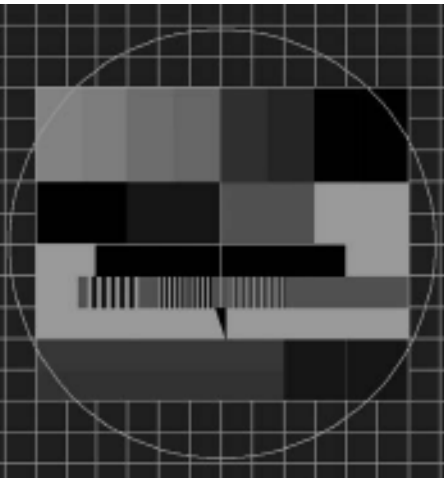
Als Big Brother noch keine Fernsehsendung war

Entwicklung des Datenschutzrechts

Henning Kahlert



Die Entwicklung des Datenschutzrechts in Deutschland und Europa ist wesentlich beeinflusst durch das Vorbild der USA – ein Vorbild jedoch im positiven wie im negativen Sinne. Während die ersten theoretischen Überlegungen zu dieser noch vergleichsweise jungen Rechtsmaterie aus den USA stammen, nahm die Entwicklung in Deutschland bald eine eigenständige Richtung, die sich scharf von der US-amerikanischen unterschied. Erst in jüngster Zeit treten im Zuge der Terrorismusbekämpfung wieder verstärkt gemeinsame Überlegungen in den Vordergrund, die bereits errungene Fortschritte teilweise in Frage zu stellen drohen.

Historische Entwicklung in den USA

In der vorindustriellen amerikanischen Gesellschaft war der Schutz der Privatsphäre allein durch ungeschriebene Verhaltensregeln gewährleistet. In die fremde Privatsphäre einzudringen galt und gilt als „ungehörig" und wurde durch Sozialkontrolle unterdrückt. Mit dem Aufkommen moderner Massenmedien, insbesondere der „Klatschpresse" erwiesen sich diese informellen Kontrollmittel jedoch als zunehmend wirkungslos, rechtlicher Schutz wurde erforderlich. Bereits Ende des 19. Jahrhunderts entstand in den USA das Konzept der „privacy", also eines schutzbedürftigen Raumes individueller Selbstentfaltung. Ein viel zitierter Urteilsspruch aus dem Jahre 1880 definiert *privacy* als *„right to be let alone"*.

Die amerikanische Rechtsentwicklung war auch in diesem Bereich derjenigen in Europa weit voraus. In der Folge entwickelte sich das Konzept der *privacy* in den USA jedoch in eine andere Richtung, als dies später in Europa und insbesondere in Deutschland der Fall sein sollte: In den USA stand und steht nämlich eindeutig der Abwehr von *government intrusion* im Vordergrund, also von staatlichem Handeln und insbesondere der Datensammlung durch staatliche Stellen. Allerdings wird daraus kein Schutzanspruch vor Datensammlung abgeleitet, sondern Informationsansprüche der Betroffenen gegen die Behörden, die ihre Unterlagen in weiten Bereichen offen legen müssen – auch dies eine Idee, die langsam auch in Deutschland Fuß fasst. Allerdings beginnt hierzulande erst die Diskussion um die Informationsfreiheit, also die Forderung nach einem Anspruch auf Zugang zu Behördeninformationen, ohne dafür ein konkretes rechtliches Interesse geltend machen zu müssen.

Im Bereich der privatwirtschaftlichen Datensammlung und Datenauswertung gibt es dagegen in den USA bis heute keine umfassenden gesetzlichen Schutzvorkehrungen, lediglich Regelungen in Einzelbereichen. So sind etwa die Ausleihdaten von Videotheken und Nutzungsdaten beim Kabelfernsehen geschützt, nicht aber Daten über Bankkonten, medizinische Dokumentationen und Personalakten, Verbindungsdaten von Telefonanschlüssen oder Daten über den Gebrauch von Kreditkarten. Statt dessen verlässt man sich auf das Prinzip „*notice and choice*": Die Unternehmen legen ihre Datenverarbeitungsabsichten offen, und die Verbraucherinnen und Verbraucher entscheiden sich auch aufgrund dieser Erklärung, wo sie Waren bestellen oder Konten einrichten. Datenschutz ist damit ein Wettbewerbsvorteil und wird von den Unternehmen aus eigenem Interesse verbessert. Das auf diese Weise gewährte Schutzniveau ist recht hoch.

