Humboldt-Universität zu Berlin
Institut für Informatik
Informatik in Bildung und Gesellschaft

Datenschutzrecht in der BRD
Eine Einführung

Jörg

SE Überwachungstechnologien und informationelle Selbstbestimmung

Leitung: Constanze Kurz

25. Juli 2007

Für Anna und Artur.

Inhaltsverzeichnis

1 Einführung

Während einerseits der Schutz persönlicher Daten schon vor fast 2500 Jahren eine Regelung im Hippokratischen Eid[1] fand und der Selbstdatenschutz durch Verschlüsselung von Texten sogar seit fast 4000 Jahren[2] bekannt ist, ist das Datenschutzrecht selbst ein „modernes“ Rechtsgebiet. Erst die deutliche Zunahme der Datenverarbeitung, deren Automatisierung und nicht zuletzt die negativen Erfahrungen mit staatlicher Datensammelwut und Datennutzung im Faschismus[3] haben die Notwendigkeit eines eigenständigen Rechtsgebietes deutlich gemacht.

Drei Entwicklungslinien kennzeichnen das Datenschutzrecht heute. Erstens natürlich die fortschreitende technologische Entwicklung und die damit entstandenen Möglichkeiten, immer mehr Daten in immer kürzerer Zeit zu speichern und automatisiert zu verarbeiten. Zweitens sind die staatlichen Eingriffsmöglichkeiten und -befugnisse zu nennen, deren Gefahr erst maßgeblich zur Entwicklung des Datenschutzrechtes beitrug, dann zugunsten der zunehmend privat organisierten Datenverarbeitung in den Hintergrund trat und seit Ende der neunziger Jahre des zwanzigsten Jahrhunderts – und nicht erst, wie so häufig kolportiert wird, nach dem 11. September 2001 – wieder stark anstieg. Und drittens gerade die privaten Unternehmen, deren Datensammlungen im Gegensatz zu den staatlichen nicht durch Zwang ausgebaut werden sondern durch Verführung. Sirenen gleich umgarnen sie die Kundinnen und Kunden: „Gib uns Deine Daten. Auch Du hast einen Vorteil davon. Wir geben Dir Rabatt. Du erhälst Geschenke. Es ist nur zu Deinem Besten.“

Aus der Möglichkeit der vollständigen informationellen Erfassung der Bürgerinnen und Bürger erlangen staatliche und private Stellen Informationsmacht über die Betroffenen. Um diesen dennoch eine autonome Lebensgestaltung zu ermöglichen, die selbst wiederum Grundlage einer freien Entfaltung ihrer Persönlichkeit ist, muss die Privatsphäre, und damit das Recht auf informationelle Selbstbestimmung, geschützt werden. Mit dieser Arbeit soll versucht werden, die geschichtliche Entwicklung des deutschen Datenschutzrechts[4] seit ihren Anfängen Ende der sechziger Jahre zu beleuchten und gleichzeitig eine Einführung zu geben in die Grundzüge des Bundesdatenschutzgesetzes, eine Erläuterung unterschiedlicher Regelungen für öffentliche und private Stellen sowie eine Darstellung der Rechte der Betroffenen. Die Natur einer Einführung in diese Materie erfordert eine Fokussierung auf die grundsätzlichen Regelungen, mithin eine Einschränkung auf das Bundesdatenschutzgesetz (BDSG).[5]

[1] „Was ich bei der Behandlung sehe oder höre oder auch außerhalb der Behandlung im Leben der Menschen, werde ich, soweit man es nicht ausplaudern darf, verschweigen und solches als Geheimnis betrachten.“ Zitiert nach http://www.datenschutz-berlin.de/doc/gr/hippo.htm.

[2] Das behauptet zumindest Wikipedia unter dem Eintrag „Kryptografie“ in: Wikipedia, Die freie Enzyklopädie. Bearbeitungsstand: 24. Aug 2006, 12:44. URL: http://de.wikipedia.org/w/index.php?title=Kryptografie&oldid=20584431 (Abgerufen: 1. September 2006, 13:27).

[3] Vergl. die Organisation des Holocaust mit Maschinen der IBM-Tochter DEHOMAG oder die von den Faschisten ausgenutzte Registrierung der norwegischen Jüdinnen und Juden ab 1866.

[4] Von Ausnahmen abgesehen wird sich die Arbeit ausschließlich mit dem Datenschutzrecht der BRD befassen.

[5] Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), geändert durch § 13 Absatz 1 des Gesetzes vom 5. September 2005 (BGBl. I S. 2722).

1.1 Zum Begriff des Datenschutzes

1.1.1 Datenschutz im weiteren Sinne

Wie es im bekannten „Volkszählungs-Urteil“ des Bundesverfassungsgerichts von 1983 heißt, umfasst das Persönlichkeitsrecht nach Art. 2 Abs. 1 Grundgesetz (GG) „auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.“[6] Dieser Leitgedanke ist nicht nur wesentliche Grundlage für die Begründung des Rechts auf informelle Selbstbestimmung, sondern beschreibt gleichzeitig den Rahmen des Datenschutzes im weiteren Sinne.

Gesetzlich konkretisiert wurde in diesem Zusammenhang zuerst das Recht am eigenen Bild, das in den §§ 22ff. Kunsturhebergesetz (KUG) geregelt ist. Noch älter sind berufsständische Geheimhaltungspflichten wie das standesrechtlich geregelte Arztgeheimnis, das kirchenrechtlich normierte Beichtgeheimnis oder die anwaltliche Schweigepflicht sowie das Bankgeheimnis, bei dem es sich um eine vertragliche oder vorvertragliche Nebenpflicht handelt. Daneben existieren auch Geheimhaltungspflichten für bestimmte (amtliche) Sachbereiche. Dazu zählen etwa das Sozialgeheimnis nach § 35 1. Sozialgesetzbuch (SGB I), das Statistikgeheimnis nach § 16 Bundesstatistikgesetz (BStatG), das Steuergeheimnis gemäß § 30 Abgabenordnung (AO) oder das Meldegeheimnis gemäß § 5 Absatz 1 Melderechtsrahmengesetz (MRRG). Diese Regelungen sind nicht zahnlos, sie werden flankiert von einem strafrechtlichen Geheimnisschutz – dem Berufsgeheimnis gemäß § 203 Abs. 1 Strafgesetzbuch (StGB) und dem Amtsgeheimnis gemäß § 203 Abs. 2 und Abs. 3 StGB. –, einem Zeugnisverweigerungsrecht gemäß § 53 Strafprozessordnung (StPO) und einem Beschlagnahmeverbot gemäß § 97 StPO. Weiterhin gibt es Regelungen zum speziellen Geheimnisschutz auch oft in Arbeitsverträgen oder sie folgen aus Art. 10 GG.

1.1.2 Datenschutz im engeren Sinne

Als Datenschutz im engeren Sinne gelten nur die Datenschutzgesetze. Hier ist in erster Linie das Bundesdatenschutzgesetz (BDSG) zu nennen, dem auf Landesebene die Landesdatenschutzgesetze beigestellt sind. Daneben gibt es spezielle Regelungen für sachlich abgegrenzte Bereiche. Dazu zählen das Gesetz über den Datenschutz bei Telediensten (Teledienstedatenschutzgesetz – TDDSG) und der Staatsvertrag über Mediendienste (Mediendienste-Staatsvertrag – MDStV).

1.2 Geschichte des Datenschutzes

Die Geschichte des Datenschutzes im modernen Sinne beginnt Mitte der sechziger Jahre des zwanzigsten Jahrhunderts in den USA, als in breitem Maße die elektronische Datenverarbeitung Einzug hielt. Zwei Problemkomplexe begründeten die öffentliche Debatte über die Gefahren, die dadurch für den Einzelnen auftreten konnten. Einerseits kam es wiederholt zu Fehlern bei der Verarbeitung personenbezogener Daten, die insbesondere auch dann Eingang in die Berichterstattung der Presse fanden, wenn es sich um Fehler bei der Feststellung der individuellen Kreditwürdigkeit handelte. Diese Computerfehler führten unter

[6] BVerfGE 65, S. 1ff., C. II. 1. a).

anderem zu Abschaltungen des Stromes bei vermeintlich säumigen oder zahlungsunfähigen Schuldnern oder zur Nichtgewährung von Krediten, was bei einer auf Kredit basierenden Wirtschaft schwerwiegende Konsequenzen für die Betroffenen bedeutete.[7] Andererseits gab es Bestrebungen, „eine Nationale Datenbank zur Erfassung aller verfügbaren Informationen über Bürger und Bürgerinnen der Vereinigten Staaten“[8] einzurichten. Dieses Ansinnen traf auf scharfen Widerstand in der Öffentlichkeit, insbesondere als bekannt wurde, dass bereits zahlreiche individuelle Dossiers über eine Vielzahl von Menschen existierten, und diese Datenbestände in der Nationalen Datenbank vereinigt werden sollten.

