Sinn und Unsinn des Datenschutzes

Hans Peter Bull

Sinn und Unsinn des Datenschutzes

Persönlichkeitsrecht und Kommunikationsfreiheit in der digitalen Gesellschaft

Mohr Siebeck

Hans Peter Bull, geboren 1936; 1978–83 Bundesbeauftragter für den Datenschutz; 1988–95 Innenminister des Landes Schleswig-Holstein; Professor emeritus für Öffentliches Recht und Verwaltungslehre an der Universität Hamburg.

ISBN 978-3-16-154182-7

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über *http://dnb.dnb.de* abrufbar.

© 2015 Mohr Siebeck Tübingen. www.mohr.de

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Das Buch wurde von Gulde-Druck in Tübingen gesetzt, auf alterungsbeständiges Werkdruckpapier gedruckt und von der Buchbinderei Nädele in Nehren gebunden.

Inhaltsverzeichnis

I. Einleitung: Eine Erfolgsgeschichte auf unklarer Grundlage

Datenschutz ist eine Erfolgsgeschichte. Aber darüber, was dieser Begriff eigentlich bedeutet und wie weit Datenschutz reichen kann, herrscht Unklarheit, und manche zweifeln sogar daran, dass Datenschutz überhaupt etwas bewirkt. Die Debatte darüber ist festgefahren.

Angeblich leben wir in einer „digitalen Gesellschaft". In jeder zweiten Ausgabe der großen Tages- und Wochenzeitungen lesen wir, dass die Informationstechnik unser Leben radikal verändere, dass demnächst Maschinen die Herrschaft über uns erlangen werden, dass die Geheimdienste jeden von uns „im Visier" haben und die Konzerne mit Hilfe der „Big Data" unser Alltagsleben prägen. „Computer entscheiden über Kredite, Algorithmen erkennen frühzeitig, ob Frauen schwanger sind: Derzeit verändert sich etwas Grundsätzliches im Verhältnis von Mensch und Maschine".[1] Die Medien scheinen sich mit den Datenschutzbeauftragten und den Fachpolitikern einig zu sein, dass durch die intensive Verarbeitung persönlicher Daten die Grundrechte aller Menschen auf dieser Welt aufs schwerste gefährdet sind, und fordern unisono „mehr" oder „besseren" Datenschutz. Ein anderer Beobachter aber sagt (in einem Vortrag vor Datenschützern!), „es wäre problemlos möglich, einen Vortrag zum Thema

[1] Süddeutsche Zeitung vom 25./26.4.2015, S. 36.

‚Warum ich nicht glaube, dass Datenschützer wirklich meine Daten schützen' zu halten".[2]

Staatliche „Überwachung" mittels Datenauswertung und private Daten-„Ausbeutung" gelten gleichermaßen als schwere Eingriffe in die individuelle Freiheit fast aller lebenden Menschen und als Gefahren für Rechtsstaat und Demokratie. Geradezu apokalyptisch erscheint die Bedrohung durch Geheimdienste wie den amerikanischen NSA, aber fast ebenso stark fühlen sich viele durch die Datenverarbeitung im Internet, speziell in den „sozialen Netzwerken" bedroht. Dass Unmengen von Daten in unsichtbaren „Wolken" gespeichert werden – nämlich in riesigen gemeinsamen Datenzentren außerhalb der Stellen, die sie einmal erhoben haben – wird ebenso als Übel empfunden wie die Fernüberwachung häuslicher technischer Anlagen, das Fernmessen des Energieverbrauchs und die automatische „Kommunikation" zwischen Minicomputern in und an körperlichen Gegenständen. Die Angst vor der Künstlichen Intelligenz verbindet sich mit der Konkurrenzangst der europäischen Computer- und Internetwirtschaft angesichts der ökonomischen Macht der global tätigen US-amerikanischen Konzerne von Microsoft bis Facebook. Das Schlagwort „Big Data" dient als Chiffre für die Verfügbarkeit unvorstellbar großer Mengen an Daten und weckt allein für sich schon die gleichen Assoziationen wie der allwissende und allmächtige „Big Bro-

[2] Göttrik Wewer, Wundermittel Transparenz? Über Informationsfreiheit und Transparenzgesetze, Vortrag auf dem 3. Symposium der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am 11. September 2014, in: Alexander Dix/Gregor Franßen/Michael Kloepfer/Peter Schaar/Friedrich Schoch /Andrea Voßhoff/Deutsche Gesellschaft für Informationsfreiheit (Hrsg.), Informationsfreiheit und Informationsrecht. Jahrbuch 2014, S. 161 (172).

