Hansjürgen Garstka

Informationelle Selbstbestimmung und Datenschutz

Das Recht auf Privatsphäre

»*Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.*«

Mit diesem Leitsatz erkannte das Bundesverfassungsgericht am 15. Dezember 1983 das Recht auf informationelle Selbstbestimmung als Bestandteil unserer verfassungsmäßigen Ordnung an. Der Datenschutz, der in den USA, in Deutschland und vielen anderen Ländern seit Anfang der 70er-Jahre in Gesetzen geregelt war und den Missbrauch der Datenverarbeitung verhindern sollte, war fortan ein Grundrecht. Im Grundgesetz ist dieses Grundrecht zwar nicht ausdrücklich enthalten, das Bundesverfassungsgericht hat jedoch in vielen Urteilen die informationelle Selbstbestimmung als eine der wesentlichen Grundlagen unserer Rechtsordnung bestätigt.

Auch international ist der Datenschutz als wesentliches Element der Informationsgesellschaft anerkannt. Fast gleichzeitig haben die OECD[1] und der Europarat[2] 1980/81 in zwei wichtigen Dokumenten ihre Mitgliedsstaaten angehalten, Datenschutzgesetze zu erlassen. Die Vereinten Nationen folgten

Artikel 8 Europäische Grundrechtecharta [Schutz personenbezogener Daten]

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

1990.[3] Nachdem die Europäische Union 1995 zunächst Datenschutzrichtlinien geschaffen hatte,[4] wurde der Datenschutz im Jahr 2000 in den Katalog der Grundrechte der Europäischen Grundrechtecharta aufgenommen (s. S. 48).[5]

1. Geschichte des Datenschutzes

Die Geschichte des modernen Datenschutzes beginnt Anfang der 60er-Jahre des 20. Jahrhunderts in den USA. Die amerikanische Regierung plante, beim Statistischen Bundesamt mit Hilfe der damals allerdings noch relativ wenig entwickelten Computertechnik eine Datenbank aufzubauen, in der alle amerikanischen Staatsbürgerinnen und -bürger erfasst werden sollten. In der Bevölkerung wurde dieser Plan als schwerer Eingriff in das Recht empfunden, vom Staat in Ruhe gelassen zu werden; der Eingriff in die Privatsphäre (»Right to Privacy«) erschien vielen als unverhältnismäßig. Im Laufe der Debatte wurde aufgedeckt, dass die amerikanische Armee viele Millionen von Daten über politisch verdächtige Personen oder Auskunfteien große Mengen von Daten persönlichster Natur (zum Beispiel über Krankheiten und Schulzeugnisse) gesammelt hatte.

Ergebnis der Debatte war, dass die Datenbank nicht errichtet, aber der »Privacy Act« (Privatsphärengesetz) verabschiedet wurde, der die amerikanische Bundesregierung zur Einhaltung von Grundprinzipien zur Sicherung der Privatsphäre verpflichtete.[6] Ein fundamentaler Mangel ist der Umstand, dass die Gesetzgebung nicht auf Privatunternehmen ausgedehnt wurde. Dies führt heute zu heftigen Debatten, wie der Datenschutz bei amerikanischen Unternehmen beim Export von Daten von Europa nach den USA gewährleistet werden kann.

Die Diskussion in den USA löste Aktivitäten in allen Industriestaaten aus. Auch in der Bundesrepublik Deutschland kam es zu einer Debatte über die Notwendigkeit gesetzlicher Regelungen. Das Bundesland Hessen reagierte bereits 1970 mit einem Gesetz, das den Begriff Datenschutz in die deutsche Rechtssprache einführte. Er hat inzwischen in alle Sprachen der Welt Eingang gefunden (zum Beispiel data protection, protection de données, zaschtschyta datych). Dies ist eigentlich verwunderlich, weil er falschen Assoziationen Vorschub leistet: Anliegen des Datenschutzes ist nicht der Schutz der Daten, sondern der Schutz der Menschen vor der Verarbeitung von Daten.

1978 trat das erste Bundesdatenschutzgesetz in Kraft. Es verpflichtete Bundesbehörden und Privatwirtschaft auf die Einhaltung bestimmter materieller Regelungen bei der Datenverarbeitung und schuf ein umfangreiches System an Bürgerrechten und Kontrollmechanismen. Die Länder schufen in der Folge Landesdatenschutzgesetze für die Landesverwaltungen.

1983 wurde das Bundesverfassungsgericht von mehr als 1000 Beschwerdeführern angerufen, weil diese sich trotz der Datenschutzgesetzgebung durch

die geplante Volkszählung in ihren Rechten verletzt fühlten. In dem berühmten Volkszählungsurteil brachte das Gericht die Volkszählung zu Fall und entwickelte das Grundrecht auf informationelle Selbstbestimmung.[7]

Die wichtigsten Aussagen sind, dass die Verarbeitung personenbezogener Daten stets einen Eingriff in das allgemeine Persönlichkeitsrecht darstellt, der nur auf einer gesetzlichen Grundlage zulässig ist. Die Gesetze müssen normenklar und für Bürgerinnen und Bürger erkennbar regeln, was zulässig ist. Daten dürfen nur zu den Zwecken verarbeitet werden, zu denen sie erhoben wurden; Zweckänderungen bedürfen ebenfalls einer Rechtsgrundlage. Es dürfen nur so viele Daten verarbeitet werden, wie für den Zweck unbedingt erforderlich sind. Das Urteil zwang dazu, Bundes- und Landesdatenschutzgesetze an die Vorgaben des Verfassungsgerichts anzupassen. Der Bundesgesetzgeber ließ sich bis 1990 dazu Zeit.