Die Angst vor der totalen Überwachung durch einen omnipräsenten und allwissenden „Großen Bruder“ im Orwellschen Sinne nahm plötzlich reale Gestalt an. Die lange US-amerikanische Tradition eines sich nicht in die privaten Belange seiner Bürgerinnen und Bürger einmischenden Staates, die sich auch in der Definition von Privatheit als „Recht, allein gelassen zu werden“ (*right to be let alone*) oder der Ablehnung eines einheitlichen Personaldokumentes manifestierte, schien ein Ende gefunden zu haben. Dennoch konnten sich die Kritikerinnen und Kritiker damals noch durchsetzen und so verschwand diese Idee vorläufig wieder in der Versenkung.[9] Die in diesem Zusammenhang geforderten Datenschutzregelungen mündeten schließlich in den „Privacy Act 1974“, jedoch galt dieses nur für staatliche Bundesbehörden, nicht aber für andere öffentliche oder gar private Stellen. Das Gesetz untersagte die Zweckentfremdung von personenbezogenen Daten und räumte Betroffenen Benachrichtigungs-, Auskunfts- und Berichtigungsansprüche sowie ein grundsätzliches Schadensersatzrecht gegenüber diesen Behörden ein.[10] Im gleichen Jahr wurde nach den Erfahrungen aus dem Watergate-Skandal der „Freedom of Information Act“ grundlegend überarbeitet – das „Recht auf Information“ einer „informierten Öffentlichkeit“ sollte also in Ergänzung eines „Rechts auf Privatheit“ garantieren, dass die Bürgerinnen und Bürger den Staat kontrollieren können, dieser seine Bürgerinnen und Bürger jedoch nicht.

1.2.1 Der „Mikrozensus“-Beschluss des BVerfG

Bevor im Jahre 1970 das Bundesministerium des Innern einen Forschungsauftrag an die Universität Regensburg mit dem Ziel erteilte, ein Datenschutzkonzept[11] zu erarbeiten, fasste das Bundesverfassungsgericht zwei richtungsweisende Beschlüsse zum sich herausbildenden Datenschutz: den „Mikrozensus“-Beschluss 1969 und den „Scheidungsakten“-Beschluss 1970.

Der Erste Senat des BVerfG hatte zu entscheiden, ob Teile des Mikrozensusgesetzes in der Fassung vom 05.12.1960 gegen Art. 1 und Art. 2 GG verstoßen, weil die Verpflichtung zur Beantwortung von Fragen über Urlaubs- und Erholungsreisen nach Ansicht des Amtsgerichts (AG) Fürstenfeldbruck die Intimsphäre der Befragten verletzte. Im Ausgangsverfahren hatte eine Frau gegen einen Bußgeldbescheid Klage erhoben, der gegen sie wegen der Nichtbeantwor-

[7] *Tinnefeld et al.*, Datenschutzrecht, S. 79.

[8] *Tinnefeld et al.*, Datenschutzrecht, S. 80.

[9] Diese Aussage gilt jedoch nicht absolut. Bereits lange vorher sammelte das FBI ausführliche Informationen über politische Gegnerinnen und Gegner wie Mitlieder der Communist Party oder der Black Panthers. Und spätestens seit „9/11“ ist der Widerstand gegen exzessives Datensammeln weitgehend marginalisiert.

[10] *Tinnefeld et al.*, Datenschutzrecht, S. 81.

[11] *Steinmüller et al.*, Grundfragen des Datenschutzes, BT-Drucksache 6/3826 Anlage 1.

tung der Fragen zu Urlaubs- und Erholungsreisen im Rahmen der Durchführung des Mikrozensus festgesetzt war und das AG Fürstenfeldbruck machte die Entscheidung über diese Klage von der Verfassungsmäßigkeit des Mikrosensusgesetzes abhängig.

Das BVerfG entschied am 16.07.1969, dass die Regelungen im Mikrozensusgesetz „weder gegen Art. 1 Abs. 1 und Art. 2 Abs. 1 GG noch gegen andere Bestimmungen des Grundgesetzes“[12] verstießen. Gleichwohl setzte das Gericht Grenzen: Weil das Grundgesetz dem einzelnen Bürger einen unantastbaren Bereich prvater Lebensgestaltung gewähre, der der Einwirkung der öffentlichen Gewalt entzogen sei,[13] widerspreche es der menschlichen Würde, den Menschen zum bloßen Objekt im Staat zu machen.[14] „Mit der Menschenwürde wäre es nicht zu vereinbaren, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist.“[15] Im Zusammenhang mit statistischen Befragungen führte das Gericht aus: „Eine statistische Befragung zur Person kann deshalb dort als entwürdigend und als Bedrohung des Selbstbestimmungsrechtes empfunden werden, wo sie den Bereich menschlichen Eigenlebens erfaßt, der von Natur aus Geheimnischarakter hat, und damit auch diesen inneren Bezirk zu statistisch erschließbarem und erschließungsbedürftigem Material erklärt.“[16] Weil die Befragung zu Urlaubs- und Erholungsreisen weder zur Offenlegung der Intimsphäre zwinge noch die einzelnen Details Geheimnischarakter besäßen und sich alle Daten auch ohne die Betroffenen ermitteln ließen, sei die Menschenwürde nicht beeinträchtigt und daher sei das Mikrozensusgesetz verfassungsgemäß.

Ein gutes halbes Jahr später, am 15.01.1970, fällte das BVerfG den „Scheidungsakten“-Beschluss. Gegen einen im Ruhestand befindlichen Oberstadtdirektor wurde ein Disziplinarverfahren wegen des Verdachts der Unterhaltung eines „ehebrecherischen Verhältnisses“ durchgeführt. Der Untersuchungsführer im Disziplinarverfahren erbat im Wege der Rechts- und Amtshilfe bei der zuständigen Zivilkammer die Akten aus dem Ehescheidungsverfahren des Beschuldigten zur Einsichtnahme, die ihm auch – ohne Kenntnis oder Einwilligung des betroffenen Ehepaares – gewährt wurde. Nachdem der Betroffene von dem Vorgang Kenntnis erhalten hatte, klagte er vor dem Oberlandesgericht (OLG) Hamm gegen die Herausgabeverfügung. Die Klage wurde abgewiesen, der Betroffene machte vor dem BVerfG die Verletzung seiner verfassungsmäßigen Rechte geltend. Das BVerfG erklärte, der Beschluss des OLG verletze den Betroffenen in seinem Grundrecht aus Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG, hob den Beschluss auf und verwies die Sache zurück an das OLG Hamm.[17]

Im Urteil wird der datenschutzrechtliche Erlaubnisvorbehalt definiert. Danach dürfen schutzwürdige personenbezogene Daten nur aufgrund von Gesetzen oder mit der Einwilligung der Betroffenen verarbeitet werden. Bei der Anwendung der Gesetze muss zudem immer das Verhältnismäßigkeitsprinzip beachtet werden.

[12] BVerfGE 27, 1, 5.
[13] BVerfGE 6, 32, 41.
[14] BVerfGE 5, 85, 204.
[15] BVerfGE 27, 1, 6.
[16] BVerfGE 27, 1, 7.
[17] BVerfGE 27, 344.

1.2.2 Die ersten Datenschutzgesetze

Bereits 1969 hatte der damalige Chef der Hessischen Staatskanzlei und spätere erste Hessische Datenschutzbeauftragte, Birkelbach, den Auftrag gegeben, „das Modell einer besonderen, neutralen und unabhängigen Instanz zu entwerfen“, um den Risiken von „Herrschaftsbegünstigung und einseitiger Informationsmacht“ durch die elektronische Datenverarbeitung zu begegnen.[18] Ende 1970 wurde dann das erste deutsche Datenschutzgesetz in Hessen verabschiedet,[19] es war gleichzeitig auch weltweit das erste.[20] Nach einer fast sechs Jahre dauernden Diskussion über Notwendigkeit und Inhalt einer gesetzlichen Regelung der Verarbeitung personenbezogener Daten wurde am 12.11.1976 dann das Bundesdatenschutzgesetz (BDSG) im Bundestag beschlossen.[21] In der Folge wurden in allen (damaligen) Bundesländern Landesdatenschutzgesetze beschlossen, zuletzt 1981 in Hamburg.