ther" in Orwell's Roman „1984": das „diffus bedrohliche Gefühl des Beobachtetseins".[3]

Weltweit ist starker Protest gegen die Praktiken von NSA & Co. geäußert worden, aber offenbar ohne dass die Geheimdienste eingelenkt hätten. Die nationalen Regierungen sind gefordert, sich gegen die Amerikaner stark zu machen. Grundlegende und dauerhafte Abhilfe wird aber nicht nur von internationalen Vereinbarungen und von der Abschottung der nationalen Datenverarbeitungssysteme erhofft, sondern darüber hinaus von neuen rechtlichen Regelungen. Gefordert wird ein „digitales Menschenrecht auf Privatsphäre",[4] und die „informationelle Selbstbestimmung" soll auf nationaler, supranationaler und internationaler Ebene umfassend ausgebaut werden.

Bei aller berechtigten Empörung über die Abhörpraktiken einiger Geheimdienste und über andere Formen schwerer Missachtung von Grundrechten ist die generelle Vorstellung von den Risiken, die durch die Nutzung persönlicher Daten verursacht werden, in wichtigen Aspekten unscharf, und die Konsequenzen sind nicht zu Ende gedacht. Die vermeintliche Einigkeit über die tatsächli-

---

[3] So eine Formulierung des BVerfG, bezogen auf die „anlasslose Speicherung von Telekommunikationsdaten", gemeinhin „Vorratsdatenspeicherung" genannt, vgl. das Urteil v. 2.3.2010, BVerfGE 125, 260 (320). „Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens" können nach Ansicht des BVerfG auch durch die automatische Erfassung von Kfz-Kennzeichen entstehen, vgl. Urteil v. 11.3.2008, BVerfGE 120, 378 (402).

[4] Grundlegende Erörterung bei Max-Otto Baumann, Privatsphäre als neues digitales Menschenrecht? Ethische Prinzipien und aktuelle Diskussionen, hrsg. v. Deutschen Institut für Vertrauen und Sicherheit im Internet (DIVSI), Reihe Diskussionspapiere, Hamburg 2015 (mit zahlreichen Nachweisen aus der internationalen Diskussion).

chen Phänomene wie über ihre Bewertung ist in Wahrheit brüchig. Was Datenschutz bedeutet, ist viel umstrittener als die Kommentare der Medien uns glauben machen wollen. Einigkeit herrscht auf den Konferenzen der Datenschutzbeauftragten, die freilich auf Außenstehende wie „Feldmessen für Gläubige" wirken.[5] Als anerkannte Experten erwarten die Aufsichtsbehörden von den Nichtexperten Gefolgschaft, und scheinbar folgen ihnen fast alle. Doch dieser Eindruck trügt, denn bei genauem Hinsehen bröckelt die Fassade.

Schon das Szenario, das den Überlegungen der herrschenden öffentlichen Meinung zugrunde liegt, ist in weiten Teilen irreal. Die „digitale Gesellschaft" ist nichts anderes als die Gesellschaft, die sich der elektronischen Informations- und Kommunikationstechnik bedient; ihre sozialen, wirtschaftlichen und politischen Strukturen sind deutlich weniger mysteriös und bedrohlich als sie dargestellt werden.[6] Richtig ist zwar: Es bestehen unglaubliche *Möglichkeiten* der Erhebung, Auswertung und Nutzung von Daten über die meisten Menschen – aber

---

[5] Göttrik Wewer, Wundermittel Transparenz? (Fn. 2), S. 161 (172).

[6] Klar und überzeugend gegen die Idee einer aus Technik hervorgehenden Gesellschaftsform: Lutz Hachmeister, Es gibt keine digitale Gesellschaft, FAZ v. 1.6.2015, S. 9. Unter dem Titel „Die digitale Gesellschaft" (2012) behandeln Markus Beckedahl und Falk Lüke laut Untertitel „Netzpolitik, Bürgerrechte und die Machtfrage"; das ist – wie in der Einleitung (S. 10) versprochen – „ein verständliches und teils auch vergnüglich zu lesendes Buch über die Netzpolitik und ihre Bedeutung für die Gesellschaft von morgen", aber keine Gesellschaftstheorie. Peter Schaar hat sein neuestes Buch überschrieben mit „Das digitale Wir" und spricht von „transparenter Gesellschaft", „Internetgesellschaft" oder „Informationsgesellschaft" (Hamburg 2015).