Ebenfalls erheblich verspätet wurde die Europäische Datenschutzrichtlinie umgesetzt. Obwohl die Anpassungsfrist bereits 1998 abgelaufen war, traten die neuen Regelungen des Bundesdatenschutzgesetzes (BDSG) erst am 23. Mai 2001 in Kraft.[8] Es besteht Einigkeit zwischen allen Experten, dass dieses neue Gesetz zu kompliziert ist und den Anforderungen an die modernen Informationstechnologien nicht gerecht wird. Bereits parallel zum Gesetzgebungsverfahren zum neuen BDSG hat daher das Bundesinnenministerium ein Gutachten in Auftrag gegeben, um zu prüfen, wie das Datenschutzrecht von Grund auf modernisiert werden kann. Das Ergebnis ist im September 2001 vorgelegt worden.[9]

2. Die Risiken

Die Datenschutzdebatte in den 60er-Jahren in den USA hatte als Bezugspunkt das »Right to Privacy«, das Recht auf Privatsphäre, das von den jungen Anwälten Samuel Warren und Louis Brandeis 1890 in einem berühmten Aufsatz entwickelt worden war.[10] Sie vertraten die These, dass nicht erst die physische Beeinträchtigung von Rechtsgütern wie körperlicher Zwang, Entzug der Freiheit oder Eingriffe in das Eigentum rechtlich von Bedeutung sind, sondern bereits das Sammeln von Informationen (wobei dieser Begriff den Autoren noch unbekannt war). Sie schrieben: »Das Recht sichert jedem Individuum das Recht zu, grundsätzlich zu bestimmen, in welchem Ausmaß seine Gedanken, Gefühle und Empfindungen anderen mitgeteilt werden.«[11] Es ist sicherlich kein Zufall, dass der Leitsatz des Volkszählungsurteils an diese Formulierung angelehnt ist.

Warren und Brandeis reagierten mit ihrem Aufsatz auf indiskrete Veröffentlichungen in der Boulevardpresse, die damals gerade ihren Aufschwung nahm. Sie sahen allerdings noch relativ klar umgrenzbare Gefahren: Der heimliche Beobachter, der verdeckt oder unverdeckt Privates, für ihn nicht Be-

stimmtes zur Kenntnis nimmt; die Offenbarung intimer Kenntnisse ohne Einwilligung oder Wissen der Betroffenen an die Öffentlichkeit oder an andere Stellen; die Verzerrung des Persönlichkeitsbildes durch falsche Darstellung oder auch nur durch Weglassen wichtiger Details.

In der Informationsgesellschaft globalisieren sich nicht nur die Nutzungsformen der Informationstechnik, sondern auch deren Risiken. Die Nutzung der Telekommunikation ermöglicht nicht nur dem Späher am Schlüsselloch, sondern jedem am Telekommunikationsprozess Beteiligten, Daten zu erheben und damit in die Sphäre der Betroffenen einzudringen. Hinzu kommt, dass früher die Verarbeitung stark durch die Schranken des Ortes, der Zeit, aber auch durch die Menge der Informationen eingeengt war. Diese Schranken sind mit dem Internet entfallen: Daten können in Sekunden von einem Ort der Welt an den anderen übertragen werden, die quantitativen Grenzen fallen mit der Fortentwicklung von Verarbeitungs-, Speicher- und Übertragungskapazitäten weg.

Dies ermöglicht eine Konnektivität der Daten, wie sie früher unmöglich schien. Daten aus den verschiedensten Datensammlungen können in kürzester Zeit miteinander verglichen und durchgerastert werden, um festzustellen, auf wen oder auf was bestimmte Merkmalskombinationen weltweit zutreffen. Für den normalen Internetnutzer legen die Suchmaschinen davon Zeugnis ab, die kommerziellen Nutzer versuchen, durch Data-Mining-Konzepte diesen Effekt für ihre Geschäftszwecke zu nutzen. Hat früher bereits die Speicherung von Daten, sei es auf dem Papier oder im Computer, bereits Mühe und Raum gekostet, und entstand dadurch eine natürliche Barriere zum unbegrenzten Datensammeln, bestehen nunmehr keinerlei Hindernisse mehr, alles über jeden zu sammeln, wie erforderlich dies auch sein mag. Auch Sammlungen, die ohnehin vorhanden sind (zum Beispiel die kaufmännische Buchführung über Einkäufe und Bestellungen) können ohne jede Schwierigkeit sekundären Nutzungen zugeführt werden (Verwendung für eigene oder fremde Werbung, Überwachung des Personals und so weiter). Selbst so einleuchtende neue Instrumente wie eine Gesundheitschipkarte zum Einsatz in Notfällen kann den künftigen Arbeitgeber dazu verführen, einen Blick in die Daten zu werfen, bevor die Einstellungsentscheidung getroffen ist.

Eine erhebliche Verlockung zur Zweckentfremdung von Daten stellt eine technische Eigenschaft elektronischer Telekommunikationseinrichtungen dar: Im Gegensatz zum klassischen »Fernmeldenetz« hinterlässt die Nutzung der Telekommunikation Spuren: Nach Beendigung einer Verbindung sind Daten hierüber nach wie vor vorhanden, jeder Zugriff auf Datenbestände wird protokolliert, jede Vermittlungsstelle kann die durchlaufenden Datenströme »absaugen« und speichern. Die Auswertung, gegebenenfalls die Zusammenführung dieser Daten gestattet, das Verhalten der Teilnehmer zu analysieren, Profile zu bilden und diese für vielfältige Zwecke zu verwenden, sei es zur Werbung, sei es zur Ausspähung des persönlichen Verhaltens für die verschiedensten unlauteren Zwecke.

Man begegnet immer wieder Pharisäern, die davon überzeugt sind, jeder dürfe über sie alles wissen, man habe nichts zu verbergen. Abgesehen davon, dass wohl jeder seine Geheimnisse hat, die er anderen nicht preisgeben möchte, wird dem Einzelnen dabei das wesentliche Risiko nicht bewusst. Das Wissen, dass Außenstehende jederzeit über Daten über das eigene Verhalten verfügen können, wirkt auf das eigene Verhalten zurück. Diese Umkehrung der informationellen Selbstbestimmung wurde vom Bundesverfassungsgericht eindrucksvoll beschrieben: Wer davon überzeugt ist, dass andere Stellen Daten über seine Verhaltensweisen speichern und weitergeben, wird sein eigenes Verhalten ändern, wird von seinen grundrechtlich verbrieften Freiheitsrechten nicht mehr in dem Maße Gebrauch machen, wie ihm dies die Verfassung garantiert.

