, Thomas: Ausgespäht und abgespeichert. München 2008.

Zusammenschau von Überwachungstechnologien und Hinweisen, wie man sich zur Wehr setzen kann.

Sofsky, Wolfgang: Die Verteidigung des Privaten. München 2007.

Kultursoziologischer Essay zum gesellschaftlichen Stellenwert der Privatsphäre.

Solove, Daniel: Understanding Privacy, Cambridge 2008.

Profunde Einführung in die aktuelle Datenschutzdebatte.

Stöcker, Cristian: Nerd Attack! Eine Geschichte der digitalen Welt vom C64 bis zu *Twitter* und *Facebook*, bpb-Schriftenreihe, Bonn 2011.

Durch das Netz werden die private und öffentliche Kommunikation verändert. Eine Art historischer Reisebericht durch die computerbasierte Kommunikation von den Wurzeln der digitalen Revolution bis zur Omnipotenz von Information in den sozialen Netzwerken.

Tangens, Rena/padeluun (Hrsg.): Schwarzbuch Datenschutz. Hamburg 2006.

Sammlung der »Preisträger« des deutschen BigBrotherAwards 2000 bis 2006, den Oscars für Datenkraken.

Verbraucherzentrale Bundesverband e. V.: Meine Daten gehören mir – Datenschutz im Alltag, Berlin 2010.

Das Ratgeberbuch enthält zahlreiche Tipps für Verbraucherinnen und Verbraucher, wie sie im Alltag ihr Recht auf informationelle Selbstbestimmung wahren und verteidigen können.

Wagner, Ulrike/Brüggen, Niels/Gebel, Christa: Persönliche Informationen in aller Öffentlichkeit? Jugendliche und ihre Perspektive auf Datenschutz und Persönlichkeitsrechte in Sozialen Netzwerkdiensten (JFF – Institut für Medienpädagogik in Forschung und Praxis), München 2010, im Internet unter http://www.blm.de/apps/documentbase/data/pdf1/JFF-Bericht_Datenschutz_Persoenlichkeitsrechte.pdf.

Die Studie untersucht Präsentationsstrategien Jugendlicher im Netz sowie ihr Verhältnis zum Datenschutz.

Warren, Samuel D./Brandeis, Louis D.: The Right to Privacy (dt.: Das Recht auf Privatheit), in: Harvard Law Review Bd. IV (Nr. 5/1890); Originalfassung im Internet unter htttp://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (20.11.2011); deutsche Übersetzung im Internet unter https://www.datenschutzzentrum.de/allgemein/20111219-Warren-Brandeis-Recht-auf-Privatheit.html.

Die beiden Juristen begründen in ihrem historischen Aufsatz erstmals das Konzept der Privatsphäre. Auslöser war die damals entstehende Pressefotografie, die zur Abbildung vieler Menschen in Boulevardmedien führte.

Zeh, Juli/Trojanow, Ilija: Angriff auf die Freiheit. Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte, München 2009.

Engagierte Auseinandersetzung mit der politischen Debatte um Sicherheit und Terrorbekämpfung.

Urteile des Bundesverfassungsgerichts

Übersicht wichtiger Entscheidungen zum Recht auf informationelle Selbstbestimmung[1]

Mikrozensus:
Beschluss vom 16. Juli 1969 – Az. 1 BvL 19/63, BVerfGE 27/1. Im Internet unter http://www.servat.unibe.ch/dfr/bv027001.html

Überwachung nach dem G10 Gesetz:
Beschluss vom 20. Juni 1984 – Az. 1 BvR 1494/78, BVerfGE 67, 157. Im Internet unter http://www.servat.unibe.ch/dfr/bv067157.html

Volkszählungsurteil:
Urteil vom 15. Dezember 1983 – Az. 1 BvR 209/83 u. a., BVerfGE 65, 1. Im Internet unter http://www.servat.unibe.ch/dfr/bv065001.html

Großer Lauschangriff:
Urteil vom 3. März 2004 – Az. 1 BvR 2378/98; 1 BvR 1084/99, BVerfGE 109, 279. Im Internet unter http://www.bundesverfassungsgericht.de/entscheidungen/rs20040303_1bvr237898.html

1 Die Beiträge in diesem Band verweisen auf Entscheidungen des Bundesverfassungsgerichts (BVerfG) unter Angabe der Fundstelle in den Entscheidungsbänden des BVerfG (zum Beispiel: BVerfGE 65, 1) und auf das jeweilige Aktenzeichen (zum Beispiel: Az. 1 BvR 209/83).
Sämtliche Urteile (ab 1998) sind im Internet abrufbar unter www.bundesverfassungsgericht.de. Dort können die einzelnen Entscheidungen entweder unter ihrem Aktenzeichen oder unter Angabe der Fundstelle in den Entscheidungsbänden aufgerufen werden.
In Bibliotheken ist die Suche jeweils über die Fundstelle in den Entscheidungsbänden möglich.