über die *tatsächlichen* Praktiken, die realistischen Aussichten und die absehbaren Vor- und Nachteile sind ebenso viele Legenden wie zutreffende Erkenntnisse im Umlauf. Um die richtigen Gegenmaßnahmen zu ergreifen, müssen erst einmal die Gefahren genau bezeichnet werden; Übertreibungen verursachen übermäßige Reaktionen, die ihrerseits Schaden anrichten. Viele der normativen Ideen, die den düsteren Prognosen entgegengestellt werden, sind einseitig, nicht mit entgegenstehenden anderen, ebenso gewichtigen Interessen abgewogen, und damit erweisen sie sich als doppelgesichtig: Der beabsichtigte Schutz für den einen wirkt als Freiheitsbeschränkung für einen anderen.

Kommunizieren ist wie Atmen: Jeder und jede muss mit anderen kommunizieren und dabei auch Informationen über Dritte austauschen. Niemand kann alle Informationen, die über ihn entstehen, selbst beherrschen; vollständige „informationelle Selbstbestimmung" war seit je unmöglich und ist es heute, angesichts der undurchschaubaren Fülle der Datenberge erst recht. Für die Übermittlung personenbezogener Informationen braucht sich niemand zu rechtfertigen, solange damit keine Rechte eines Dritten verletzt werden. Ob meine Äußerung erlaubt ist oder ob sie jemandem schadet, kann und will ich möglichst selbst beurteilen. Nach dem geltenden Datenschutzrecht aber werden alltägliche Kommunikationsvorgänge komplizierter und aufwendiger; denn datenschutzrechtliche Pflichten bedeuten bürokratische Lasten: Anzeige-, Informations- und Dokumentationspflichten, Kosten, Rechtfertigungslasten und Unterwerfung unter staatliche Kontrolle.

Wohlgemerkt: Behörden und Unternehmen müssen solche Einschränkungen hinnehmen, Private nur bedingt,

nämlich wenn und soweit sie ihrerseits durch Datenverarbeitung Macht über andere Menschen ausüben können. Wer wie Facebook, Twitter, WhatsApp usw. mit den Daten Geschäfte macht, muss sich an nutzerfreundliche Regeln halten. Soweit die Nutzung der Internetdienste nicht lebensnotwendig ist, kann ihre Entwicklung zwar dem Markt überlassen bleiben. Aber je stärker wir von den elektronischen Angeboten abhängig werden, desto strenger muss der Staat auf faire Bedingungen achten – auch um die Ängste der Menschen vor Manipulation zu dämpfen – selbst wenn manche dieser Ängste unbegründet sind.

Ich werbe also für ein realistisches, nüchternes Verständnis der Lage, für die Auflösung der Wertungswidersprüche und für eine Konzentration der Kräfte auf die wichtigen Probleme. Wir sollten uns wieder auf die Wurzeln von Privatheit und Persönlichkeitsschutz besinnen und die Instrumente dafür so gestalten, dass sie zu den neu aufgetretenen Phänomenen passen und effektiv sind. Das Ziel kann nicht sein, die Individuen voneinander und von der Gesellschaft möglichst perfekt abzuschirmen, sondern ein freiheitliches Zusammenleben der Menschen zu fördern. Auch wenn es immer wieder betont wird, dass der Einzelne das Recht auf „informationelle Selbstbestimmung" hat, ist dieser Begriff nicht wirklich hilfreich genug, die vorhandenen Probleme in den Griff zu bekommen. Informationelle Selbstbestimmung bedeutet jedenfalls nicht das Monopol der Selbstdarstellung; andere dürfen sich aus meinem Verhalten und meinen Äußerungen ein eigenes Bild von mir machen.

Richtig verstandener Datenschutz sollte verstanden werden als *fairer, respektvoller, grundrechtskonformer Umgang mit persönlichen Informationen*. Anders als die bloß auf das Individuum bezogene Formel von der Selbst-

bestimmung enthält der Fairness-Begriff eine inhaltliche Komponente, „Respekt" verweist darauf, dass der Datenverwender die Würde des Einzelnen wahren soll, und die Grundrechtskonformität muss multidimensional verstanden werden: Den Grundrechten des einen stehen die der anderen gegenüber; zwischen beiden Positionen muss abgewogen werden.