3. Die Antwort: Grundprinzipien des Datenschutzes

In der Debatte um den »Privacy Act« in den USA wurden die Grundprinzipien entwickelt, die heute den Datenschutzstandard weltweit prägen. Sie kommen am deutlichsten in der erwähnten UNO-Resolution zum Ausdruck. Hierzu gehören:

- *Der Grundsatz der Rechtmäßigkeit und der Beachtung von Treu und Glauben:* Formen der Datenverarbeitung, die gegen die Menschenwürde verstoßen (Speicherung von Daten, die durch Folter erhoben wurden) oder die unter Täuschung erhoben wurden (Erhebung von Daten durch Kreditinformationsunternehmen unter »Legende«, das heißt verdeckter Identität), sind auszuschließen.
- *Der Grundsatz der Richtigkeit:* Datenverarbeiter sind nicht nur verpflichtet, richtige Daten zu verarbeiten, sondern die Richtigkeit auch regelmäßig zu überprüfen (die Verhaftung einer Person, nach der irrtümlich gefahndet wurde, und die mangels Datenpflege in internationalen Fahndungsdateien noch immer gespeichert ist, ist auszuschließen).
- *Der Grundsatz der Zweckbestimmung:* Daten dürfen grundsätzlich nur zu dem Zweck verwendet werden, zu dem sie erhoben wurden; zweckwidrige Nutzung sowie zu lange Speicherung sind auszuschließen (eine systematische Auswertung von Verhaltensprofilen kommt nicht in Betracht).
- *Der Grundsatz des Auskunftsrechts der Betroffenen:* Jeder soll wissen, wer welche Daten über ihn verarbeitet (auch die Sicherheitsbehörden haben grundsätzlich Auskunft zu erteilen).
- *Der Grundsatz der Nichtdiskriminierung:* Besonders sensible Daten, die zu einer Diskriminierung von Betroffenen führen können, dürfen nicht oder jedenfalls nur unter sehr beschränkten Voraussetzungen verarbeitet werden (ethnische Zugehörigkeit, Sexualleben, weltanschauliche Überzeugungen).

Weitere Grundsätze betreffen die Informationssicherheit, die Kontrollmechanismen oder den grenzüberschreitenden Datenverkehr.

Dieser über alle Ländergrenzen hinweg geltende Datenschutzstandard reicht jedoch vor dem Hintergrund der aktuellen Entwicklung der Informationstechnik nicht aus. Insbesondere der Ausbau der Telekommunikationsnetze und der auf ihnen betriebenen Informationsdienste zeigt die Notwendigkeit von Regelungen, die das bisher übliche Schema der Datenschutzgesetzgebung verlassen.

Zwar kommt in den Datenschutzgesetzen im Prinzip der »Erforderlichkeit« schon zum Ausdruck, dass nur diejenigen Daten erhoben und verarbeitet werden sollten, die, sei es für die Erfüllung öffentlicher Aufgaben, sei es für die Vertragsabwicklung, unbedingt nötig sind. Dieser Gedanke berücksichtigt aber nicht hinreichend, dass bereits bei der Konzeption von Aufgabenstellungen, Vertragsgestaltungen oder Systemarchitekturen auf Datensparsamkeit geachtet werden sollte. Von vornherein sollten in der Gesetzgebung, aber auch im privatrechtlichen Verkehr Rechtsformen gefunden werden, die mit einem Minimum an personenbezogenen Daten auskommen. Das BDSG 2001 berücksichtigt dieses Prinzip inzwischen.

Die Forderung richtet sich insbesondere an die Anbieter von Informationsdienstleistungen. Unter dem Stichwort »Privacy Enhancing Technologies« werden Telekommunikationsformen diskutiert, die bereits das Entstehen von Datenspuren in den Netzen verhindern. Hierzu gehört, dass bei der Nutzung gebührenpflichtiger Informationstechniken zumindest optional ein anonymer Zugang angeboten wird. Zahlungsmöglichkeiten mit vorbezahlten Zahlungsmitteln oder allgemein nutzbare öffentliche Zugangsstellen sind hier Mittel der Wahl.

Informationelle Selbstbestimmung bedeutet konsequenterweise, dass dem Betroffenen auch die Option eröffnet wird, der Verarbeitung seiner eigenen Daten nicht nur zu widersprechen, sondern ausdrücklich in sie einzuwilligen. Dies wird oft genutzt, wenn vom Gesetz selbst nicht gestattete Formen der Datenverarbeitung durchgeführt werden sollen. Voraussetzung für die Wirksamkeit der Einwilligung ist, dass die Betroffenen darüber informiert sind, worauf sie sich einlassen (informed consent). Die Praxis der Online-Dienste zeigt, dass die Aufklärung der Betroffenen bei weitem nicht den hinreichenden Stellenwert besitzt.

Die schwierigsten Probleme wirft die Kontrolle des Umgangs mit der Informationstechnik auf. Weltweit ist derzeit ein zentrales Thema, ob unkontrollierter Informationsfluss im Netz zum Grundbestand der Menschenrechte gehört oder ob nicht organisatorische und technische Kontrollen zur Verhinderung der Verbreitung strafbarer Informationen wie Pornografie, Anleitung zum Bombenbau oder Volksverhetzung eingerichtet werden müssen – mit allen Folgen der informationellen Verseuchung einerseits, des Risikos überschießender Überwachung andererseits. Die Ereignisse des 11. September 2001 und die darauf in vielen Ländern geschaffenen Terrorismusbekämpfungsgesetze verschärfen dieses Dilemma.[12]

4. Geltungsbereich der Datenschutzgesetze

Für Bundesbehörden und private Unternehmen (»nicht-öffentliche Stellen«) gilt das Bundesdatenschutzgesetz (BDSG), das gesonderte Teile für Bundesbehörden und Privatunternehmen enthält. Öffentliche Stellen der Länder unterliegen den jeweiligen Landesdatenschutzgesetzen.