In dem Versuch, einerseits sämtliche Verarbeitungssituationen (von personenbezogenen Daten) einzubeziehen, andererseits jedoch den Regelungsgegenstand bewusst unscharf zu halten, um der sich rasant entwickelnden Technologie gewappnet zu sein, wurde das BDSG zu einer Ansammlung von Generalklauseln.[22] Gleichzeitig wurde im BDSG – und in den meisten anderen Landesdatenschutzgesetzen, zu den Ausnahmen gehörte das HDSG – Datenschutz und Informationsfreiheit[23] getrennt und damit ein Problem geschaffen, das bis heute fortwirkt: Datenschutz und Informationsfreiheit können gegeneinander ausgespielt werden. Dem Verlangen nach freiem Zugang zu den Verwaltungsunterlagen kann so allzuoft unter Verweis auf den „Datenschutz“ entgegengetreten werden.[24]

1.2.3 Das Volkszählungsurteil des BVerfG

Das Urteil des BVerfG vom 15.12.1983 stellt eine Zäsur in der Geschichte des Datenschutzes dar. Seine Bedeutung weist weit über den eigentlichen Regelungsgegenstand – das Volkszählungsgesetz 1983 – hinaus, es gewinnt seine Tragweite vor allem aus dem Symbolwert der für 1983 geplanten Volkszählung selbst. Obwohl die erfragten Informationen weit weniger detailliert sein sollten und damit auch viel weniger in die Privatsphäre der Bürgerinnen und Bürger eingreifen würden als beim Mikrozensus 1963,[25] wurde die Volkszählung zum Kristallisationspunkt aller Ängste und Befürchtungen, die sowohl die technologische Entwicklung im Allgemeinen als auch die damit erleichterten Datenverarbeitungs- und Kontrollmöglichkeiten im Besonderen weckten.[26] Neben die bisher nur individuell gemachten Erfahrungen mit der Informationssammlung durch Behörden trat eine kollektive Komponente: alle Bürgerinnen und Bürger unterlagen der

[18] *Hassemer et al.*, 25 Jahre Datenschutz, S. 14ff.

[19] Hessisches Datenschutzgesetz (HDSG) vom 6.10.1970.

[20] *Simitis* in BDSG, Einleitung, Rn. 1.

[21] „Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung“, BGBl. I, S. 201.

[22] *Simitis* in BDSG, Einleitung, Rn. 20.

[23] Im HDSG sowie allgemein bis in die achziger Jahre wurde darunter zunächst nur die Freiheit der parlamentarischen Opposition verstanden, an die Daten der Regierung ohne deren Genehmigung gelangen zu können.

[24] *Simitis* in BDSG, Einleitung, Rn. 21ff.

[25] Vergl. 1.2.1.

[26] *Simitis* in BDSG, Einleitung, Rn. 27ff.

gleichen Informationspflicht zum gleichen Zeitpunkt. Das tiefe Misstrauen gegenüber einer weder in ihrer Technizität noch in ihren Konsequenzen vollständig durchschaubaren Informationstechnologie und die „Furcht vor einer unkontrollierten Persönlichkeitserfassung“[27] durchzog dabei alle Bevölkerungsgruppen, unabhängig von Beruf, Einkommen, sozialer Stellung, Bildungsgrad oder politischer Überzeugung. Die Dystopie Orwells schien am Vorabend des Jahres 1984 Realität zu werden.

Eine Beurteilung der Entscheidung muss dennoch aus verschiedenen Gründen ambivalent ausfallen.

Rechtsdogmatisch hat das Gericht mit diesem Urteil mitnichten juristisches Neuland betreten. Dass Einschränkungen von Grundrechten einer ausdrücklichen gesetzlichen Grundlage bedürfen, war zu diesem Zeitpunkt eine bereits seit Jahrzehnten gefestigte Rechtsprechung des BVerfG.[28] Dass dies auch für den Umgang mit personenbezogenen Daten gilt, hat das Gericht auch schon im „Scheidungsakten“-Beschluss[29] festgestellt, genauso wie das Erfordernis der strengen Zweckbindung für die Erhebung und Verarbeitung personenbezogener Daten und den Vorrang der Selbstauskunft. Auch das „Recht auf informationelle Selbstbestimmung“, das das Gericht als Teil des allgemeinen Persönlichkeitsrechtes nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zur Grundlage seiner Ausführungen gemacht hat, war zu diesem Zeitpunkt weder neu noch umstritten. Allerdings ist es dem Gericht hier gelungen, Inhalt und Schranken dieses Grundrechts ausführlich zu erläutern.[30]

Politisch war das Urteil verheerend. Der Widerstand der Boykottbewegung, die durchaus in weiten Teilen die gesamte parlamentarische Willensbildung und Entscheidungsfindung in Frage stellte und delegitimierte, wurde durch die Verrechtlichung der immanent politischen Auseinandersetzung gezähmt.[31] Und so verschwand die Boykottbewegung nach dem Urteil von der politischen Bühne, obwohl das BVerfG weder jede Volkszählung – vor allem nicht jede andere Datensammlung – verboten hatte noch die Kompetenz des Staates zur Erhebung und Erfassung von Daten auch nur unwesentlich reduziert, sondern maximal kanalisiert hatte.[32] Letztendlich wurden damit die „Lebensinteressen“, hier das Recht auf informationelle Selbstbestimmung, mit Systemerhaltungs- und Systembestandsinteressen „kompatibel gemacht“, also de facto eingeschränkt.[33]

Einerseits behauptet Bull, weil das Gericht verlangt habe, dass die Datenverarbeitung überschaubar und dabei kontrollierbar bleiben muss, auch und gerade durch den Einzelnen, ließe sich daraus ableiten, dass die staatliche Datenverarbeitung insgesamt verfassungswidrig wird, „wenn der Bürger keine halbwegs zutreffende Vorstellung mehr von ihren Methoden haben kann.“[34] Dieser „point of no return“ müsse politisch definiert werden und wurde nach Bulls Meinung schon mit der Einführung der maschinenlesbaren Personalausweise erreicht.[35] Andererseits erkennt er, dass der hinhaltende Widerstand all jener, die gegen eine umfassende Neuregelung der Informationsverarbeitung waren, erfolgreich

[27] BVerGE 65, 1, 41.
[28] Keine Ahnung, aber wahrscheinlich „Lüth“, oder?
[29] BVerfGE 27, 344.
[30] *Schapper et al.*, Informationelle Selbstbestimmung, S. 317.
[31] *Massing*, Verrechtlichung, S. 98ff.
[32] *Bull*, Hoffnungen und Enttäuschungen, S. 174.
[33] *Massing*, Verrechtlichung, S. 104.
[34] *Bull*, Hoffnungen und Enttäuschungen, S. 176f.
[35] *Bull*, Hoffnungen und Enttäuschungen, S. 178.

war.[36] Damit folgt er dem damaligen Hamburgischen Datenschutzbeauftragten Schapper, der meint, sie gaben „die Überlegungen des BVerfG als beiläufige und folgenlose Bemerkungen“ aus und setzten sich damit durch.[37] Denninger bezeichnet diese Art des Umgangs mit dem Beschluss als „gesetzförmlichen Grundrechtsleerlauf“ und führt aus: „Ein formal detaillistischer Regelungsperfektionismus verbindet sich mit einer minimalen inhaltlichen Befugnisbegrenzung, die jedenfalls den status quo einer an der Verwaltungseffizient orientierten Praxis absichert, wenn sie nicht vielmehr noch deren Möglichkeiten erweitert.“[38]

Nicht zuletzt muss dem BVerfG vorgehalten werden, mit seiner Fixierung auf die Datenverarbeitung durch öffentliche Stellen die tatsächliche Gefahr für die Betroffenen verkannt zu haben. „Alle reden von der Volkszählung, niemand von der SCHUFA.“[39]