II. Grundbegriffe

Um Klarheit über die tatsächlichen Zusammenhänge zu gewinnen, müssen zunächst einige zentrale Begriffe geklärt werden, die heute die Wahrnehmung der Phänomene durch Wissenschaft und Medien bestimmen. Die üblichen Begriffe sind nämlich kaum geeignet, die Situation richtig zu begreifen: Wo von „Daten" gesprochen wird, sind in einem großen Teil der Fälle „*Informationen*" gemeint, und „Datenschutz" heißt nicht nur Schutz der Daten (vor der Kenntnisnahme Dritter), sondern auch Schutz *vor* den Daten (also der schädlichen Wirkung der Daten auf die Interessen des Betroffenen).[7]

1. Daten, Informationen und Wissen

Schon der Begriff „*Daten*", der in allen Datenschutzgesetzen vorkommt, wird vielfach missverstanden. Richtig angewandt, sind damit nur die Zeichen gemeint, die auf einem *Träger* (Papier, Magnetband, Computer-Festplatte, USB-Stick usw.) gespeichert sind. Sie sollen eine inhaltliche Aussage, eine „*Information*" ausdrücken.[8] Dass sie

[7] Dazu lesenswert: Kai von Lewinski, Die Matrix des Datenschutzes. Besichtigung und Ordnung eines Begriffsfeldes, 2014.

[8] Zum Informationsbegriff vgl. a. Friedrich Schoch, Öffentlichrechtliche Rahmenbedingungen einer Informationsordnung, in: VVDStRL 57 (1998), S. 158 ff. (166 mit Anm. 26 ff.). Schoch verwen-

tatsächlich diese Funktion erfüllen, setzt aber die Kenntnisnahme durch eine Person voraus. Ein Kommunikationsprozess kommt nur zustande, wenn ein „*Informationssubjekt*" mit anderen Informationssubjekten im Austausch steht. „Als Information stellt sich der Informationsträger nur für ein Informationssubjekt dar".[9]

„Als Informationssubjekte sehen wir in erster Linie Menschen. Es kann offen bleiben, ob Maschinen als Informationssubjekte betrachtet werden dürfen. Maschinen, die eine große Anzahl innerer Zustände annehmen können, können jedoch mit Normen, Zielen, Strategien usw. gefüttert werden. Auch dann unterscheiden sie sich vom Menschen immer dadurch, dass sie keine Absichten haben können und dass sie auch nicht über ein inneres Auge für ihre eigenen Informationsbestände verfügen; dieses innere Auge ist das, was wir beim Menschen als Bewusstsein bezeichnen."[10]

Der Informationsgehalt einer Information steht nicht ein für alle Mal fest, sondern hängt vom *Kontext* ab, u. a. vom Vor- oder Zusatzwissen, über das ein Informationssubjekt verfügt oder das es sich beschaffen kann.

„Eine irgendwo abgelegte Information (Vertragstext, Datenbankinhalte usw.) kann von jedem anders verstanden werden, so

---

det einen anderen Informationsbegriff als hier vertreten, stimmt aber in dem entscheidenden Punkt (Empfängerbezug) überein.

[9] Klaus Lenk, Der Staat am Draht, 2004, S. 33 f. Zu der „semiotischen Leiter" Zeichen – Daten – Information – Wissen vgl. Lenk/Meyerholt/Wengelowski, Wissen managen in Staat und Verwaltung, 2014, S. 35 ff. – Ein rein „objektiver" Informationsbegriff, der etwa auf Qualität, Inhalt oder Wert des Mitgeteilten abstellt, mag in anderen Zusammenhängen sinnvoll erscheinen, aber nicht als Element eines Rechts der Informations*beziehungen* wie des Datenschutzes.

[10] Lenk aaO. (Fn. 9).

wie ein Musikstück immer wieder unterschiedlich interpretiert wird. Der Kontext gibt der Information daher ihren Gehalt."

Durch Weitergabe der Information an ein anderes Informationssubjekt kann sich ihre Bedeutung ändern; unter Umständen geht der Sinn ganz verloren. Lenk zitiert dazu den Computerpionier Heinz Zemanek:

„Nur die Zeichenketten der Information hat die Informationstechnik in ihrem elektronischen Griff – ihre Bedeutung begleitet die Zeichen wie eine Wolke, sie schwebt um die Ketten herum. Dieses Bild aus der Barockzeit eignet sich hervorragend dazu, die Transparenz der Bedeutung und die Schwierigkeiten ihrer Erfassung im Bewusstsein zu halten."[11]