Datenschutz in Deutschland

Auch in Deutschland wurden die Gefahren, die aus einer unbeschränkten Sammlung und Auswertung persönlicher Daten zu erwachsen drohten, mit der fortschreitenden Entwicklung der elektronischen Datenverarbeitung nach dem Ende des zweiten Weltkrieges zunehmend deutlich – zunächst jedoch vornehmlich für eine Minderheit, weil die Sammlung und Auswertung der Daten weitgehend unbemerkt von der Öffentlichkeit vonstatten gingen und unmittelbare negative Auswirkungen nicht sogleich offensichtlich wurden. Dennoch zeigten sich in der Rechtsprechung erste Ansätze eines Schutzes der „privacy", zunächst noch unabhängig von einem technischen Bezug. Bereits im Jahre 1969 entschied das Bundesverfassungsgericht (zu einem Gesetz, das eine Statistik der Bevölkerung und des Erwerbslebens anordnete), das Grundgesetz gewährleiste einen unantastbaren Bereich privater Lebensgestaltung; hiermit sei eine zwangsweise Registrierung und Katalogisierung des Menschen in seiner ganzen Persönlichkeit nicht zu vereinbaren (BVerfGE 27, 1, 6).

1970 erließ Hessen das weltweit erste Datenschutz-Gesetz, 1973 folgte mit dem schwedischen *datalagen* das erste nationale Datenschutz-Gesetz. In Deutschland wurde 1977 auf Bundesebene das Bundesdatenschutzgesetz (BDSG) in seiner ersten Fassung verabschiedet. Die Reaktionen auf dieses Gesetz waren – vorsichtig formuliert – zurückhaltend; selbst seine Befürworterinnen und Befürworter hielten es für eine Notlösung, während seine Gegnerinnen und Gegner eine Regelung für schlicht nicht erforderlich hielten. Ursache für diese fehlende Begeisterung dürfte hauptsächlich gewesen sein, dass die Gefahren einer zentralen Datensammlung noch nicht deutlich wurden: Computer waren langsam und teuer und daher nicht weit verbreitet.

Die Volkszählungs-Entscheidung des Bundesverfassungsgerichts

Dies änderte sich erst über 10 Jahre später, nämlich mit dem Vorhaben der damaligen Bundesregierung unter Helmut Schmidt, eine umfassende Volkszählung durchzuführen. Das „Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1983)“ sah umfangreiche Auskunftspflichten aller betroffenen volljährigen Deutschen vor: Diese hatten neben ihren vollen Personalien auch ihre Religionszugehörigkeit zu offenbaren und mussten detaillierte Angaben zu ihrer Wohnung und ihrer Arbeitsstätte machen. Unrichtige oder unvollständige Angaben konnten mit empfindlichen Geldbussen geahndet werden. Was der Staat mit den so gesammelten Daten anfangen wollte, ging aus dem Gesetz nicht hervor.

Erstmals war damit eine größere Zahl von Personen gleichzeitig und in gleicher Art und Weise mit einem Datensammlungs- und Verarbeitungsvorgang konfrontiert. Der Widerstand gegen dieses Gesetz wurde so zum Kristallisationspunkt der bislang nur unterschwellig vorhandenen Bedenken gegen staatliche Datensammlung. Weite Teile der Bevölkerung kündigten offen an, die Angabe persönlicher Daten verweigern zu wollen. Zahlreiche Bürgerinnen und Bürger erhoben Verfassungsbeschwerde gegen das Volkszählungsgesetz, die das Bundesverfassungsgericht im Dezember 1983 für zum Teil begründet erklärte.

Diese Entscheidung darf als Meilenstein auf dem Weg des modernen Datenschutzes bezeichnet werden. Das Gericht stellte fest, im Mittelpunkt der grundgesetzlichen Ordnung stünden Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirke. Ihrem Schutz diene nicht zuletzt das aus Art. 2 Abs.1 in Verbindung mit Art. 1 Abs. 1 Grundgesetz (GG) abgeleitete *allgemeine Persönlichkeitsrecht*, das im Hinblick auf die moderne technische Entwicklung und den damit verbundenen neuen Gefahren neue Bedeutung gewinne. Unter den Bedingungen der automatischen Datenverarbeitung ließen sich Daten aus verschiedenen Quellen zu Persönlichkeitsbildern zusammenstellen, ohne dass die Betroffenen deren Richtigkeit oder Verwendung kontrollieren könnten. Individuelle Selbstbestimmung sei jedoch nur dann möglich, wenn sich die Betroffenen auch entsprechend ihrer Entscheidungen verhalten könnten und nicht befürchten müssten, dass ihr Verhalten in allen Details aufgezeichnet und gespeichert würde. Das Gericht postulierte so ein *Recht auf informationelle Selbstbestimmung*, mit dem eine Gesellschaft unvereinbar sei, in der die Bürgerinnen und Bürger nicht mehr abschätzen könnten, wer was wann und bei welcher Gelegenheit über sie wisse; alle Betroffenen müssten daher grundsätzlich selbst über die Preisgabe und Verwendung ihrer persönlichen Daten bestimmen können.