Obwohl dem Gesetzgeber durch das Urteil des BVerfG eindeutige Vorgaben zur Ausgestaltung eines verfassungskonformen Datenschutzrechtes gemacht wurden, zog sich die Debatte über die Novellierung des BDSG bis Anfang der neunziger Jahre ergebnislos hin. Der Ende 1990 in Gesetzesform[40] gegossene und am 1.6.1991 in Kraft getretene Kompromiss zwischen öffentlichen und privaten Datensammlern war aus der Sicht der Datenschutzbeauftragten mehr als enttäuschend. Anstelle einer grundlegenden – auch inhaltlichen – Überarbeitung im Lichte des „Volkszählungs“-Urteils hatte der Gesetzgeber ausschließlich das Notwendigste getan und dabei gleichzeitig das Gefälle zwischen dem Datenschutzstandard im öffentlichen und privaten Bereich vergrößert. Wenn es zu Erweiterungen der Betroffenenrechte gegenüber privaten datenverarbeitenden Stellen kam, wurden gleichzeitig deren Befugnisse erweitert.[41]

1.2.4 Europäisierung des Datenschutzrechtes

Bereits 1976 fordert das Europaparlament den Rat zur Verabschiedung einer Datenschutzrichtlinie auf, aber erst 1995 kommt der Rat dieser Forderung nach. Am 24.10.1995 wird die Richtlinie „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ beschlossen.[42] Damit war der Gesetzgeber verpflichtet, innerhalb von drei Jahren die eigenen Datenschutzregelungen an die Vorgaben aus Brüssel anzupassen. Der gesetzte Termin war bereits weit überschritten, als am 23.5.2001 das neue EU-konforme BDSG in Kraft trat.[43]

Neben den sich aus der EU-Datenschutzrichtlinie zwingend ergebenden Gesetzesänderungen enthält das BDSG 2001 auch bereits einige Grundsätze eines modernen Datenschutzrechts. Dazu gehören bspw. der sog. Systemdatenschutz – Datenvermeidung und Datensparsamkeit, Datenschutz durch Technik oder Datenschutzaudits – und Ansätze zur Selbstregulierung.[44] Gleichzeitig blieb das Datenschutzgefälle zwischen dem öffentlichen und privaten Bereich bestehen.

[36] *Bull*, Hoffnungen und Enttäuschungen, S. 174.
[37] *Schapper*, Dritter Tätigkeitsbericht, S. 4.
[38] *Denninger*, Informationelle Selbstbestimmung, S. 128, so im Ergebnis auch *Bull*, Hoffnungen und Enttäuschungen, S. 182 und 192.
[39] *Schneider*, DÖV, S. 164.
[40] BGBl. I, S. 2954.
[41] *Gola et al.*, BDSG, Einleitung, Rn. 7.
[42] Richtlinie 95/46/EG.
[43] BGBl. I, S. 904.
[44] *Gola et al.*, BDSG, Einleitung, Rn. 12.

Dennoch lassen sich einige positive Entwicklungen nachzeichnen.

So wurde erstens der Anwendungsbereich des Gesetzes insbesondere für die Privatwirtschaft erweitert, sowohl sachlich als auch räumlich. Zweitens wurde mit der Ausweitung der Benachrichtigungspflicht und des Auskunftsrechts die Transparenz gegenüber den Betroffenen erweitert. Die Erweiterung von Verarbeitungseinschränkungen durch die gesetzliche Einräumung eines allgemeinen Widerspruchsrechts für die Betroffenen, die Geltung des Vorrangs der Direkterhebung auch im nichtöffentlichen Bereich und das weitgehende Verarbeitungsverbot „besonderer Arten" personenbezogener Daten sind ein dritter Eckpunkt der Novellierung, und viertens wurde die Position der Datenschutzbeauftragten bei der Datenschutzkontrolle gestärkt.

Die Entwicklung des deutschen Datenschutzrechts ist damit keineswegs abgeschlossen. Einerseits soll das Datenschutzrecht grundsätzlich überarbeitet und modernisiert werden, sowohl inhaltlich als auch im Hinblick auf die Übersichtlichkeit der Regelungen.[45] Andererseits steht der Datenschutz unter dauerndem Beschuss von Sicherheitspolitikern, deren Fabulieren einer allgemeinen und allumfassenden Terrorgefahr eine faktische Abschaffung des Datenschutz insbesondere für staatliche Überwachungsorgane einfordert.

2 Datenschutzrecht heute

2.1 Aufbau des BDSG

Das Bundesdatenschutzgesetz ist in sechs Abschnitte gegliedert. Im ersten Abschnitt werden die datenschutzrechtlichen Grundbegriffe definiert und für alle Datenverarbeiter geltende Normen festgelegt. Die Trennung der datenschutzrechtlichen Regelungen für öffentliche und nicht-öffentliche – also private – Stellen zeigt sich an den folgenden beiden Abschnitten. Während die Datenverarbeitung der öffentlichen Stellen im zweiten Abschnitt geregelt werden, enthält der dritte Abschnitt Regelungen für nicht-öffentliche Stellen und öffentlichrechtliche Wettbewerbsunternehmen. Der vierte Abschnitt regelt den Umgang mit Sondergeheimnissen sowie die Datenverarbeitung durch Forschungseinrichtungen und Medien. Bußgeld- und Strafvorschriften sind im fünften Abschnitt geregelt, der sechste Abschnitt enthält die Übergangsvorschriften, zu denen insbesondere die Weitergeltung von Begriffsbestimmungen aus früheren Fassungen des BDSG gehört.

2.2 Gesetzeszweck und Anwendungsbereich

Während das BDSG 77 die Betroffenen noch vor dem „Missbrauch" der personenbezogenen Daten schützen wollte, hat bereits das BDSG 90 den Zweck weiter formuliert. Das Gesetz soll jetzt den Betroffenen vor Beeinträchtigung in seinem Persönlichkeitsrecht – also dem Rechtsgut, als dessen Ausprägung das BVerfG das Recht auf informationelle Selbstbestimmung bestimmte – bereits beim „Umgang mit seinen personenbezogenen Daten" schützen. Obwohl in diesem Zusammenhang weder der Begriff „Datenschutz" noch der Begriff „informationelle Selbstbestimmung" benutzt wird – im Gegensatz zu den meisten

[45] *Gola et al.*, Grundzüge, S. 12f.

Landesdatenschutzgesetzen –, handelt es sich um identische Schutzzielbestimmungen.[46]

Das BDSG gilt beim Umgang mit personenbezogenen Daten sowohl für öffentliche Stellen des Bundes als auch der Länder, für letztere jedoch nur, wenn sie den „Datenschutz nicht durch Landesgesetz“ geregelt haben.[47] Auch nicht-öffentliche Stellen unterliegen den Regelungen des BDSG, wenn sie personenbezogene Daten „automatisiert oder dateigebunden“ verarbeiten. Dies gilt nicht, wenn die nicht-öffentlichen Stellen Daten „ausschließlich für persönliche Tätigkeiten“ erheben, verarbeiten oder nutzen.[48]

Mit Ausnahme des Verwaltungsverfahrensgesetzes sind alle Rechtsvorschriften des Bundes, die den Umgang mit personenbezogenen Daten regeln, dem BDSG vorrangig. Einerseits ist der Term „Rechtsvorschriften“ sehr weit gefasst und umfasst dabei sowohl Gesetze als auch Verordnungen. Andererseits gehen die bereichsspezifischen Regelungen nur dann vor, wenn ihre Tatbestandsbeschreibung genau deckungsgleich ist. In diesem Prinzip der Subsidiarität zeigt sich der Charakter des BDSG als Auffanggesetz.[49]

Auch räumlich ist das BDSG nicht immer einschlägig. So gilt es grundsätzlich für alle datenverarbeitenden Stellen, die in der Bundesrepublik ihren Sitz haben. Liegt der Sitz außerhalb der Bundesrepublik, jedoch in einem EU- oder EWR-Staat[50], dann gilt das BDSG nur, wenn die Daten in der BRD durch eine Niederlassung erhoben, verarbeitet oder genutzt werden. Liegt der Sitz in einem Drittland, dann gilt das BDSG in jedem Fall. Mit dieser Regelung soll verhindert werden, dass für personenbezogene Daten ein Datenschutzstandard gilt, der unterhalb der europäischen Normen liegt.[51] In jedem dieser Fälle, also gerade auch dann, wenn das BDSG nicht anwendbar ist, besitzen die Aufsichtsbehörden dennoch ein Kontrollrecht, falls die verantwortlichen Stellen in der Bundesrepublik personenbezogene Daten erheben, verarbeiten oder nutzen.