TK-Verbindungsdaten:
Urteil vom 2. März 2006 – Az. 2 BvR 2099/04, BVerfGE 115, 166. Im Internet unter http://www.bundesverfassungsgericht.de/entscheidungen/rs20060302_2bvr209904.html

Vorbeugende Telefonüberwachung:
Urteil vom 27. Juli 2005 – Az. 1 BvR 668/04, BVerfGE 113, 348. Im Internet unter http://www.bundesverfassungsgericht.de/entscheidungen/rs20050727_1bvr066804.html

Rasterfahndung:
Beschluss vom 4. April 2006 – Az. 1 BvR 518/02, BVerfGE 115, 320. Im Internet unter http://www.bundesverfassungsgericht.de/entscheidungen/rs20060404_1bvr051802.html

Online-Durchsuchung:
Urteil vom 27. Februar 2008 – Az. 1 BvR 370/07 und 1 BvR 595/07, BVerfGE 120, 274. Im Internet unter http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html

Kfz-Abgleich:
Urteil vom 11. März 2008 – Az. 1 BvR 2074/05 und 1 BvR 1254/07, BVerfGE 120, 378. Im Internet unter http://www.bundesverfassungsgericht.de/entscheidungen/rs20080311_1bvr207405.html

Präventive Videoüberwachung:
Beschluss vom 17. Februar 2009 – Az. 1 BvR 2492/08, BVerfGE 122, 342. Im Internet unter http://www.bundesverfassungsgericht.de/entscheidungen/rs20090217_1bvr249208.html

Vorratsdatenspeicherung:
Urteil vom 2. März 2010 – Az. 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08, BVerfGE 125, 260. Im Internet unter http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html

Abkürzungen

a. a. O.	am angegebenen Ort
Abk.	Abkürzung
ABR	Verfahrenskennzeichen für Beschwerden beim Bundesarbeitsgericht
Abs.	Absatz
A-Drs.	Ausschuss-Drucksache
Anm.	Anmerkung
Art.	Artikel
Az.	Aktenzeichen
Aufl.	Auflage
BAG	Bundesarbeitsgericht
Bd.	Band
BDSG	Bundesdatenschutzgesetz
betr.	betreffend(en)
BetrVG	Betriebsverfassungsgesetz
BfV	Bundesamt für Verfassungsschutz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungen des Bundesgerichtshofs in Strafsachen
BKA	Bundeskriminalamt
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BND	Bundesnachrichtendienst
BR-Drs.	Drucksache des Bundesrats
BT-Drs.	Drucksache des Bundestages, im Internet unter http://dip.bundestag.de/
BT-Pl.	Plenarprotokoll des Bundestages
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts (Veröffentlichungsreihe des Gerichts), mit Angabe des Bandes; s. auch die Übersicht wichtiger Entscheidungen zum Recht auf informelle Selbstbestimmung in diesem Band, S. 448 f.
BVerfGK	Kammerentscheidungen des Bundesverfassungsgerichts
BvR	Verfahrenskennzeichen für Beschwerden gem. Art. 93 Abs. 1 Nr. 4a und 4b GG beim Bundesverfassungsgericht
bzgl.	bezüglich
bzw.	beziehungsweise
ca.	circa
CR	Computer und Recht (Zeitschrift)
DAG	Datenschutzauditgesetz
ders/dies.	der-/dieselbe
d. h.	das heißt
DNA	Desoxyribonukleinsäure
DuD	Datenschutz und Datensicherheit (Zeitschrift)
DuR	Demokratie und Recht (Zeitschrift)
DVBl.	Deutsches Verwaltungsblatt
ebd.	ebenda
EDV	elektronische Datenverarbeitung
EG	Europäische Gemeinschaft(en)
EGMR	Europäischer Gerichtshof für Menschenrechte
etc.	et cetera
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EUV, EU-Vertrag	Vertrag über die Europäische Union
f.	folgende
ff.	fortfolgende
gem.	gemäß
GBl.	Gesetzblatt
GG	Grundgesetz für die Bundesrepublik Deutschland
ggf.	gegebenenfalls
GS Schl.-H.	Gesetzessammlung des schleswig-holsteinischen Landesrechts
Hrsg.	Herausgeber
hg.	herausgegeben
i. d. F.	in der Fassung
IMEI	*International Mobile Equipment Identity* (Kennung des Mobilfunkgerätes)
IMSI	*International Mobile Subscriber Identity* (Kennung der Mobilfunkkarte)