Die Datenschutzgesetze gelten nur für personenbezogene Daten. Die Daten müssen sich also auf bestimmte Personen beziehen. Allerdings reicht die Möglichkeit aus, mit verhältnismäßigen Mitteln die Person ausfindig zu machen. Datensätze, in denen zwar kein Name, aber Geburtsdatum und Geburtsort vorkommen, fallen darunter. Schwierig zu beantworten, aber von erheblicher Konsequenz ist die Frage, ob Kennzeichnungen, die technischen Geräten zugeordnet sind (zum Beispiel Telefonnummern, IP-Adressen, künftig GUIDs), einen Personenbezug herstellen. Sie stellt sich vor allem bei dynamischer Adressenvergabe. Da nicht unterschieden werden kann, ob es sich um eine statische oder dynamische Zuordnung handelt, aber die Provider die Zuordnung kennen (entsprechende Protokollierung vorausgesetzt), sind Informationen, die sich auf derartige Kennzeichnungen beziehen, als personenbezogen anzusehen, so dass die Datenschutzgesetze gelten.

Besondere Regeln gelten für besondere Arten personenbezogener Daten, nämlich Angaben über ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben. Sie werden häufig auch sensible Daten (richtiger: sensitive Daten) genannt. Sie dürfen nur verarbeitet werden, wenn ein Gesetz das ausdrücklich vorsieht oder die Betroffenen eingewilligt haben.

Das Datenschutzrecht differenziert zwischen einzelnen Phasen des Umgangs mit Daten. So gibt es gesonderte Regelungen für die Datenerhebung bei öffentlichen Stellen sowie im öffentlichen und nicht öffentlichen Bereich für die Datenübermittlung. Im privaten Bereich ist die Geltung des BDSG auf die Verarbeitung von Daten in automatisierten Verfahren oder nicht automatisierten Dateien beschränkt. Der Umgang mit Daten in Akten fällt nicht unter das BDSG. Angesichts der zunehmenden Automatisierung spielt das aber kaum mehr eine Rolle.

Ausgenommen sind auch Verarbeitungen, die ausschließlich für *persönliche oder familiäre Zwecke* erfolgen, wobei etwa bei der Verbreitung von Daten im Internet genau zu prüfen ist, ob die Grenzen privater Nutzung nicht überschritten werden.

Bestehen neben dem BDSG beziehungsweise den Landesdatenschutzgesetzen besondere Rechtsvorschriften, die auf personenbezogene Daten anzuwenden sind, gehen diese vor (Subsidiarität der allgemeinen Datenschutzgesetze); dies hat insbesondere Bedeutung für den Bereich der Sicherheitsbehörden (Strafprozessordnung, Polizeigesetze, Verfassungsschutzgesetze), der Sozialverwaltung (Vorrang des Sozialgesetzbuches, insbesondere SGB X) oder im Bereich anderer Berufs- und besonderer Amtsgeheimnisse (zum Bei-

spiel ärztliche Schweigepflicht, Steuergeheimnis), aber auch für die Verarbeitung von Daten bei der Telekommunikation.

5. Zulässigkeit der Datenverarbeitung

Die Datenschutzgesetze wenden sich an verantwortliche Stellen, die Daten für sich selbst erheben, verarbeiten oder nutzen. Werden Daten von anderen Stellen im Auftrag verarbeitet, bleibt die Zuständigkeit beim Auftraggeber. Wenn also jemand bei einem Webhost eine Website einrichtet, bleibt er selbst für die Inhalte verantwortlich.

Das deutsche Datenschutzrecht geht davon aus, dass die Verarbeitung personenbezogener Daten nur erlaubt ist, wenn hierfür eine Befugnisnorm vorliegt (»Verbot mit Erlaubnisvorbehalt«). Dieses angesichts der Entwicklung der Informationstechnik anachronistisch anmutende Prinzip wird allerdings dadurch abgemildert, dass die Erlaubnistatbestände sehr weit formuliert sind. So gibt es weit gefasste Befugnisse zur Verarbeitung personenbezogener Daten zum einen auf Grund des BDSG beziehungsweise der Landesgesetze selbst, zum anderen auf Grund einer Rechtsgrundlage in Spezialgesetzen oder auf Grund der Einwilligung der Betroffenen.

In der Praxis muss in umgekehrter Reihenfolge geprüft werden: Zunächst muss festgestellt werden, ob eine Einwilligung in die Verarbeitung der Daten vorliegt. Diese Voraussetzung ist die weitestgehende, setzt allerdings eine umfassende Information über den Zweck der Erhebung, Verarbeitung oder Nutzung sowie über die Folgen der Verweigerung der Einwilligung voraus. Die Einwilligung, die nur wirksam ist, wenn sie auf der freien Entscheidung des Betroffenen beruht, muss in der Regel schriftlich abgegeben werden. Soll die Einwilligung über ein Telekommunikationsnetz eingeholt werden, sind die Bestimmungen des Teledienstrechtes zur elektronischen Einwilligung zu beachten (siehe unten). Sollen besondere Arten personenbezogener Daten verarbeitet werden, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

Liegt keine Einwilligung vor, ist zunächst zu prüfen, ob spezialrechtliche Regelungen die Verarbeitung der Daten gestatten. Hiervon gibt es auf Bundes- und Landesebene Hunderte von Vorschriften. Diese gehen nur in dem Umfang den allgemeinen Datenschutzregelungen vor, als sie deckungsgleiche Interessen berücksichtigen. Fehlt zum Beispiel in einem Gesetz eine Auskunftsregelung über die gespeicherten Daten, heißt das nicht, dass kein Auskunftsanspruch besteht, sondern hier kommt der Anspruch des BDSG wieder zum Zuge. Liegen beide Voraussetzungen nicht vor, sind die Rechtsgrundlagen des Bundes- beziehungsweise der Landesdatenschutzgesetze selbst zu prüfen.

Entgegen den Vorgaben der Europäischen Datenschutzrichtlinie, die eine Unterscheidung zwischen öffentlichem und nicht-öffentlichem Bereich nicht

kennt, wird die materielle Zulässigkeit des Umgangs mit personenbezogenen Daten in diesen Bereichen nach wie vor unterschiedlich geregelt.