Auch nach heutigem Verständnis enthält die Entscheidung des Bundesverfassungsgerichts einige *zentrale Grundforderungen des Datenschutzes*: Die Bindung jeglicher Verarbeitung personenbezogener Daten an einen bestimmten (zuvor definierten und inhaltlich klar umrissenen) Zweck; eine transparente, d.h. nachvollziehbare Ausgestaltung des Erfassungs- und Verarbeitungsvorgangs und die Einwilligung der Betroffenen als – grundsätzlich immer erforderliche – Zulässigkeitsvoraussetzung jeglicher Datenverarbeitung.

Reform des Bundesdatenschutzgesetzes

Obgleich das Bundesverfassungsgericht recht konkrete Vorgaben für die weitere Ausgestaltung des Datenschutzrechts gemacht hatte, ging die weitere Entwicklung des BDSG nur langsam voran. Statt die allgemeinen Vorschriften im BDSG anzupassen, erließ der Gesetzgeber eine wahre Flut von *bereichsspezifischen Regelungen*: In jedes Gesetz, das dem Staat den Umgang mit personenbezogenen Daten erlaubte, wurde eine Vorschrift eingefügt, die diese Datenverarbeitung im jeweiligen Kontext regelte. Die Folge war (und ist bis heute) eine unüberschaubare Menge von Spezialregelungen, die sich inhaltlich nur im Detail unterscheiden, die es aber dennoch den Betroffenen erschweren, ihre Rechte zu wahren. Die vom Bundesverfassungsgericht ebenfalls erhobene Forderung nach Transparenz, also Durchschaubarkeit des Verfahrens, wurde so ad absurdum geführt.

Erst 1990 wurde das BDSG reformiert. Wesentliches Ziel dabei war es, nicht allein die missbräuchliche Verarbeitung personenbezogener Daten zu verhindern, sondern allgemein den Verarbeitungsvorgang nachvollziehbaren Regeln zu unterwerfen.

Inzwischen hatte auch die Europäische Union den Datenschutz entdeckt, und zwar insbesondere als Hindernis für den gemeinsamen Markt: Mitgliedstaaten mit einem hohen Schutzniveau verweigerten Unternehmen den „Export“ von personenbezogenen Daten in EU-Staaten mit niedrigerem Schutzniveau. Um zu verhindern, dass sich hieraus Hindernisse für den freien Waren- und Dienstleistungsverkehr ergeben könnten, verabschiedete die Gemeinschaft 1995 die Datenschutz-Richtlinie[1]. Sie sollte den Datenschutz auf ein einheitliches Niveau bringen und – als dessen Folge – die freie Übertragbarkeit der Daten gewährleisten. Die Mitgliedstaaten, darunter auch Deutschland, hatten ihre nationalen Rechtsvorschriften an die Vorgaben der Richtlinie anzupassen; eine erneute Überarbeitung des BDSG wurde notwendig. Mit der üblichen Verspätung erfolgte diese Anpassung im Jahre 2001 durch die Neufassung des BDSG. Eine umfassende Modernisierung des Datenschutzrechts stellte diese Neufassung nicht dar; vielmehr war es erklärtes Ziel der Neuregelung, lediglich die dringend erforderlichen Anpassungen vorzunehmen und die Modernisierung des Datenschutzrechts „möglichst bald“ durch eine völlige Neufassung abzuschließen. Auf diese Neufassung warten wir noch heute.

Wie geht es weiter?

Die Diskussion über eine grundlegende Reform des Datenschutzes kam durch die Neufassung des BDSG 2001 nicht zum Erliegen. Als Kernprobleme des bestehenden Datenschutzrechts in Gestalt des BDSG, das mitunter als „Dino-

saurier“ verspottet wird, können schlagwortartig die folgenden drei Punkte genannt werden:

Das tradierte Regelungsmodell eines – subsidiären – Datenschutzgesetzes, das durch eine Unzahl von Spezialregelungen mit überwiegend identischem Inhalt verdrängt wird, steht der vom Verfassungsgericht geforderten Transparenz entgegen. Es erscheint daher sinnvoll, bereichsspezifische Regelungen so weit als möglich zu streichen und die grundlegenden Fragen konzentriert im BDSG zu regeln.