insb.	insbesondere
IT	*Information Technology,* dt. Informationstechnologie
i. E.	im Erscheinen
i. V. m.	in Verbindung mit
JR	Juristische Rundschau (Zeitschrift)
JZ	Juristenzeitung
LT-Drs.	Drucksache eines Landtags/Länderparlaments
MAD	Militärischer Abschirmdienst
MDStV	Mediendienstestaatsvertrag
MMR	MultiMedia und Recht (Zeitschrift für Informations-, Telekommunikations- und Medienrecht)
m. w. N.	mit weiteren Nachweisen
n. F.	neue Fassung
NGO	Non Govermental Organisation, dt. Nichtregierungsorganisation
NJOZ	Neue Juristische Online-Zeitschrift
NJW	Neue Juristische Wochenschrift
NK	Neue Kriminalpolitik (kriminologische Zeitschrift)
Nr.	Nummer
NStZ	Neue Zeitschrift für Strafrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
OSZE	Organisation für Sicherheit und Zusammenarbeit in Europa
PC	Personal Computer
Pkt.	(Gliederungs-)Punkt
PNR	*Passenger Name Record* (Fluggastdatensatz)
RFID	*Radio Frequency Identification* (→ RFID)
RL	Richtlinie
Rn.	Randnummer
Rs.	Rechtssache
s.	siehe
S.	Seite oder Satz
SMS	Short Message Service (Nachrichtenformat für Mobiltelefone)
s. o.	siehe oben
sog.	sogenannte
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
SÜG	Sicherheitsüberprüfungsgesetz
SWIFT	*Society for Worldwide Interbank Financial Telecommunication* (→ SWIFT)
TDDSG	Teledienstedatenschutzgesetz
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TMG	Telemediengesetz
u. a.	unter anderem/und andere
UN	United Nations, dt. Vereinte Nationen
usw.	und so weiter
u. U.	unter Umständen
v.	von/vom
vgl.	vergleiche
vs.	versus
WP	*Working Paper,* dt. Arbeitspapier
z. B.	zum Beispiel
ZRP	Zeitschrift für Rechtspolitik

Webseiten

Artikel-29-Arbeitsgruppe bei der Europäischen Kommission
http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

Die Indexseite der EU-Kommission für Justiz listet sämtliche Arbeitspapiere der →Artikel-29-Arbeitsgruppe auf, die sich mit der Verwirklichung des Datenschutzes in der Europäischen Union befassen.

BfDI – Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
http://www.bfdi.bund.de

Die Webseite des BfDI enthält eine Übersicht der gesetzlichen Grundlagen des Datenschutzes, seine Tätigkeitsberichte, Informationen zu einzelnen Themenbereichen sowie ein Datenschutz-Forum zum Austausch mit anderen Interessierten.

BSI für Bürger
https://www.bsi-fuer-buerger.de

Auf der Serviceseite des Bundesamtes für Sicherheit in der Informationstechnik (BSI) werden Informationen zur Datensicherheit in allen Bereichen der Informationstechnik bereitgestellt.

Bürger-Cert
https://www.buerger-cert.de

Das Bürger-CERT des Bundesamtes für Sicherheit in der Informationstechnik (BSI) informiert und warnt Bürgerinnen und Bürger sowie kleine Unternehmen schnell und kompetent vor Computerviren, -würmern und Sicherheitslücken in Computeranwendungen.

De-Mail
http://www.de-mail.de

Informationen des BSI zur Funktionsweise und den Nutzungsmöglichkeiten von →De-Mail. Die Seite enthält eine Auflistung der akkreditierten Anbieter des sicheren Maildienstes.

Deutschland sicher im Netz
http://www.sicher-im-netz.de

Ein Angebot des gleichnamigen Vereins, das Datenschutz- und weitere Anwendungs-Tipps für die Verbraucherseite und Unternehmen, aber auch für Kinder, Jugendliche, Eltern und Lehrkräfte bereit hält. Angeboten werden u. a. Surf-Tipps für Schülerinnen und Schüler, ein Lernkoffer zur Medienbildung in der Schule und eine kindgerechte Internetseite (www.internauten.de).

Electronic Frontier Foundation
https://www.eff.org

Internetseite einer Nichtregierungsorganisation mit Sitz in San Fransisco, die sich mit der Wahrung von Bürgerrechten in der digitalen Welt beschäftigt. Die Seite beinhaltet Stellungnahmen und Informationen zu gerichtlichen Verfahren.