2.3 Öffentliche und nicht-öffentliche Stellen

Als öffentliche Stellen im Sinne des Gesetzes gelten die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen und Vereinigungen unbeachtlich ihrer Rechtsform. Soweit sie hoheitliche Aufgaben der öffentlichen Verwaltung übernehmen, gehören auch nicht-öffentliche Stellen dazu. Gleichzeitig gelten jedoch für öffentlich-rechtliche Vereinigungen, die „am Wettbewerb teilnehmen“[52], fast ausschließlich die Regelungen für die nicht-öffentlichen Stellen.

Dagegen gelten alle anderen natürlichen und juristischen Personen, Gesellschaften und sonstigen Personenvereinigungen, die nicht als öffentliche Stellen behandelt werden, als nicht-öffentliche Stellen.

Zwar gilt die Kompliziertheit dieser Regelungen zur Abgrenzung von öffentlichen und nicht-öffentlichen Stellen als Versuch, öffentliche Stellen an einer Flucht in die schwächeren Standards der Privaten zu hindern, aber das eigentli-

[46] *Gola et al.*, BDSG, § 1, Rn. 3.
[47] *Gola et al.*, Grundzüge, S. 37.
[48] *Gola et al.*, BDSG, § 1, Rn. 20f.
[49] *Gola et al.*, BDSG, § 1, Rn. 23f.
[50] Abkommen über den Europäischen Wirtschaftsraum
[51] *Gola et al.*, Grundzüge, S. 43f.
[52] Vergl. §§ 12, 27 BDSG.

che Problem wird dabei nicht angegangen: Der Datenschutzstandard bei nichtöffentlichen Stellen ist bedeutend geringer als bei öffentlichen.[53]

2.4 Definitionen im Datenschutzrecht

Die zentrale Rolle im Datenschutzrecht spielen die personenbezogenen Daten, die in § 3 Abs. 1 BDSG definiert sind als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person", womit gleichzeitig eine Definition für den Begriff „Betroffener" gegeben wird. Das BDSG schützt also nur lebende natürliche Personen, nicht jedoch Verstorbene oder juristische Personen.[54] Dabei sind jedoch alle Informationen über die Betroffenen geschützt, weil „es unter den Bedingungen der automatischen Datenverarbeitung kein ‚belangloses' Datum mehr"[55] gibt.

Neben den personenbezogenen Daten als solchen gibt es im Gesetz definierte „besondere Arten personenbezogener Daten", die aufgrund ihres sensitiven Charakters besonders geschützt werden müssen. Die Definition in § 3 Abs. 9 BDSG orientiert sich dabei am Diskriminierungsverbot der Europäischen Menschenrechtskonvention[56] und beinhaltet Eigenschaften, aufgrund derer Menschen in der Vergangenheit immer wieder diskrimiert wurden, wie „die ethnische oder rassische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben". Für diese Arten von personenbezogenen Daten gilt grundsätzlich ein Verarbeitungsverbot mit sehr eng gefassten Ausnahmetatbeständen.

Nicht immer werden Daten gebraucht, die sich auf eine bestimmte oder bestimmbare Person beziehen, während gleichzeitig der ursprüngliche inhaltliche Aussagegehalt erhalten bleiben soll. In einem solchen Fall können personenbezogene Daten anonymisiert werden, so dass sie hernach – mangels Personenbezug – nicht mehr unter die Bestimmungen des BDSG fallen. Anonymisieren im Sinne des BDSG bedeutet dabei gemäß § 3 Abs. 6 die Veränderung der 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 Person zugeordnet werden können", wobei der Aufwand auch dann unverhältnismäßig groß ist, wenn er das Risiko einer Bestrafung einschließt.[57] Anonymisierung von Daten kann also immer nur relativ sein.[58] Daten gelten jedoch dann als anonymisiert, wenn der Aufwand für eine Neubeschaffung der Daten geringer ist als der für die Wiederherstellung des Personenbezugs.[59]

Demgegenüber werden beim Pseudonymisieren der Name und andere Identifikationsmerkmale „durch ein Kennzeichen" ersetzt mit dem Ziel, „die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren", wie es in § 3 Abs. 6 a heißt. Die Herstellung von pseudonymen Daten und deren vorrangige Nutzung ist hierbei – gleiches gilt auch für anonymisierte Daten – ein Teil des Systemdatenschutzes, also der Durchsetzung von Datenschutz durch technische

[53] *Tinnefeld et al.*, Datenschutzrecht, S. 258f.
[54] *Gola et al.*, BDSG, § 3, Rn. 11f.
[55] BVerGE 65, 1, (genauer Ort fehlt noch).
[56] Art. 14 EMRK
[57] *Tinnefeld et al.*, Datenschutzrecht, S. 287.
[58] *Gola et al.*, BDSG, § 3, Rn. 44.
[59] *Tinnefeld et al.*, Datenschutzrecht, S. 288.

Verfahren und organisatorische Abläufe.[60]

Um verschiedene Regelungen für verschiedene Kontexte beim Umgang mit personenbezogenen Daten aufstellen zu können, hat der Gesetzgeber verschiedene Formen des Umgangs definiert und dabei gegeneinander abgegrenzt.

Als „Vorphase der Datenverarbeitung" – und damit explizit nicht als „Teil der Verarbeitung" – definiert das BDSG die „Erhebung von Daten". Als Erhebung gilt demnach gemäß § 3 Abs. 3 „das Beschaffen von Daten über den Betroffenen", wobei dieses zielgerichtet erfolgen muss. Dies soll dann nicht der Fall sein, wenn die Daten „bei zufälligen Beobachtungen" gewonnen oder „der verantwortlichen Stelle unaufgefordert zugeleitet" werden.[61]

Werden die Daten nicht direkt beim Betroffenen erhoben, muss dieser auf geeignete Weise informiert werden.[62] Allerdings ist die Liste der Ausnahmen von der Benachrichtigungspflicht ziemlich umfangreich und beinhaltet neben einigen staatlichen Stellen – vor allem Geheimdienste und Polizeibehörden – auch mögliche überwiegende ökonomische Interessen von nicht-öffentlichen Stellen.

Den größten Teil des Begriffs „Umgang" nimmt jedoch der Sammelbegriff „Verarbeiten" ein. Unter Verarbeiten versteht das Gesetz demnach die Phasen „Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten" und definiert diese dann in § 3 Abs. 4.

Dabei gilt Speichern als „das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung", wobei Erfassen das schriftliche und Aufnehmen das technische Fixieren der Daten meint. Der Begriff des Aufbewahrens ist hierbei sehr weit gefasst und umfasst z. B. auch Sicherungskopien, „die normalerweise nicht mehr verwendet werden sollen".[63]

Das inhaltliche Umgestalten von personenbezogenen Daten wird mit dem Begriff des Veränderns beschrieben, wobei das bereits dann der Fall ist, wenn der Kontext der Daten geändert wird, also Daten aus dem bisherigen Zusammenhang herausgenommen oder Daten aus verschiedenen Dateien neu verknüpft werden, und damit ein neuer Zusammenhang mit einem neuen Aussagewert entsteht.[64] Ist die Umgestaltung der Daten nicht inhaltlich, liegt kein Verändern vor. Daher gelten Löschen, Anonymisieren und Pseudonymisieren in der Regel auch nicht als Veränderung von Daten, es sei denn, dadurch entsteht eine Neuaussage.[65]

Übermitteln ist das Bekanntgeben der Daten durch die verantwortliche Stelle an Dritte durch Weitergabe der Daten oder die Nutzung von Möglichkeiten zur Einsichtnahme in die Daten durch Dritte. Die Weitergabe von Daten an den Betroffenen selbst, an Auftragnehmer oder eigene Mitarbeiter ist jedoch kein Übermitteln im Sinne des Gesetzes.[66]

Wenn personenbezogene Daten nicht mehr gebraucht werden oder gebraucht werden dürfen, können oder müssen sie je nach Einzelfall gesperrt oder gelöscht werden. Dabei werden die Daten gesperrt, d. h. sie werden gekennzeichnet als für die weitere Nutzung oder Verarbeitung eingeschränkt, wenn es eine diesbe-

[60] *Gola et al.*, Grundzüge, S. 47.
[61] *Gola et al.*, BDSG, § 3, Rn. 24.
[62] *Tinnefeld et al.*, Datenschutzrecht, S. 298.
[63] *Gola et al.*, BDSG, § 3, Rn. 26ff.
[64] *Tinnefeld et al.*, Datenschutzrecht, S. 300f.
[65] *Gola et al.*, BDSG, § 3, Rn. 31.
[66] *Gola et al.*, BDSG, § 3, Rn. 34.