Die allgemeinen Datenschutzregelungen im *öffentlichen Bereich* stellen bereits bei der Erhebung der Daten auf die Erforderlichkeit der Kenntnis der Daten zur Erfüllung der Aufgaben der verantwortlichen Stelle ab. Ohne weitere Voraussetzung ist die Verarbeitung dieser Daten nur zu dem Zweck zulässig, zu dem die Daten erhoben wurden; weite Ausnahmekataloge weichen das Prinzip der Zweckbindung allerdings erheblich auf. Sollen die Daten an andere Stellen übermittelt werden, wird differenziert nach den Adressaten: Öffentliche Stellen erhalten die Daten im Rahmen ihrer Aufgabenerfüllung auch dann, wenn sich der Zweck ändert; an nicht-öffentliche Stellen ist die Übermittlung normalerweise nur zulässig, wenn dies für die Aufgabenerfüllung der übermittelnden Stelle selbst erforderlich ist (Beispiel: Das Sozialamt überweist die Sozialhilfe auf ein Bankkonto). Wenn derjenige, an den die Daten übermittelt werden sollen, selbst ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft macht, ist die Übermittlung nur zulässig, wenn der Betroffene kein entgegenstehendes Interesse hat.

Bei der Zulässigkeit des Umgangs mit personenbezogenen Daten durch *nicht-öffentliche Stellen* (insbesondere Privatunternehmen) wird zunächst danach unterschieden, ob die Daten zu eigenen Geschäftszwecken, also als Hilfsmittel für die eigene Geschäftstätigkeit (zum Beispiel Kunden- oder Personaldaten) oder zu fremden Zwecken mit dem Ziel der Übermittlung (Schufa, Auskunfteien, Adresshändler) verarbeitet werden.

Der Umgang mit personenbezogenen Daten im Privatbereich zu eigenen Zwecken ist – als Grundregel – immer dann zulässig, wenn er der *Zweckbestimmung eines Vertragsverhältnisses* mit dem Betroffenen dient. Dies muss eng gesehen werden: Wie verschiedene Gerichte betont haben, muss die Verarbeitung der Daten für die Vertragserfüllung erforderlich sein, ein loser Zusammenhang genügt nicht. So darf ein Arbeitgeber in einem Personalinformationssystem nicht speichern, ob jemand bei der Bundeswehr Offizier war, nur weil er meint, dass damit besondere Befähigungen zur Personalführung verbunden sind.

Über diese Grundbestimmung hinaus ist die Verarbeitung der Daten auch dann zulässig, wenn sie zur Wahrung *berechtigter Interessen* der verantwortlichen Stelle erforderlich ist und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder der Nutzung der Daten überwiegt. Diese komplizierte, aber gern genutzte Generalklausel ermöglicht, im Bereich wenig sensitiver Daten Geschäftszwecke zu verfolgen, die von vertraglichen Verhältnissen (noch) nicht abgedeckt sind, etwa im Bereich der Werbung.

Noch größere Zurückhaltung gebietet die dritte Befugnisnorm des BDSG: Danach dürfen Daten, die *allgemein zugänglich* sind, ohne Nachweis jeden eigenen Interesses verarbeitet werden, wenn nicht Belange der Betroffenen »offensichtlich« entgegenstehen. Da zum Beispiel die im Internet zur Verfügung

stehenden Daten allgemein zugänglich sind, könnte dies einen Freibrief für die Verarbeitung aller dieser Daten darstellen, etwa was die Ergebnisse personenorientierter Abfragen mit Hilfe von Suchmaschinen betrifft. Um dies zu vermeiden, muss bei der Weiterverarbeitung derartiger Daten ein strenger Maßstab an die Prüfung der schutzwürdigen Interessen der Betroffenen angelegt werden. Das Gleiche gilt für die Befugnis, wenig sensitive Daten wie Berufs-, Branchen- oder Geschäftsbeziehung, Namen, Anschrift oder Geburtsjahr listenmäßig zu übermitteln. Eine voraussetzungslose Verbreitung dieser Daten im Netz ohne die Berücksichtigung schutzwürdiger Interessen der Betroffenen ist ebenfalls ausgeschlossen. Der der informationellen Selbstbestimmung angemessene Weg ist auch in diesen Fällen die Einwilligung.

Die *geschäftsmäßige Datenverarbeitung zum Zwecke der Übermittlung* wirft insbesondere bei der Nutzung Neuer Medien ganz erhebliche Probleme auf. Bereits bei der Erhebung, Speicherung oder Veränderung (zum Beispiel durch Neugruppieren) der Daten sind entgegenstehende schutzwürdige Interessen der Betroffenen zu berücksichtigen (zum Beispiel bei der Profilbildung für den Adressenhandel). Die Übermittlung dieser Daten, und damit die Einstellung der Daten in Netze, ist darüber hinaus nur zulässig, wenn die abrufende Stelle (zum Beispiel das Unternehmen, das die Adressen ankauft) ihr berechtigtes Interesse an der Kenntnis der Daten glaubhaft dargelegt hat. Es darf kein Grund zur Annahme bestehen, der Betroffene habe ein schutzwürdiges Interesse am Ausschluss der Übermittlung (hier: der Zurverfügungstellung im Netz). Diese Voraussetzungen können nur in geschlossenen Benutzergruppen verwirklicht werden, was vom Anbieter derartiger Dienstleistungen ein hohes Maß an technisch-organisatorischen Aufwendungen verlangt.

6. Betroffenenrechte

Als eines der wichtigsten Prinzipien, ja als »Magna Charta« des Datenschutzes galt von jeher das Recht der Betroffenen auf Kenntnis der Daten, die über sie verarbeitet werden. Ein *Recht auf Auskunft* sah daher bereits das BDSG 1977 vor, wenn auch mit vielerlei Ausnahmen versehen. Die Rechte auf Transparenz der Datenverarbeitung sind im Verlauf der Gesetzgebung deutlich ausgeweitet worden. Sie haben besondere Bedeutung im Internet, da gerade hier Verarbeitungen stattfinden, die den Betroffenen nicht von vornherein bekannt sind.

Von Auskunftswünschen der Betroffenen und deren Rechten auf aktiven Informationszugang zu unterscheiden sind zunächst die unabhängig davon bestehenden Verpflichtungen der verantwortlichen Stellen zur vorherigen Information. Wird die Datenverarbeitung auf die Einwilligung der Betroffenen gestützt, sind diese auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie nach den Umständen des Einzelfalles oder auf Verlangen

auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Werden die Daten beim Betroffenen erhoben, wozu die verantwortliche Stelle in der Regel verpflichtet ist, hat diese ihre Identität, die Zweckbestimmung sowie die Kategorien von Empfängern mitzuteilen, wenn der Betroffene mit der Übermittlung nicht rechnen muss. Besteht schließlich eine rechtliche Verpflichtung zur Offenbarung von Daten, ist der Betroffene hierauf hinzuweisen, auf Wunsch auch über die Rechtsgrundlage sowie die Folgen einer Verweigerung.