Damit ist deutlich, dass die maschinelle Verarbeitung von Daten erhebliche Risiken für das richtige, nämlich das ursprünglich (von dem Informationssender) intendierte *Verstehen* der gespeicherten Informationen mit sich bringt. Die elektronischen Prozesse der Speicherung und des Abgleichs von Datenmengen erfolgen *schematisch*, nach zuvor festgelegten Merkmalen, so dass die Empfänger bei der Auswertung auf diese Merkmale festgelegt sind (die natürlich ihrerseits auslegungsfähig sind). Schon bei konventioneller Informationsübermittlung gilt: „Missverständnisse sind vorprogrammiert, wenn eine übermittelte Information auf einen anderen Verständnishorizont trifft".[12] Erst recht besteht diese Gefahr bei der elektronischen Massendatenverarbeitung. Ein typisches Beispiel bildet die Einbeziehung von „Kontaktpersonen" in polizeiliche Datensammlungen: Der Beamte, die eine Person in diese Gruppe einordnet, hat möglicherweise

[11] Heinz Zemanek, Das geistige Umfeld der Informationstechnik, 1992, S. 168; zitiert nach Lenk (Fn. 9) S. 34.

[12] Lenk (Fn. 9) S. 35.

ganz andere Vorstellungen als derjenige, der diesen Datensatz später im Rahmen eigener Ermittlungen abruft. Bei Benutzung dieser Kategorie ist also die genaue Erfassung des relevanten Zusammenhangs äußerst schwierig oder sogar unmöglich.

Es bedarf *gemeinsamer Vorverständnisse*, um Datensammlungen sinnvoll zu nutzen.[13] Oft sind sie zumindest teilweise gegeben, so wenn die Beteiligten eine gemeinsame Ausbildung oder Sozialisation aufweisen oder eine Behörden- oder Firmenkultur das Verständnis lenkt. „Hierarchische Setzungen" etwa durch Geschäftsordnungen oder Handbücher[14] können dazu beitragen, fördern aber letztlich ebenfalls das schematische Denken statt der konkret-individuellen Bedeutungssuche.

Unter den Informationen, die sich bei den Empfängern ansammeln, sind regelmäßig viele, die für das Informationssubjekt *keinen Wert* haben. Ständig werden unzählige Daten und Informationen produziert, weil die maschinellen Abläufe so gestaltet sind, dass jeder elektronische Schritt aufgezeichnet werden muss, und künftig wird in steigendem Maß auch die rein technische „Kommunikation" zwischen Minicomputern (RFID) dokumentiert werden. Die Aufzeichnung eines technischen Vorgangs in einer Maschine ist in aller Regel für Betroffene ebenso irrelevant und uninteressant, wie es die technischen Betriebsdaten des eigenen Autos oder die Vorgänge im privaten Computer sind: Man braucht sie nicht zu kennen, man überlässt ihre Auswertung (wenn sie denn nötig wird) den Experten. Relevant sind nur die Daten, die einen Informationsgehalt über die technischen Abläufe hinaus haben.

---

[13] Vgl. nochmals Lenk (Fn. 9) S. 35.
[14] Lenk aaO.

Die „Inhaltsdaten" müssen – wenn denn ein Anlass dazu besteht – aus den Unmengen automatisch aufgezeichneter „Verkehrsdaten" herausgesucht werden. Alle anderen müssen „aus dem Verkehr gezogen", also gelöscht werden; sonst sind die Datenspeicher in kurzer Zeit nicht mehr benutzbar. Erst nach dieser ersten Filterung wird die Speicherung interessant.

Das gilt für den Normalfall, vermutlich für mehr als 99 Prozent aller technischen Aufzeichnungen, z. B. Leistungs- und Energieverbrauchsdaten in Autos, Strommessgeräten („smart metering"), Computern aller Art. Es wird aber viel darüber nachgedacht, welche Erkenntnisse über die Nutzer aus solchen technischen Aufzeichnungen gewonnen werden können, wenn jemand sich vornimmt, sie mittels raffinierter Annahmen über menschliche Verhaltensweisen (Wahrscheinlichkeiten, statistische Häufigkeit) auf verborgene Inhalte zu durchforschen. Es gehört zu den Merkwürdigkeiten der Datenschutzdiskussion, dass derartige Spekulationen zum Maßstab für die Beurteilung alltäglicher Vorgänge gemacht werden. Man erklärt seltene Ausnahmefälle für „typisch" und überlegt, welche rechtlichen Hürden dagegen erforderlich sein könnten. Diese Methode führt zu einer Hypertrophie der Vorsorge.