zügliche Verpflichtung der datenverarbeitenden Stelle gibt oder bei Widerspruch des Betroffenen, gleichzeitig aber z. B. eine gesetzliche Aufbewahrungspflicht für die Daten existiert. Die Kennzeichnung muss dabei die Nutzungs- und Verarbeitungsmöglichkeiten tatsächlich einschränken, also organisatorisch und/oder technisch, indem die Datenträger z. B. getrennt aufbewahrt werden oder ein gesperrter Datensatz von einem Datenverarbeitungsystem nicht angezeigt wird. Ein einfacher Vermerk über die Sperrung reicht jedensfalls nicht.[67]

Der Begriff des Löschens ist im Gegensatz zum Begriff des Anonymisierens als absolut zu verstehen. Das „Unkenntlichmachen gespeicherter personenbezogener Daten" meint die physikalische Vernichtung der Daten, so dass sie nicht mehr rekonstruierbar sind. Eine Freigabe der Daten zum Überschreiben – nichts anderes vollziehen die meisten logischen Löschbefehle in der IT – ist demnach keine Löschung im Sinne des Gesetzes, genauso wie Daten nicht gelöscht sein können, wenn und so lange noch Sicherungskopien existieren.[68]

Innerhalb der Begrifflichkeit des Umgangs mit personenbezogenen Daten stellt das Nutzen einen Auffangtatbestand dar, der immer dann greifen soll, wenn eine bestimmte Verwendung der Daten nicht oder nicht eindeutig einer der Verarbeitungsphasen zugeordnet werden kann.[69] Nutzen ist also grundsätzlich jede Verwendung der Daten, wenn es sich nicht um Verarbeitung handelt.

Neben den Betroffenen werden im BDSG drei Gruppen von Stellen definiert, deren Verhalten beim Umgang mit personenbezogenen Daten geregelt werden soll.

Gemäß § 3 Abs. 7 BDSG ist verantwortliche Stelle „jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt". Verantwortliche Stelle ist dabei jeweils die gesamte Organisation, Behörde oder juristische Person, nicht nur z. B. deren Rechenzentrum.[70] Damit sich datenverarbeitende Stellen nicht ihrer datenschutzrechtlichen Verantwortlichkeit entziehen können, gelten Auftragnehmer bei der weisungsgebundenen Auftragsdatenverarbeitung „als fiktiver Teil der Auftrag gebenden [...] Stelle".[71] Damit handelt es sich in diesem Fall bei der Datenübertragung zwischen Auftraggeber und Auftragnehmer auch nicht um eine Übermittlung im Sinne des BDSG. Anders wird die sog. Funktionsübertragung behandelt, bei der der Auftragnehmer eigenverantwortlich agiert und die Verarbeitung personenbezogener Daten lediglich als Nebenzweck betroffen ist.[72] Hierbei stellt eine Datenübertragung sehr wohl eine Übermittlung im Sinne des Gesetzes dar und bedarf daher eines Erlaubnistatbestandes, z. B. einer gesetzlichen Regelung oder der Einwilligung des Betroffenen.[73]

Die Definition des Empfängers wurde bei der Novellierung neu in das Gesetz aufgenommen: „Empfänger ist jede Person oder Stelle, die Daten erhält." Dabei ist unbeachtlich, in welchem Verhältnis der Empfänger zur verantwortlichen Stelle steht, es kann sich also um untergeordnete Organisationseinheiten, Auftragnehmer bei der Auftragsdatenverarbeitung oder außenstehende Dritte

[67] *Tinnefeld et al.*, Datenschutzrecht, S. 303.
[68] *Tinnefeld et al.*, Datenschutzrecht, S. 303ff.
[69] *Gola et al.*, BDSG, § 3, Rn. 42.
[70] *Gola et al.*, BDSG, § 3, Rn. 48.
[71] *Gola et al.*, Grundzüge, S. 38.
[72] Die Abgrenzung zwischen Auftragsdatenverarbeitung und Funktionsübertragung (auch Outsourcing) ist in der Praxis häufig schwierig.
[73] *Gola et al.*, Grundzüge, S. 39.

handeln.[74]

Dritter im Sinne des Gesetzes ist jeder „außerhalb der verantwortlichen Stelle“ mit Ausnahme der Betroffenen und der Auftragsdatenverarbeiter, wenn dieser seinen Sitz innerhalb der EU hat.

2.5 Datenvermeidung und Datensparsamkeit

Im Rahmen der Novellierung 2001 wurde der Grundsatz der Datenvermeidung und Datensparsamkeit als § 3 a in das Gesetz aufgenommen, um – unter dem Konzept „Datenschutz durch Technik“ – die Gefahren für das informationelle Selbstbestimmungsrecht der Betroffenen bereits auf technischer Ebene zu mindern.[75] Allerdings gilt dieser Grundsatz als „unverbindliche, weil praktisch nicht zwangsweise durchsetzbare Zielvorgabe“[76], auch weil die Kontrollbehörden mangels Befugnissen nur „Anregungen“ geben können.[77]

Datenvermeidung meint das Verhindern der Erhebung personenbezogener Daten, indem z. B. nur anonymisierte Daten erhoben und verarbeitet werden, die Übermittlung nur von anonymisierten Daten an Dritte oder das frühzeitige Löschen personenbezogener Daten. Im Umfeld des Internets ist vor allem der Verzicht auf Cookies und ähnliche Identifizierungsverfahren datenvermeidend.[78]

Ist Datenvermeidung nicht möglich oder nicht erwünscht, sollen zumindest „so wenig personenbezogene Daten wie möglich“ verarbeitet werden. Dieses Ziel der Datensparsamkeit hat zwei Aspekte: Einerseits soll die Zahl der von der Datenverarbeitung betroffenen Personen minimiert werden, andererseits der Umfang der erhobenen Daten.[79] Da insbesondere letzterem ein beträchtliches ökonomisches Interesse entgegensteht, weil gerade eine große Informationstiefe als Voraussetzung individualisierter Werbung gilt, bleiben datensparsame Systeme weiterhin selten. Dabei gelten insbesondere solche Systeme als datensparsam, die eine pseudonyme Nutzung ermöglichen oder pauschal statt nutzungsabhängig abgerechnet werden (Flatrates).

2.6 Ermächtigungsgrundlagen

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten steht unter einem sog. Erlaubnisvorbehalt, d. h. sie ist nur zulässig, „soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.“[80] Die Alternativen lauten daher: Einwilligung, Normen des BDSG und andere Rechtsvorschriften.[81]

Eine Einwilligung ist gemäß § 4 a nur wirksam, wenn sie freiwillig erfolgt und die Betroffenen vorher über den Zweck der Erhebung, Verarbeitung und Nutzung der Daten unterrichtet wurden. Spätestens auf Nachfrage müssen die Betroffenen auch auf die Folgen der Verweigerung der Einwilligung hingewiesen werden. Die Einwilligung muss vor der Erhebung, Verarbeitung und Nutzung der

[74] *Gola et al.*, BDSG, § 3, Rn. 51.
[75] *Bizer* in BDSG, § 3 a, Rn. 1.
[76] *Gola et al.*, BDSG, § 3 a, Rn. 2.
[77] *Bizer* in BDSG, § 3 a, Rn. 83.
[78] *Bizer* in BDSG, § 3 a, Rn. 57ff.
[79] *Bizer* in BDSG, § 3 a, Rn. 62ff.
[80] § 4 Abs. 1 BDSG
[81] Das „oder“ ist abgesehen von Ausnahmefällen ein „exklusiv-oder“, vergl. *Walz* in BDSG, § 4, Rn. 6.