Electronic Privacy Information Center (EPIC)
http://epic.org

Internetseite eines amerikanischen Forschungszentrums, das sich mit datenschutzrechtlichen Themen sowie der Meinungsfreiheit beschäftigt. EPIC veröffentlicht Studien und Jahresreporte zu aktuellen Themen (z. B. Körperscanner, *Facebook*, → *Cloud Computing*) in englischer Sprache.

Europäischer Datenschutzbeauftragter
http://www.edps.europa.eu

Internetseite des Europäischen Datenschutzbeauftragten mit Stellungnahmen, Empfehlungen, Presseinformationen sowie Informationen zu allgemeinen Fragen des Datenschutzes auf europäischer Ebene.

Klicksafe
http://www.klicksafe.de

Initiative der EU für mehr Sicherheit im Netz. Bietet Informationsmaterial und Hinweise zu einem sicheren Umgang mit dem Internet.

Personalausweis
http://www.personalausweisportal.de/DE/Home/home_node.html

Informationsportal des Bundesministeriums des Innern rund um den neuen Personalausweis und dessen Funktionen.

Privacy International
https://www.privacyinternational.org

Internetauftritt der Nichtregierungsorganisation *Privacy International* mit Informationen zu internationalen Kampagnen gegen Verletzungen der Privatsphäre.

Projekt Datenschutz
http://www.projekt-datenschutz.de

Das von privater Seite betriebene Projekt dokumentiert Datenschutzvorfälle in Unternehmen, Organisationen und Behörden sowie Datenschutz-Aktivitäten der Politik.

Surfer haben Rechte
http://www.surfer-haben-rechte.de

Die vom Bundesverbraucherministerium geförderte und von der Verbraucherzentrale Bundesverband verantwortete Seite gibt Tipps zum Verbraucherdatenschutz im Internet.

Surfen ohne Risiko
http://www.surfen-ohne-risiko.net

Die Webseite bietet Informationen darüber, wie sich Kinder ohne Risiko im Internet bewegen können und schafft einen sicheren Surfraum zum Ausprobieren.

Verbraucher sicher online
http://www.verbraucher-sicher-online.de

Die vom Bundesverbraucherministerium geförderte und von der Technischen Universität Berlin erstellte Webseite gibt praktische, allgemein verständliche Tipps zur Datensicherheit im Internet.

Virtuelles Datenschutzbüro
http://www.datenschutz.de

Das Portal des virtuellen Datenschutzbüros erschließt fast sämtliche Internetauftritte unabhängiger Datenschutzstellen im deutschsprachigen Raum. Es wird vom Unabhängigen Landeszentrum für Datenschutz (ULD) Schleswig-Holstein betrieben.

webhelm
http://www.webhelm.de

Die Plattform – eine Werkstatt-Community für Urheberrecht, Datenschutz und Persönlichkeitsrechte – möchte jugendliche Surferinnen und Surfer sensibilisieren und mit zahlreichen Tipps ihren selbstverständlichen Umgang mit dem Internet stärken. Die vom JFF – Institut für Medienpädagogik entwickelte Website wendet sich nicht nur an Jugendliche, sondern auch an Eltern und pädagogische Fachkräfte, die dort eine eigene Rubrik finden.

ZafTDa – Zentralarchiv für Tätigkeitsberichte des Bundes- und der Landesdatenschutzbeauftragten und der Aufsichtsbehörden für den Datenschutz
http://www.thm.de/zaftda/

Die Technische Hochschule Mittelhessen stellt die seit 1971 erschienenen Tätigkeitsberichte (TB) des Bundes- und der Landesdatenschutzbeauftragten sowie der Aufsichtsbehörden für den Datenschutz zur Verfügung.

Datenschutzbehörden

(Stand: 7/2012)

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Husarenstraße 30, 53117 Bonn
Tel.: 0228/997 799-0
Fax: 0228/997 799-550
E-Mail: poststelle@bfdi.bund.de, pressestelle@bfdi.bund.de
Internet: http://www.datenschutz.bund.de

Der Landesbeauftragte für Datenschutz Baden-Württemberg
Königstraße 10a, 70173 Stuttgart
Postfach 10 29 32, 70025 Stuttgart
Tel.: 0711/61 55 41-0
Fax: 0711/61 55 41-15
E-Mail: poststelle@lfd.bwl.de
Internet: http://www.baden-wuerttemberg.datenschutz.de

Der Bayerische Landesbeauftragte für den Datenschutz
(Bayern, öffentlicher Bereich)
Wagmüllerstraße 18, 80538 München
Postfach 22 12 19, 80502 München
Tel.: 089/212 672-0
Fax: 089/212 672-50
E-Mail: poststelle@datenschutz-bayern.de
Internet: http://www.datenschutz-bayern.de