Während diese Bestimmungen sowohl für den öffentlichen als auch für den nicht-öffentlichen Bereich gleichermaßen gelten, enthält das BDSG für die *Erhebung der Daten ohne Kenntnis der Betroffenen* differenzierte Regelungen. Im öffentlichen Bereich sind die Betroffenen in derselben Weise zu unterrichten als wenn die Daten bei diesen selbst erhoben würden, hinzu kommt eine Benachrichtigungspflicht über vorgesehene Übermittlungen. Die Benachrichtigungspflichten im nicht-öffentlichen Bereich sind ähnlich ausgestaltet, hinzu kommt hier jedoch die Verpflichtung, auch die Art der gespeicherten Daten mitzuteilen.

Beide Bereiche kennen eine Vielzahl von Ausnahmen, die den Umfang der Benachrichtigungspflicht deutlich relativieren. Die Ausnahmekataloge unterscheiden sich im Einzelnen, jedoch spielen die Tatbestände, dass der Betroffene auf andere Weise Kenntnis von Speicherung und Übermittlung erlangt hat oder dass die Verarbeitung der Daten gesetzlich vorgeschrieben ist, in beiden Bereichen die größte Rolle. Sicherheitsinteressen des Staates und die Abwehr von Gefährdungen des Geschäftszweckes sind selbstredend ebenfalls Gründe, von der Benachrichtigung abzusehen.

Für die Wahrung der Interessen der Betroffenen von größerer Bedeutung ist das *aktive Auskunftsrecht*. Hierbei werden nicht nur die Umstände der Datenverarbeitung im Allgemeinen mitgeteilt, sondern die tatsächlich zur Person des Betroffenen gespeicherten Daten, einschließlich ihrer Herkunft, die Empfänger oder Kategorien von Empfängern und der Zweck der Speicherung. Der Anspruch im öffentlichen und nicht-öffentlichen Bereich ist im Wesentlichen gleich ausgestaltet. Die Ausnahmen entsprechen im Wesentlichen denjenigen bei der Unterrichtungspflicht.

Berichtigung, Löschung und Sperrung (das heißt eine Einschränkung der Nutzungsmöglichkeiten) sind in der Regel von der verantwortlichen Stelle ohne Beteiligung des Betroffenen vorzunehmen. Allerdings kann dieser selbst tätig werden: Wird die Richtigkeit von Daten vom Betroffenen bestritten und lässt sich weder die Richtigkeit noch die Unrichtigkeit feststellen, sind die Daten zu sperren. Nicht-öffentliche Stellen dürfen besondere Arten von Daten, zu denen in diesem Fall auch Daten über strafbare Handlungen oder Ordnungswidrigkeiten zählen, auch ohne Eingreifen des Betroffenen nur speichern, wenn diese bewiesen werden können.

Ganz neu im deutschen Datenschutzrecht ist das Recht der Betroffenen, der Erhebung, Verarbeitung und Nutzung wegen ihrer besonderen persönlichen Situation zu widersprechen, selbst wenn die Verarbeitung der Daten

ansonsten rechtmäßig ist. Diese Regelung hat vor allem da Bedeutung, wo die Rechtmäßigkeit auf pauschale Güterabwägungen gestützt wird, bei der häufig die spezielle persönliche Lebenssituation nicht berücksichtigt werden kann. So kann künftig ein Arbeitnehmer der Speicherung von Daten zu seiner betrieblichen Förderung widersprechen, wenn er selbst diese Förderung gar nicht in Anspruch nehmen will.

Im Bereich der Werbung oder der Markt- und Meinungsforschung besteht ein generelles Widerspruchsrecht ohne Angabe von Gründen; der Betroffene ist hierüber zu unterrichten. Eine Sonderregelung besteht für Adress-, Telefon-, Branchen- sowie vergleichbare Verzeichnisse: Der Betroffene hat das Recht, selbst zu entscheiden, ob diese Daten elektronisch oder gedruckt weiterverbreitet werden dürfen, entsprechende Kennzeichnungen sind in den Verzeichnissen anzubringen.

Bei unzulässiger oder unrichtiger Erhebung, Verarbeitung oder Nutzung besteht ein besonderer Schadensersatzanspruch. Dieser Anspruch ist jedoch nur im öffentlichen Bereich als Gefährdungshaftung ausgestaltet, das heißt ein Verschulden der verantwortlichen Stellen spielt keine Rolle. Bei schweren Persönlichkeitsverletzungen kann entsprechend dem Schmerzensgeld auch immaterieller Schadensersatz verlangt werden. Im nicht-öffentlichen Bereich entfällt dagegen die Schadensersatzpflicht, wenn die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

7. Technische und organisatorische Maßnahmen

Das neue BDSG enthält eine Reihe von Regelungen, die die weltweit diskutierte Hinwendung des Datenschutzes zu technischen Lösungen (»*privacy enhancing technologies*«) und zur Selbstregulierung der verantwortlichen Stellen widerspiegeln. Wenig verändert gegenüber den vorherigen Bestimmungen ist die Verpflichtung zur Gewährleistung einzelner Maßnahmen zur *Datensicherheit*, die nach wie vor in einer Anlage zum BDSG aufgelistet sind. Neu ist, dass der Schutz (auch) vor zufälliger Zerstörung oder Verlust in den Katalog der Kontrollmaßnahmen aufgenommen wurde. Die Sicherstellung der Verfügbarkeit der Datenverarbeitung wurde damit zu einer datenschutzrechtlichen Aufgabe.