Daten erfolgen und dabei grundsätzlich schriftlich. Zwar gilt sie als „Ausübung des Selbstbestimmungsrechts“[82], aber in Wirklichkeit handelt es sich um eine Fiktion: „Wo [...] die Betroffenen in aller Regel nur die Wahl haben, die Fragen zu beantworten oder auf den Vertrag zu verzichten und sich auch durch einen Wechsel des potentiellen Vertragspartners grundsätzlich nichts ändert, ist die Einwilligung bedeutungslos.“[83]

Neben der Zulässigkeit der Datenverarbeitung durch Einwilligung der Betroffenen existieren weitere Regelungen im BDSG. Bei öffentlichen Stellen gelten für die Erhebung von Daten § 4 Abs. 2 und 3 und § 13, für die Verarbeitung und Nutzung § 14 sowie für die Übermittlung §§ 4 b, 4 c, 15 und 16 als Erlaubnisnormen, außerdem § 6 b für Videoüberwachung und § 6 c für Datenverarbeitung mit Chipkarten. Für nicht-öffentliche Stellen ist die Zulässigkeit der Erhebung in §§ 4 Abs. 2 und 3, 28 Abs. 1, 29 Abs. 1 und § 30 Abs. 1 geregelt und die Verarbeitung und Nutzung in §§ 28, 29, 30 und 35. Konkret heißt das, dass bei öffentlichen Stellen vor allem auf die Erforderlichkeit zur Erfüllung ihrer Aufgaben abgestellt wird, während es bei privaten Stellen in erster Linie darum geht, die Datenverarbeitung im Rahmen der Zweckbestimmung eines Vertragsverhältnisses o. ä. zu ermöglichen.

Viele weitere Zulässigkeitstatbestände werden in anderen Rechtsvorschriften geregelt. Dazu gehören einerseits Gesetze und Rechtsverordnungen des Bundes und der Länder, dabei insbesondere Polizei- und Staatsschutzgesetze, aber auch sozialrechtliche Regelungen und verschiedene Möglichkeiten von Auskunftsersuchen staatlicher Stellen. Andererseits kann sich die Zulässigkeit der Datenverarbeitung auch aus Satzungen öffentlich-rechtlicher Körperschaften ergeben, nicht jedoch aus solchen von juristischen Personen des privaten Rechts. Auch der normative Teil von Tarifverträgen und Betriebsvereinbarungen gilt wegen seiner unmittelbaren Außenwirkung als Rechtsvorschrift im Sinne des Gesetzes.[84]

2.7 Unabdingbare Rechte

Neben den Erlaubnisvorbehalt bei der Erhebung, Verarbeitung und Nutzung der Daten hat der Gesetzgeber eine zweite „Grundschutznorm“[85] gesetzt, die sowohl Voraussetzung als auch Bestandteil des Rechts auf informationelle Selbstbestimmung ist. Dazu hat er in § 6 Abs. 1 BDSG unabdingbare Rechte definiert, also solche, die „nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden“ können. Dies sind die Rechte auf Auskunft, Berichtigung, Löschung und Sperrung.

Das Recht auf Auskunft, also das Recht zu wissen, „wer was wann und bei welcher Gelegenheit über (sie) weiß“[86], ist fundamental für jede Durchsetzung des Datenschutzes, insbesondere im Sinne des Selbstdatenschutzes. Nur so kann der Betroffene überhaupt überprüfen, ob die Datenverarbeitung durch die verantwortliche Stelle rechtmäßig ist. Mit dem dadurch erlangten Wissen kann der Betroffene dann seine anderen Rechte durchsetzen – die Rechte auf Berichtigung, Löschung oder Sperrung.

[82] *Gola et al.*, BDSG, § 4 a, Rn. 2.
[83] *Simitis* in BDSG, § 4 a, Rn. 3.
[84] *Simitis* in BDSG, § 4 a, Rn. 9ff.
[85] *Dix* in BDSG, § 6, Rn. 3.
[86] BVerfGE 65, 1, 43.

Für den öffentlichen Bereich wird das Auskunftsrecht in § 19 BDSG geregelt, für den nicht-öffentlichen Bereich in § 34. Gemäß § 19 Abs. 7 muss die Auskunft unentgeltlich erfolgen, gemäß § 34 Abs. 5 zumindest grundsätzlich, in jedem Fall jedoch bei begründetem Verdacht auf Unrichtigkeit der Daten oder Unzulässigkeit der Speicherung gemäß § 34 Abs. 5 Satz 4 oder bei einer persönlichen Einsichtnahme vor Ort gemäß § 34 Abs. 6. Während die Ausnahmen von der Pflicht zur Auskunftserteilung im privaten Bereich gemäß § 34 Abs. 4 stark beschränkt sind, enthält § 19 unzählige Ausnahmeregelungen, vor allem im Bereich der Sicherheits- und Staatsschutzorgane gemäß § 19 Abs. 3 und 4. In vielen solcher Fälle muss die Ablehnung gemäß § 19 Abs. 5 nicht begründet werden, wobei darüber ausschließlich die verantwortliche Stelle entscheidet. Obwohl diese Auskunftsverweigerung mit dem Grundgesetz unvereinbar ist, wie das BVerfG im „Volkszählungs"-Urteil ausführlich begründet hat, wird solches Verhalten durch Gerichte[87] und den Gesetzgeber weiter gestützt und sogar ausgebaut.[88]

Berichtigung, Löschung und Sperrung sind in § 20 für öffentliche Stellen und in § 35 für nicht-öffentliche Stellen geregelt. Die Pflicht zur Berichtigung unrichtiger personenbezogener Daten besteht für die datenverarbeitende Stelle unabhängig von einem Antrag des Betroffenen.[89] Sie gilt auch bei unbedeutenden Unrichtigkeiten und Bagatellfehlern.[90] Richtig oder unrichtig können jedoch nur Tatsachenangaben sein, nicht jedoch Werturteile. Im Gegensatz zur weiten Auslegung von Werturteilen beim Schutz der freien Meinungsäußerung nach Art. 5 GG soll hier die Grenze zugunsten der Tatsachenbehauptungen gezogen werden.[91] Auch die Löschungspflicht besteht unabhängig von einem Antrag des Betroffenen beim Vorliegen der Voraussetzungen von § 20 Abs. 2 und § 35 Abs. 2 Satz 2. Soweit die personenbezogenen Daten nicht gelöscht werden können, weil dem z. B. gesetzliche oder vertragliche Aufbewahrungsfristen entgegenstehen oder die Löschung aus technischen Gründen „nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist", sind sie gemäß § 20 Abs. 3 und § 35 Abs. 3 zu sperren. Personenbezogene Daten sind auch dann zu sperren, wenn der Betroffene die Richtigkeit der Daten bestreitet und „sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt".[92]

Gleichzeitig kann der Betroffene auch der rechtmäßigen Verarbeitung von personenbezogenen Daten widersprechen. In diesem Fall dürfen die Daten gemäß § 20 Abs. 5 und § 35 Abs. 5 weder erhoben, verarbeitet noch genutzt werden, es sei denn, eine Rechtsvorschrift verpflichtet dazu.

Neben den unabdingbaren Rechten haben die Betroffenen seit 2001 einen echten Schadensersatzanspruch, weil der Gesetzgeber dazu durch die EG-Datenschutzrichtlinie gezwungen wurde.[93] Gleichwohl wurde dieser Anspruch sofort wieder eingeschränkt, und zumindest nicht-öffentlichen Stellen ist in § 7 Satz 2 die Möglichkeit gegeben worden, sich selbst zu entlasten. Für öffentliche Stellen existiert eine solche Entlastungsmöglichkeit nicht, für diese gilt eine Gefähr-

[87] So z. B. das Bundesverwaltungsgericht in einem Urteil vom 20.02.1990 (AZ. 1 C 42/83), in: NJW 1990, S. 2761ff.

[88] Ausführlich zu den staatlichen Begründungsversuchen und ihrer Geschichte und rechtlichen Einordnung sowie den Gegenargumenten dazu: *Schwan*, Überwachungsstaat, S. 292ff.

[89] *Mallmann* in BDSG, § 20, Rn. 9; *Dix* in BDSG, § 35, Rn. 9.

[90] *Gola et al.*, BDSG, § 20, Rn. 3; *Dix* in BDSG, § 35, Rn. 7.

[91] *Mallmann* in BDSG, § 20, Rn. 19.