Bayerisches Landesamt für Datenschutzaufsicht
(Bayern, nicht-öffentlicher Bereich)
Promenade 27, 91522 Ansbach
Tel.: 0981/531 300
Fax: 0981/535 300
E-Mail: poststelle@lda.bayern.de
Internet: http://www.lda.bayern.de

Berliner Beauftragter für Datenschutz und Informationsfreiheit
An der Urania 4-10, 10787 Berlin
Tel.: 030/13 889-0
Fax: 030/215 50 50
E-Mail: mailbox@datenschutz-berlin.de
Internet: http://www.datenschutz-berlin.de

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht (Brandenburg)
Stahnsdorfer Damm 77, 14532 Kleinmachnow
Tel.: 033203/356-0
Fax: 033203/356-49
E-Mail: poststelle@lda.brandenburg.de
Internet: http://www.lda.brandenburg.de

Die Landesbeauftragte für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen
Arndtstraße 1, 27570 Bremerhaven
Tel.: 0471/596-2010 od. 0421/361-2010
Fax: 0421/496-18495
E-Mail: office@datenschutz.bremen.de
Internet: http://www.datenschutz-bremen.de

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit
Klosterwall 6 (Block C), 20095 Hamburg
Tel.: 040/428 54-4040
Fax: 040/428 54-4000
E-Mail: mailbox@datenschutz.hamburg.de
Internet: http://www.datenschutz-hamburg.de

Der Hessische Datenschutzbeauftragte
Gustav-Stresemann-Ring 1, 65189 Wiesbaden
Postfach 31 63, 65021 Wiesbaden
Tel.: 0611/1408-0
Fax: 0611/1408-900 oder -901
E-Mail: poststelle@datenschutz.hessen.de
Internet: http://www.datenschutz.hessen.de

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern
Schloss Schwerin, 19053 Schwerin
Tel.: 0385/59 49 4-0
Fax: 0385/59 49 4-58
E-Mail: datenschutz@mvnet.de
Internet: http://www.lfd.m-v.de

Der Landesbeauftragte für den Datenschutz Niedersachsen
Brühlstraße 9, 30169 Hannover
Tel.: 0511/120 45 00
Fax: 0511/120 45 99
E-Mail: poststelle@lfd.niedersachsen.de
Internet: http://www.lfd.niedersachsen.de

Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen
Kavalleriestraße 2-4, 40213 Düsseldorf
Postfach 20 04 44, 40102 Düsseldorf
Tel.: 0211/38 424-0
Fax: 0211/38 424-10
E-Mail: poststelle@ldi.nrw.de
Internet: https://www.ldi.nrw.de

Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz
Hintere Bleiche 34, 55116 Mainz
Postfach 30 40, 55020 Mainz
Tel.: 06131/208-2449
Fax: 06131/208-2497
E-Mail: poststelle@datenschutz.rlp.de
Internet: http://www.datenschutz.rlp.de

Unabhängiges Datenschutzzentrum Saarland
Fritz-Dobisch-Straße 12, 66111 Saarbrücken
Postfach 10 26 31, 66026 Saarbrücken
Tel.: 0681/94 781-0
Fax: 0681/94 781-29
E-Mail: poststelle@datenschutz.saarland.de
Internet: http://www.datenschutz.saarland.de

Der Sächsische Datenschutzbeauftragte
Bernhard-von-Lindenau-Platz 1, 01067 Dresden
Tel.: 0351/493-5401
Fax: 0351/493-5490
E-Mail: saechsdsb@slt.sachsen.de
Internet: http://www.saechsdsb.de

Landesbeauftragter für den Datenschutz Sachsen-Anhalt
Leiterstraße 9, 39104 Magdeburg
Postfach 1947, 39009 Magdeburg
Tel.: 0391/81 803-0, Freecall: 0800 915 3190 (Festnetz der DTAG und nur aus Sachsen-Anhalt)
Fax: 0391/81 803-33
Internet: http://www.sachsen-anhalt.de/index.php?id=18637

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Holstenstraße 98, 24103 Kiel
Postfach 71 16, 24171 Kiel
Tel.: 0431/988-1200
Fax: 0431/988-1223
E-Mail: mail@datenschutzzentrum.de
Internet: https://www.datenschutzzentrum.de

Thüringer Landesbeauftragter für den Datenschutz
Jürgen-Fuchs-Straße 1, 99096 Erfurt
Postfach 900455, 99107 Erfurt
Tel.: 0361/37 71 905
Fax: 0361/37 71 904
E-Mail: poststelle@datenschutz.thueringen.de
Internet: http://www.thueringen.de/datenschutz