Die Hinwendung zu neuen Formen des Datenschutzes kommt am stärksten in der Verpflichtung zum Ausdruck, dass sich Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel auszurichten haben, keine (*Datenvermeidung*) oder so wenig personenbezogene Daten wie möglich (*Datensparsamkeit*) zu erheben, zu verarbeiten oder zu nutzen. *Anonymisierung* oder gegebenenfalls zur *Pseudonymisierung* (das heißt die Zuordnung von Daten ist nur den Betroffenen selbst oder ganz bestimmten Institutionen möglich) sind so weit wie möglich anzubieten. Die Erforderlichkeit von Daten darf daher

nicht mehr erst nach Fertigstellung der Verfahren und Programme beurteilt werden, sondern muss bereits bei der Konzeption selbst geprüft werden.

8. Besondere Formen der Datenverarbeitung

Neu im BDSG ist das Verbot, automatische Entscheidungen hinsichtlich der Bewertung einzelner Persönlichkeitsmerkmale zu fällen, die für den Betroffenen eine ungünstige rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen. Das hat zum Beispiel Bedeutung bei der automatischen Berechnung der Kreditwürdigkeit durch Scoringverfahren.

Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) hat das BDSG neu geregelt. Sowohl die Beobachtung selbst als auch die Verarbeitung und Nutzung der dabei gewonnenen Daten setzen jeweils eine Bewertung der Erforderlichkeit für die Aufgabenerfüllung (öffentliche Stellen) oder für die Durchsetzung des Hausrechts (öffentliche und nicht-öffentliche Stellen) voraus. Bei anderen berechtigten Interessen (zum Beispiel Dokumentation von Vorgängen) müssen die Zwecke konkret festgelegt werden. Eine Reihe technischer Regelungen, zum Beispiel zur Information der Betroffenen oder zur frühzeitigen Löschung, kommt hinzu. Diese Bestimmungen sind nur anwendbar, wenn Videotechnik zur gezielten Beobachtung von Personen eingesetzt wird; Aufnahmen von Räumen und Landschaften, bei denen Personen nur Beiwerk sind, fallen nicht darunter. Andererseits schließt der Erforderlichkeitsgrundsatz den Einsatz der Videotechnik im Internet (Webcam) ohne ausdrückliche Einwilligung der gezielt beobachteten Personen generell aus, da eine Verbreitung der Aufnahmen im Internet nie erforderlich ist. Die Notwendigkeit der Einwilligung ergibt sich auch aus dem Kunsturhebergesetz.

Auch der Einsatz mobiler personenbezogener Speicher- und Verarbeitungsmedien ist nunmehr im BDSG geregelt. Diese Bestimmungen betreffen Chipkarten und andere Geräte (zum Beispiel Tokens, Handys und so weiter), die über eigene Datenverarbeitungskapazitäten verfügen. Hier werden neue Anforderungen an Transparenz und Technikgestaltung gestellt, insbesondere zur Erkennbarkeit von Kommunikationsvorgängen, die auf dem Medium eine Datenverarbeitung auslösen. Das Zusammenwachsen von Medien- und Kommunikationstechnik wird dieser Bestimmung große Bedeutung verschaffen.

9. Selbstregulierung, Selbstdatenschutz

Die Intransparenz der Informationsverarbeitung für Außenstehende erzwingt eine zunehmende Beteiligung der verantwortlichen Stellen an der Ausge-

staltung der Regelungen einerseits (*Selbstregulierung*) sowie eine durch technische Maßnahmen unterstützte Einbeziehung der Betroffenen andererseits (*Selbstdatenschutz*). Im Rahmen der Selbstregulierung bietet das BDSG Berufsverbänden und anderen Vereinigungen an, Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen durch die Aufsichtsbehörden prüfen zu lassen. Bei einem positiven Prüfergebnis stellen die in der Verhaltensrichtlinie enthaltenen Grundsätze eine verbindliche Interpretation der datenschutzrechtlichen Regelungen dar. Die Möglichkeiten der Betroffenen selbst, Mittel zu ergreifen, die dem Schutz ihrer personenbezogenen Daten dienen (Selbstdatenschutz), sind im Datenschutzrecht noch nicht ausgeprägt. Von zentraler Bedeutung wird künftig das Recht auf anonymes oder pseudonymes Handeln im Geschäftsverkehr, aber auch im Kontakt mit öffentlichen Stellen sein. Die Anbieter von Hard- und Software, aber auch Diensteanbieter müssen mehr als bisher den Betroffenen Mittel in die Hand geben, den Umfang der Daten, die über sie verarbeitet werden, selbst festzulegen. Die seit neuem in die Browser eingebaute P3P-Funktion, mit der die Nutzer in gewissem Umfang selbst bestimmen können, was der Anbieter einer Website mit den Nutzungsdaten macht, ist ein wichtiger Schritt in diese Richtung.[13]

10. Kontrollstellen

Das deutsche Datenschutzrecht sah von Anfang an unterschiedliche Kontrollinstitutionen für die Einhaltung der datenschutzrechtlichen Vorschriften vor. Für den öffentlichen Bereich des Bundes und der Länder wurden von Anfang an unabhängige Datenschutzbeauftragte ernannt, die ihre Befugnisse zur Förderung der informationellen Selbstbestimmung teilweise energisch wahrnahmen und damit zur Verbreitung des Datenschutzgedankens in der Öffentlichkeit erheblich beitrugen. Für den nicht-öffentlichen Bereich wurden die Länder verpflichtet, Aufsichtsbehörden zu benennen, die allerdings in der Regel in den Innenministerien angesiedelt wurden, ohne dass ihnen hinreichende Arbeitsmöglichkeiten und eine den Landesbeauftragten vergleichbare Unabhängigkeit eingeräumt wurden. Diese Aufgabe wird nach dem Vorbild einiger Länder, die von Anfang an dieses Regelungsmodell gewählt hatten (wie die Stadtstaaten Hamburg und Bremen), zunehmend den Landesbeauftragten übertragen.

Daneben sehen das BDSG für die Bundesbehörden und Privatunternehmen, die Landesdatenschutzgesetze für die Landesbehörden die Bestellung von internen Datenschutzbeauftragten vor, die im Unternehmen oder in der Behörde auf die Einhaltung datenschutzrechtlicher Bestimmungen hinwirken sollen. Eine Sonderrolle, die sich aus dem Rundfunk- und Religionsprivileg des Grundgesetzes ergibt, spielen die Datenschutzbeauftragten der öf-

fentlichen Rundfunk- und Medienanstalten sowie diejenigen der Religionsgesellschaften.