Aus Informationen kann *Wissen* werden. Aber Informationen sind nicht mit Wissen gleichzusetzen. Die Maschine, die die Daten und damit auch die Informationen speichert, „weiß" selbst gar nichts, und ebenso wenig weiß „das Internet" etwas über seine Benutzer. Der Mensch, der die Informationen zur Kenntnis nimmt und nutzt, baut sein Wissen aus den Informationsmengen auf, indem er sie filtert, überprüft, strukturiert und mit den vorhandenen Beständen abgleicht. Nur das nach solchen

Prüfungen für richtig und nützlich gehaltene Wissen führt die Menschheit auf den Weg des Fortschritts – und vielleicht sogar den einen oder anderen zur individuellen Weisheit. Solange die neuen Möglichkeiten der Informations- und Kommunikationstechnik nicht „klug und souverän" genutzt werden, leben wir nicht in einer „Wissensgesellschaft".[15]

Informatiker und Ökonomen betonen angesichts des Phänomens „Big Data", dass die automatisierte Auswertung der riesigen vorhandenen Informationsmengen mit Hilfe hochentwickelter Algorithmen zunehmend neue, originelle und mit menschlicher Intelligenz nicht erlangbare Erkenntnisse (insbesondere Korrelationen, angeblich aber auch Wahrscheinlichkeiten) produziere. Das trifft wohl für manche naturwissenschaftliche Forschungen zu, aber ob es auch für sozialwissenschaftliche Aussagen gilt, ist zweifelhaft. Der Beitrag, den der Mensch auch in diesen Konstellationen tatsächlich leistet, darf jedenfalls nicht unterschätzt werden. Denn auch die interessanteste Ausschöpfung des Datenbergwerks setzt voraus, dass jemand Fragen, Thesen oder Vermutungen formuliert, und eben dies kann die künstliche Intelligenz der Maschinen nicht. Die Qualität der technisch generierten Aussagen hängt letztlich nicht von der Menge der verarbeiteten Daten, sondern von der Plausibilität der zugrunde gelegten Annahmen über menschliches Verhalten ab.

2. Personenbezug

Eine wichtige Abschichtung im geltenden Datenschutzrecht ist die zwischen der Gesamtheit der gespeicherten

[15] Schoch (Fn. 8), VVDStRL 57 (1998), S. 158 ff. (167 f. Fn. 32).

und genutzten Daten und den „personenbezogenen" Daten. Um „Sachdaten" kümmert sich das Datenschutzrecht nicht. Dafür gelten unter bestimmten Umständen andere Regelungen, die z. B. die wirtschaftliche Nutzung von Daten zulassen oder einschränken – eine Funktion, die für Staat und Wirtschaft große Bedeutung haben kann; man denke nur an Geodaten oder Wetterprognosen.

Beim Datenschutz geht es um den Schutz von Interessen der Einzelnen. Sie sind die „Betroffenen" (nicht zu verwechseln mit den „Informationssubjekten", von denen soeben die Rede war, also den Menschen, die eine Information zur Kenntnis nehmen). Der Kreis der Betroffenen kann weit oder eng gezogen werden. Betroffen von der Datennutzung sind gewiss nicht nur die namentlich bezeichneten Personen, es genügt vielmehr, dass die Betroffenen „bestimmbar" sind. Das Gesetz lässt es aber offen, auf welche Weise diese Verknüpfung hergestellt wird. Wer den von einer Information Betroffenen bestimmen will, benötigt Zusatzwissen; davon haben manche viel, manche wenig oder gar nichts. Wenn die Betroffenen gegen Fehlgebrauch „ihrer" Informationen gut geschützt sein sollen, müssen die rechtlichen Schutzvorschriften auch dann angewendet werden, wenn die Nutzer einen gewissen Aufwand betreiben müssen, um die Identität festzustellen. Vor denen, die weiter gar nichts über mich wissen als eine triviale Angabe – z. B. meinen Geburtstag –, braucht mich das Gesetz kaum zu schützen, wohl aber (wenn die sonstigen Voraussetzungen zutreffen) vor denen, die schon andere Informationen über mich besitzen und die neuen damit verbinden können. Andererseits soll das Gesetz allgemein gelten und darf nicht von vornherein die bestinformierten Datenempfänger privilegieren. Daraus folgt, dass der Personenbezug sehr weit ausgelegt werden muss,

Sachregister