Europäischer Datenschutzbeauftragter
(European Data Protection Supervisor)
Büro: Rue Montoyer 63, B-1047 Brussels (Brüssel)
Post: Rue Wiertz 60, B-1047 Brussels
Tel.: 0032-2-283 19 00
Fax: 0032-2-283 19 50
E-Mail: edps@edps.europa.eu
Internet: http://www.edps.europa.eu

Datenschutzorganisationen

Arbeitskreis Vorratsdatenspeicherung (AK Vorrat)
erreichbar über FoeBuD (s. u.)
E-Mail: kontakt@vorratsdatenspeicherung.de
Internet: http://www.vorratsdatenspeicherung.de

Bundesverband der Datenschutzbeauftragten Deutschlands e. V. (BvD)
Budapester Straße 31, 10787 Berlin
Tel.: 030/2196 4397
Fax: 030/2196 4392
Publikation: BvD-News
E-Mail: bvd-gs@bvdnet.de
Internet: http://www.bvdnet.de

Chaos Computer Club e. V. (CCC)
Mexikoring 21, 22297 Hamburg
Postfach 600480, 22204 Hamburg
Fax: 010/4018 0140
Publikation: die datenschleuder
E-Mail: mail@ccc.de
Internet: http://www.ccc.de

Deutsche Vereinigung für Datenschutz e. V. (DVD)
Rheingasse 8-10, 53113 Bonn
Tel.: 0228/222 498
Fax: 0228/243 8470
Publikation: DatenschutzNachrichten (DANA)
E-Mail: dvd@datenschutzverein.de
Internet: http://www.datenschutzverein.de

Digitale Gesellschaft e. V.
Schönhauser Allee 6/7, 10119 Berlin
Tel.: 0177/750 3541
E-Mail: info@digitalegesellschaft.de
Internet: http://digitalegesellschaft.de

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FifF)
Goetheplatz 4, 28203 Bremen
Tel.: 0421/333 659 255
Fax: 0421/336 592 56
Publikation: FifF-Kommunikation
E-Mail: fiff@fiff.de
Internet: http://www.fiff.de

Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD)
Pariser Straße 37, 53117 Bonn
Tel.: 0228/694 313
Fax: 0228/695 638
Publikation: GDD-Mitteilungen
E-Mail: info@gdd.de
Internet: https://www.gdd.de

Hamburger Datenschutzgesellschaft e. V. (HDG)
Erik-Blumenfeld-Platz 27a, 22587 Hamburg
Tel.: 040/3990 6032
E-Mail: info@hamdg.de
Internet: http://www.hamdg.de

Humanistische Union e. V. (HU)
(vereinigt mit der Gustav Heinemann-Initiative)
Haus der Demokratie und Menschenrechte
Greifswalder Straße 4, 10405 Berlin
Tel.: 030/2045 0256
Fax: 030/2045 0257
Publikationen: vorgänge, Mitteilungen der HU, Grundrechte-Report
E-Mail: info@humanistische-union.de
Internet: http://www.humanistische-union.de

Internationale Liga für Menschenrechte e. V. (ILMR)
Haus der Demokratie und Menschenrechte
Greifswalder Straße 4, 10405 Berlin
Tel.: 030/396 2122
Fax: 030/396 2147
E-Mail: vorstand@ilmr.de
Internet: http://www.ilmr.de

Komitee für Grundrechte und Demokratie e. V.
(Grundrechtekomitee)
Aquinostraße 7-11, 50670 Köln
Tel.: 0221/972 6920
Fax: 0221/972 6931
E-Mail: info@grundrechtekomitee.de
Internet: http://www.grundrechtekomitee.de

Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e. V. (FoeBuD)
Marktstraße 18, 33602 Bielefeld
Tel.: 0521/175 254
Fax: 0521/611 72
E-Mail: mail@foebud.org
Internet: https://www.foebud.org, https://www.bigbrotherawards.de, http://www.stoprfid.de, http://www.spychip.de

Autorinnen und Autoren

Albers, Marion, Prof. Dr. jur., Professorin für Öffentliches Recht, Informations- und Kommunikationsrecht, Gesundheitsrecht und Rechtstheorie an der Universität Hamburg. Kontakt: http://www.jura.uni-hamburg.de/personen/albers

Allen, Richard, Director of European Public Policy bei *Facebook*. Kontakt: http://www.facebook.com/ricallan

Bartmann, Franz-Joseph, Dr. med., Viszeral- und Unfallchirurg, Präsident der Ärztekammer Schleswig-Holstein, amtierender Vorsitzender der Fort- und Weiterbildungsgremien sowie des Telematikausschusses der Bundesärztekammer. Kontakt: http://www.aeksh.de

Beckedahl, Markus, Blogger auf netzpolitik.org und Vorsitzender des Digitale Gesellschaft e. V. Kontakt: http://www.netzpolitik.org bzw. markus@netzpolitik.org.