Während Datenschutz ursprünglich auf die Kontrolle staatlicher Sammel- und Verarbeitungstätigkeit konzentriert war, erfolgt unter den heutigen Bedingungen der überwiegende Teil der elektronischen Datenverarbeitung durch Private. Dennoch ist das Datenschutzrecht mit seiner Regelungs- und Kontrollstruktur immer noch auf die Kontrolle staatlichen Handelns zugeschnitten. Schwer verständliche Regelungen, verbunden mit lückenhafter Kontrolle, fördern jedoch die Einhaltung der Datenschutzvorschriften nicht. Eine Reform des Datenschutzes muss bei den Privaten selbst ansetzen und Datenschutz attraktiver machen. Hier blickt man über den Atlantik und versucht, US-amerikanische Konzepte wie „*Datenschutz durch Marktwirtschaft*“ auch hierzulande umzusetzen. Unternehmen sollen es im freien Wettbewerb als vorteilhaft empfinden, Datenschutz zu gewährleisten, dadurch steigt das allgemeine Schutzniveau. So attraktiv diese Idee auch erscheint, müssen dabei jedoch die wesentlichen Unterschiede zwischen der amerikanischen und der deutschen Ausgangslage beachtet werden. In Europa und insbesondere in Deutschland hat Datenschutz einen höheren Stellenwert als in den USA und steht den Bürgerinnen und Bürgern als einklagbares Grundrecht zu. Ein rein auf freiwilliger Basis organisierter Datenschutz ist damit nicht vereinbar.

Zuletzt müssen die Betroffenen mehr als bislang in die Lage versetzt werden, selbst ihre Privatsphäre zu definieren und zu schützen. Hier wird verstärkt auf technische Hilfsmittel wie Verschlüsselung von Emails und Sicherheitstechniken im Internet-PC gesetzt, die verhindern sollen, dass alle Daten für jedermann offensichtlich werden. Diese rein privaten Initiativen müssen ebenso gefördert werden wie eine umfassende Sicherheits-Infrastruktur auf breiter Basis, die die anonyme Inanspruchnahme von Dienstleistungen über das Internet ermöglicht. Dies wiederum ist den Strafverfolgungsbehörden ein Dorn im Auge.

Stiefkind Datenschutz

Die weitere Entwicklung des Datenschutzrechts wird nicht zuletzt von der Bedeutung abhängen, die der Privatsphäre und ihrem Schutz allgemein beigemessen wird. Hier lassen sich in letzter Zeit zwei neue Entwicklungstendenzen feststellen:

Zum einen scheinen immer mehr Menschen nicht auf mehr Privatsphäre Wert zu legen, sondern im Gegenteil auf deren völliges Fehlen. Sie lassen sich in Wohncontainer einsperren und rund um die Uhr auch bei intimsten Verrichtungen von Kameras filmen (wobei hier nicht der Frage nachgegangen werden soll, wer bedauernswerter ist: Diejenigen Menschen, die sich derart filmen lassen, oder diejenigen, die ihnen dabei zuschauen). „Big Brother“, einst Schreckensbild eines allmächtigen Überwachungsstaates, ist zum Sinnbild einer neuartigen Unterhaltungsform geworden, in der sich Faszination und Ekel die Waage halten. Die Schwelle dessen, was das Bundesverfassungsgericht einst den „unantastbaren Bereich privater Lebensgestaltung“ bezeichnete, sinkt beständig. Eine Gesellschaft, in der diese Einstellung verbreitet ist, hat keinen Bedarf nach Datenschutz.

Zum anderen hat sich auch die Einstellung der Bürgerinnen und Bürger gegenüber dem Staat und damit gegenüber der von ihm betriebenen Datensammlung und Datenauswertung gewandelt. Erschien den Kämpferinnen und Kämpfern gegen das „Volkszählungsgesetz“ der Staat in seiner scheinbar grenzenlosen Neugier noch als Gegner, erhofft man sich heute vom Staat verstärkt Schutz gegen Bedrohungen, die von gewaltbereiten Dritten ausgehen, etwa muslimischen Extremisten. Einschränkungen der persönlichen Freiheit erscheinen hinnehmbar, wenn damit eine Verbesserung der individuellen Sicherheit verbunden ist. Seit der internationalen Zunahme des Terrorismus macht man sich geradezu verdächtig, wenn man von Datenschutz spricht – hat man denn etwas zu verbergen?

„Datenschutz leuchtet den Bürgern nicht mehr so wie früher als ein unverzichtbares Grundrecht ein. Heute würden sie nicht mehr für ein Grundrecht auf Privatheit oder auf Datenschutz auf die Strasse gehen“, resümiert Winfried Hassemer, der Vizepräsident des Bundesverfassungsgerichts, in einem Interview in der F.A.Z. vom 22. April 2004.

Ziel eines modernen Datenschutzrechts muss es jetzt sein, einen Ausgleich zu finden zwischen dem legitimen Informationsbedürfnis des Staates, der zur Wahrnehmung seiner Aufgaben auf eine zuverlässige Datengrundlage angewiesen ist, und den Freiheitsinteresse der Bürgerinnen und Bürger, denen daran gelegen sein sollte, sich nicht zu tief in die Karten schauen zu lassen.

Henning Kahlert ist Doktorand in Karlsruhe.

Anmerkungen:

1 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.