[92] § 20 Abs. 4 BDSG

[93] *Simitis* in BDSG, § 7, Rn. 4.

dungshaftung.[94] Außerdem haften nicht-öffentliche Stellen nicht für immatrielle Schäden, während es diese Einschränkung bei öffentlichen Stellen richtigerweise nicht gibt.[95]

3 Zusammenfassung und Ausblick

Das aufgeklärte und autonome Individuum, das die moderne bürgerliche Gesellschaft als Bezugspunkt ihrer ideologischen Grundlagen postuliert, muss in diesem Kontext notwendig auch die Kontrolle über seine eigene Außendarstellung besitzen. Das Recht des Individuums, selbstbestimmt zu entscheiden, ob es sich in die Privatheit zurückziehen oder in die Öffentlichkeit begeben will, und die Grenzen der eigenen Privatsphäre zu ziehen, ist Basis für die freie Entfaltung der Persönlichkeit. Doch erst die Zunahme der automatisierten Datenverarbeitung hat die Notwendigkeit offenkundig werden lassen, diesem Recht einen besonderen Ausdruck zu verleihen. Das Recht auf informationelle Selbstbestimmung ist daher gerade kein Recht auf Schutz der Daten sondern auf Schutz der Menschen, auf die sich die Daten beziehen.[96]

Zur immanent politischen Begründung eines entstehenden Datenschutzrechtes trat bald die sich ausbreitende Angst vor einem Kontrollverlust an eine fast gänzlich unverstandene Technologie hinzu. Je weniger der Einzelne vom Verwaltungsablauf und der dabei eingesetzten Technik verstand, desto größer wurde das Misstrauen gegenüber einer ausufernden Bürokratie, die sich für jeden seiner Schritte zu interessieren schien. Die völlige Ignoranz der politischen Klasse – und mit ihr der Rest der gesellschaftlichen Eliten – gegenüber den Ängsten der breiten Masse der Bevölkerung bei der versuchten Durchführung einer Volkszählung im Jahre 1983 bildete den Nährboden für eine große Koalition der „Ausgestoßenen“: die politischen Outlaws verbündeten sich mit der bildungsbürgerlichen Mitte, die techno-affine Subkultur mit den technologisch Überflüssigen, die „Überlebenden“ der „Startbahn West“ mit den ängstlichen „Spießern“. Die von einigen wenigen eingereichte Verfassungsbeschwerde gegen das “Volkszählungsgesetz 1983“ war einerseits juristisch erfolgreich und markierte damit andererseits den Kulminationspunkt des Erfolges der Bewegung als Volksbewegung. Die danach einsetzende Verrechtlichung des Datenschutzdiskurses führte zu einer Exklusion der Betroffenen. Neben das staatliche Informationsinteresse trat verstärkt ein privatwirtschaftliches, das weniger bedrohend als vielmehr verführend die Preisgabe privater Daten einforderte. Das schwächere datenschutzrechtliche Schutzniveau gegenüber nicht-öffentlichen Stellen ist daher längst von der Realität überholt.

Dennoch haben sich im Datenschutzrecht drei wichtige Säulen herausgebildet: der Grundsatz der Datenvermeidung und Datensparsamkeit für Datenverarbeitungssysteme, der datenschutzrechtliche Erlaubnisvorbehalt mit dem Vorrang der Selbstauskunft und die Existenz unabdingbarer Rechte der Betroffenen. Trotz aller rechtlicher und faktischer Einschränkungen bei den einzelnen Säulen besteht dennoch im Moment nicht die Gefahr eines Zusammenbruchs des gesamten Datenschutzgebäudes, auch wenn die Zahl der Unterminierungsversuche stetig zunimmt und deren Zielstrebigkeit erschreckt. Seit der (Wieder-)Entdeckung

[94] *Simitis* in BDSG, § 8, Rn. 13.
[95] *Simitis* in BDSG, § 7, Rn. 32.
[96] *Gola et al.*, Grundzüge, S. 1.

eines Hobbes'schen „Grundrechts auf Innere Sicherheit“ in den siebziger Jahren des zwanzigsten Jahrhunderts durch die konservativen und rechten InnenpolitikerInnen aller Couleur müssen sich Persönlichkeits- und Freiheitsrechte vermehrt nachrangig behandeln lassen. Die Ausweitung staatlicher – und in den letzten Jahren zunehmend auch privater – Überwachungsmaßnahmen stellt dabei durchaus einen frontalen Angriff auf das Recht auf informationelle Selbstbestimmung dar. Wenn Datenschutz im politischen Diskurs nur noch als „Täterschutz“ bezeichnet wird – und wenn nicht gerade Bundestagsabgeordnete in der Diätendebatte ihre Liebe zum Datenschutz, genauer: zum Schutz ausschließlich ihrer eigenen Daten, entdecken – und die große Mehrheit der Bevölkerung dies offensichtlich ähnlich sieht, dem zumindest ausgesprochen gleichgültig gegenübersteht oder sich gar fröhlich dabei überschlägt, die eigenen Daten möglichst als erstes überall preiszugeben, sieht die Zukunft des Datenschutzes tiefschwarz aus. Mit dem Kampf gegen den Terrorismus, der in der bürgerlichen Gesellschaft nichts weiter ist als der Terrorismus der Anderen, führen die Apologeten des modernen Obrigkeitsstaates gleichzeitig einen Kampf gegen die Freiheit des Individuums.

Die Frage, wer den Kampf gewinnen wird, ist dabei durchaus noch offen.

4 Literatur

Bull, Hans Peter, Vom Datenschutz zum Informationsrecht – Hoffnungen und Enttäuschungen, in: *Hohmann, Harald* (Hrsg.), Freiheitssicherung durch Datenschutz, 1. Aufl., Suhrkamp Verlag, Frankfurt am Main, 1987, S. 173–204; zitiert als: *Bull*, Hoffnungen und Enttäuschungen.

Denninger, Erhard, Das Recht auf informationelle Selbstbestimmung, in: *Hohmann, Harald* (Hrsg.), Freiheitssicherung durch Datenschutz, 1. Aufl., Suhrkamp Verlag, Frankfurt am Main, 1987, S. 127–172; zitiert als: *Denninger*, Informationelle Selbstbestimmung.

Durner, Wolfgang, Zur Einführung: Datenschutzrecht, in: JuS 3/2006, S. 213-217, Beck Verlag, München; zitiert als: *Durner*, Datenschutzrecht.

Gola, Peter / Klug, Christoph, Grundzüge des Datenschutzrechts, Beck Verlag, München, 2003; zitiert als: *Gola et al.*, Grundzüge.

Gola, Peter / Schomerus, Rudolf, BDSG, Kommentar, 8. Aufl., Beck Verlag, München, 2003; zitiert als: *Gola et al.*, BDSG.

Hassemer, Winfried / Möller, Klaus Peter (Hrsg.), 25 Jahre Datenschutz: Bestandsaufnahme und Perspektiven, 1. Aufl., Nomos Verlagsgesellschaft, Baden-Baden, 1996; zitiert als: *Hassemer et al.*, 25 Jahre Datenschutz.

Massing, Otwin, Von der Volkszählungsbewegung zur Verrechtlichung oder: Öffentlichkeit, Herrschaftsrationalisierung und Verfahren, in: *Hohmann, Harald* (Hrsg.), Freiheitssicherung durch Datenschutz, 1. Aufl., Suhrkamp Verlag, Frankfurt am Main, 1987, S. 85–109; zitiert als: *Massing*, Verrechtlichung.

Schapper, Claus-Henning, Dritter Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten, 1985; zitiert als: *Schapper*, Dritter Tätigkeitsbericht.

Schapper, Claus-Henning / Waniorek, Gabriele, Informationelle Selbstbestimmung auch für Arbeitnehmer?, in: *Hohmann, Harald* (Hrsg.), Freiheitssicherung durch Datenschutz, 1. Aufl., Suhrkamp Verlag, Frankfurt am Main, 1987, S. 313–353; zitiert als: *Schapper et al.*, Informationelle Selbstbestimmung.

Schwan, Eggert, Auf dem Weg zum Überwachungsstaat? Plädoyer für eine rechtsstaatliche Datenverarbeitung der Polizei, in: *Hohmann, Harald* (Hrsg.), Freiheitssicherung durch Datenschutz, 1. Aufl., Suhrkamp Verlag, Frankfurt am Main, 1987, S. 276–312; zitiert als: *Schwan*, Überwachungsstaat.

Schneider, Hans, Anmerkung zum „Volkszählungs"-Urteil, in: Die Öffentliche Verwaltung, Zeitschrift für öffentliches Recht und Verwaltungswissenschaft, 37. Jahrgang, W. Kohlhammer GmbH, Stuttgart, 1984, S. 161–164; zitiert als: *Schneider*, DÖV.

Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz, Kommentar, 6. Aufl., Nomos Verlagsgesellschaft, Baden-Baden, 2006; zitiert als: *Bearbeiter* in BDSG.

Tinnefeld / Ehmann / Gerling, Einführung in das Datenschutzrecht, 4. Aufl., Oldenbourg Verlag, München, Wien, 2005; zitiert als: *Tinnefeld et al.*, Datenschutzrecht.