Bieber, Christoph, Prof. Dr., Johann-Wilhelm-Welker-Stiftungsprofessur für Ethik in Politikmanagement und Gesellschaft an der NRW School of Governance, Universität Duisburg-Essen. Kontakt: christoph.bieber@uni-due.de

Billen, Gerd, Vorstand des Verbraucherzentrale Bundesverbandes e. V. und Verwaltungsrat der Stiftung Warentest. Kontakt: info@vzbv.de

Bluhm, Franziska, Chefredakteurin bei Wirtschaftswoche Online. Kontakt: http://www.wiwo.de bzw. post@franziskabluhm.de

Bock, Kirsten, Leiterin des European Privacy Seal beim Unabhängigen Landeszentrum für Datenschutz, Kiel. Kontakt: http://www.european-privacy-seal.eu bzw. kbock@datenschutzzentrum.de

Brüggen, Niels, wissenschaftlicher Mitarbeiter am JFF – Institut für Medienpädagogik in München. Kontakt: http://www.jff.de bzw. niels.brueggen@jff.de

Däubler, Wolfgang, Prof. Dr. jur., Professor für Deutsches und Europäisches Arbeitsrecht, Bürgerliches Recht und Wirtschaftsrecht an der Universität Bremen i. R. Kontakt: daeubler@uni-bremen.de

Dix, Alexander, Dr., LL.M., Berliner Beauftragter für Datenschutz und Informationsfreiheit, Vorsitzender der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation (international auch bekannt als »Berlin Group«) und Mitglied der Artikel 29-Gruppe der Europäischen Datenschutzbeauftragten. Kontakt: mailbox@datenschutz-berlin.de

Fiedler, Christoph, Dr., Rechtsanwalt, Geschäftsführer Medien- und Europapolitik im VDZ Verband Deutscher Zeitschriftenverleger, Vorsitzender des Rechtsausschusses des Europäischen Zeitschriftenverlegerverbandes FAEP, Lehrbeauftragter an den Universitäten Düsseldorf und Leipzig. Kontakt: http://www.vdz.de

Gebel, Christa, wissenschaftliche Mitarbeiterin am JFF – Institut für Medienpädagogik in München. Kontakt: http://www.jff.de bzw. christa.gebel@jff.de

Hansen, Marit, Stellvertretende Landesbeauftragte für Datenschutz Schleswig-Holstein, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel. Kontakt: https://www.datenschutzzentrum.de bzw. marit.hansen@datenschutzzentrum.de

Hartge, Dagmar, Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht des Landes Brandenburg. Kontakt: http://www.lda.brandenburg.de

Heckmann, Dirk, Prof. Dr., Mitglied des Bayerischen Verfassungsgerichtshofes, Lehrstuhl für Sicherheitsrecht und Internetrecht, Universität Passau. Kontakt: http://www.jura.uni-passau.de/heckmann.html.

Heine, Franziska, Mediengestalterin und Initiatorin der Online-Petition »Keine Indizierung und Sperrung von Internetseiten«. Kontakt: http://franziskaheine.de

Hijmans, Hielke, LL.M., Leiter des Bereichs Politik und Beratung beim Europäischen Datenschutzbeauftragten. Kontakt: http://www.edps.europa.eu

Hustinx, Peter, Europäischer Datenschutzbeauftragter, Brüssel. Kontakt: http://www.edps.europa.eu

Kamp, Meike, LL.M., Referentin für internationale Datentransfers und datenschutzfreundliche Verfahrensgestaltungen beim Berliner Beauftragten für Datenschutz und Informationsfreiheit. Kontakt: meike.kamp@web.de

Körner, Marita, Prof. Dr. jur., Universität der Bundeswehr München, Fakultät für Betriebswirtschaft, Professur für Wirtschafts- und Arbeitsrecht, Neubiberg. Kontakt: http://www.unibw.de/bw/Fakultat/we-bw/mkoerner

Langfeldt, Owe, Mitarbeiter im Bereich Politik und Konsultationen beim Europäischen Datenschutzbeauftragten, Brüssel. Kontakt: http://www.edps.europa.eu

von Lewinski, Kai, PD Dr., Juristische Fakultät der Humboldt-Universität zu Berlin. Kontakt: http://www.lewinski.eu

Loosen, Wiebke, PD Dr., Senior Researcher am Hans-Bredow-Institut für Medienforschung in Hamburg. Kontakt: http://www.hans-bredow-institut.de/de/mitarbeiter/pd-dr-wiebke-loosen

Lüke, Falk, Fachjournalist für Politik und Technik in Berlin. Kontakt: http://www.falk-lueke.de bzw. mail@falklueke.com

Martin, Angelika, Mitarbeiterin im Bereich Technik des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, Kiel. Kontakt: http://www.datenschutzzentrum.de

Papier, Hans-Jürgen, Prof. Em. Dr. Dres. h. c., Präsident des Bundesverfassungsgerichts a. D., entpflichteter Professor an der Juristischen Fakultät der Ludwig-Maximilians-Universität München. Kontakt: ls.papier@jura.uni-muenchen.de

Perreng, Martina, Juristin, Referatsleiterin in der Abteilung Recht beim Bundesvorstand des DGB. Kontakt: info.bvv@dgb.de

Petri, Thomas Dr., Bayerischer Landesbeauftragter für den Datenschutz, München. Kontakt: http://www.datenschutz-bayern.de bzw. dsb@datenschutz-bayern.de.

Polenz, Sven, Dr., LL.M., Referatsleiter für den Datenschutz in der Privatwirtschaft am Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein in Kiel. Kontakt: https://www.datenschutzzentrum.de bzw. polenz@datenschutzzentrum.de

Reppesgaard, Lars, Buchautor, Journalist und Research Consultant, doubleYUU GmbH & Co. KG, Hamburg. Kontakt: http://www.doubleyuu.com/lars

Roßnagel, Alexander, Prof. Dr., Universitätsprofessor für Öffentliches Recht mit dem Schwerpunkt Recht der Technik im Forschungszentrum für Informationstechnik-Gestaltung (IT eG) der Universität Kassel. Kontakt: http://www.uni-kassel.de/fb7/oeff_recht bzw. a.rossnagel@uni-kassel.de

Rost, Martin, Mitarbeiter im Bereich Technik beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, Kiel. Kontakt: http://www.maroki.de

Schaar, Peter, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit in Bonn und Berlin. Kontakt: http://www.bfdi.bund.de

Schallbruch, Martin, Diplom-Informatiker, IT-Direktor im Bundesministerium des Innern. Kontakt: http://www.cio.bund.de bzw. http://www.bmi.bund.de

Schmidt, Jan-Hinrik, Dr., wissenschaftlicher Referent für digitale interaktive Medien und politische Kommunikation am Hans-Bredow-Institut für Medienforschung in Hamburg. Kontakt: http://www.hans-bredow-institut.de bzw. j.schmidt@hans-bredow-institut.de

Seemann, Michael, Blogger, Publizist und Kulturwissenschaftler in Berlin. Kontakt: http://mspr0.de, http://ctrl-verlust.net bzw. mymspro@googlemail.com.

Sokol, Bettina, Präsidentin des Rechnungshofs der Freien Hansestadt Bremen.

Spaeing, Frank, externer Datenschutzbeauftragter, Mentor und Dozent der Initiative »Datenschutz geht zur Schule«. Kontakt: http://www.ds-quadrat.de/wittenberg

Spaeing, Thomas, Vorstandsvorsitzender des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e. V. in Berlin, Inhaber der ds²-Unternehmensberatung für Datenschutz. Kontakt: http://www.bvdnet.de oder http://www.ds-quadrat.de

Thomé, Sarah, LL. M., Juristin, Dozentin für Datenschutzrecht und Verwaltungsrecht an der Hochschule für Wirtschaft und Recht Berlin. Kontakt: thome@e-privacy.info

Thomsen, Sven, Leiter Technik beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein, Kiel. Kontakt: https://www.datenschutzzentrum.de bzw. sthomsen@datenschutzzentrum.de

Trepte, Sabine, Dr., Juniorprofessorin für Medienpsychologie an der Universität Hamburg und der Hamburg Media School. Kontakt: http://www.uni-hamburg.de und http://www.hamburgmediaschool.com bzw. sabine.trepte@uni-hamburg.de

Wagner, Edgar, Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz. Kontakt: http://www.datenschutz.rlp.de

Wagner, Ulrike, Dr., Direktorin des JFF – Institut für Medienpädagogik in München. Kontakt: www.jff.de bzw. ulrike.wagner@jff.de

Weichert, Thilo, Dr., Jurist und Politologe, Landesbeauftragter für Datenschutz Schleswig-Holstein, Leiter des Unabhängigen Landeszentrums für Datenschutz, Kiel. Kontakt: https://www.datenschutzzentrum.de

Wolf, Roland, Assessor, Geschäftsführer der Bundesvereinigung der Deutschen Arbeitgeberverbände, Leiter Arbeitsrecht. Kontakt: r.wolf@arbeitgeber.de

Ziercke, Jörg, Präsident des Bundeskriminalamtes, Wiesbaden. Kontakt: www.bka.de bzw. http://www.bka.de/profil/mailinfo.html