Die Bundes- und Landesdatenschutzbeauftragten werden von den Parlamenten gewählt und arbeiten weisungsfrei. Sie kontrollieren umfassend die Einhaltung der datenschutzrechtlichen Vorschriften durch öffentliche Stellen auch bei den Daten, die besonderen Berufs- und Amtsgeheimnissen unterliegen. Dafür sind ihnen alle gewünschten Informationen zur Verfügung zu stellen sowie Zugang zu Unterlagen und Zutritt zu Diensträumen zu gewähren. Anlass des Tätigwerdens der Datenschutzbeauftragten sind Beschwerden von Betroffenen, Beratungsersuchen öffentlicher Stellen, auch der Parlamente, aber auch Prüfungen von Amts wegen. In unterschiedlichen Perioden (ein- oder zweijährig) müssen Tätigkeitsberichte vorgelegt werden, die einen guten Überblick über den Stand der Datenschutzdiskussion geben. Sie sind auf den Websites der Datenschutzbeauftragten abrufbar.[14]

Den umfassenden Informationsrechten stehen allerdings keine Exekutivbefugnisse gegenüber. Die Handlungsmöglichkeiten beschränken sich vielmehr auf das Beanstandungsrecht sowie darauf, Maßnahmen zur Verbesserung des Datenschutzes zu empfehlen. Weisungsbefugnisse gegenüber öffentlichen Stellen haben die Datenschutzbeauftragten nicht.

Die Aufgaben der Aufsichtsbehörden sind deutlicher auf die Bearbeitung von Beschwerden hin orientiert. Erst seit dem neuem BDSG haben sie die Befugnis, auch von Amts wegen Überprüfungen vorzunehmen. Die Informationsrechte der Aufsichtsbehörden entsprechen denjenigen der öffentlichen Datenschutzbeauftragten. Das Handlungsinstrumentarium geht allerdings darüber hinaus: Neben dem – selbstverständlichen – Recht, Verstöße mitzuteilen und Empfehlungen zu geben, können zur Gewährleistung der Datensicherheit Maßnahmen angeordnet, bei schwerwiegenden Verstößen auch einzelne Datenverarbeitungsverfahren untersagt werden. Materielle Verstöße können als Ordnungswidrigkeiten auch mit Bußgeldern bis zu 250 000 Euro geahndet werden.

Das BDSG schreibt in der Regel die Benennung interner Datenschutzbeauftragter vor, deren Aufgabe die Sicherstellung des Datenschutzes im Betrieb beziehungsweise in der Behörde ist. Bei automatisierter Verarbeitung personenbezogener Daten gilt dies für öffentliche Stellen immer, für nicht öffentliche Stellen, wenn mehr als vier Beschäftigte mit der Datenverarbeitung befasst sind. Bei nicht automatisierter Datenverarbeitung ist ein Datenschutzbeauftragter zu benennen, wenn mindestens 20 Personen damit beschäftigt werden. Eine der wesentlichen Folgen der Benennung interner Datenschutzbeauftragter ist, dass die von der Europäischen Datenschutzrichtlinie vorgeschriebene Registrierung von Verfahren bei der Kontrollstelle durch eine interne Erfassung ersetzt wird. Die Datenschutzbeauftragten, die fachkundig und zuverlässig sein müssen, haben neben ihrer originären Aufgabe auf die Einhaltung der datenschutzrechtlichen Bestimmungen hinzuwirken, insbesondere die bei der Datenverarbeitung beschäftigten Personen fortzubilden.

11. Vorabkontrolle und Datenschutzaudit

Das neue BDSG enthält erstmals die Verpflichtung, eine Vorabkontrolle der Datenverarbeitung durchzuführen, wenn automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen. Als besonders risikoreich gelten vor allem Verarbeitungen besonderer Arten personenbezogener Daten oder Verfahren, die der Persönlichkeitsbewertung dienen sollen. Die Regelung gilt allerdings in den Fällen nicht, in denen die Verfahren mit Einwilligung der Betroffenen oder im Rahmen von Vertragsverhältnissen eingesetzt werden.

Zur Sicherstellung des internen Datenschutzes sieht das neue BDSG neben der Einrichtung von Datenschutzbeauftragten die Möglichkeit vor, ein Datenschutzaudit vornehmen zu lassen. Danach können sowohl Anbieter von Datenverarbeitungssystemen und -programmen als auch Daten verarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen unabhängig prüfen lassen. Diese Bestimmung muss allerdings noch durch ein besonderes Gesetz konkretisiert werden.

12. Besondere Regelungen für die Telekommunikation

Wie für andere Bereiche auch gelten für den Datenschutz in der Telekommunikation besondere Vorschriften, die denen des BDSG vorgehen. Dabei ist zwischen zwei Ebenen zu unterscheiden: Der Datenschutz im Bereich der technischen Telekommunikation, also bei der Übertragung und Vermittlung von Daten, wird im Telekommunikationsgesetz (TKG)[15] und den dazu erlassenen Verordnungen, hier vor allem in der Telekommunikations-Datenschutzverordnung (TDSV)[16] und der Telekommunikations-Überwachungsverordnung (TKÜV) geregelt. Diese Vorschriften gelten für alle Unternehmen, die Telekommunikationsnetze für die Öffentlichkeit betreiben (zum Beispiel Deutsche Telekom oder Mannesmann/Vodafone). Die Regulierungsbehörde für Post und Telekommunikation (Reg TP) hat hier wesentliche Genehmigungs- und Eingriffsbefugnisse.

Soweit es um die Verarbeitung von Daten durch Diensteanbieter geht, zum Beispiel durch Access-Provider oder Anbieter von Websites, gelten andere Vorschriften: Wegen der unterschiedlichen Gesetzgebungszuständigkeiten gilt für Dienste, die mehr auf die individuelle Kommunikation hin orientiert sind (zum Beispiel Teleshopping oder Telebanking), das Teledienstegesetz (TDG)[17] sowie das Teledienstedatenschutzgesetz (TDDSG) des Bundes[18], für Verteildienste, bei denen die Information der Nutzer im Vordergrund steht und die inhaltlich aufbereitet sind, der Mediendienste-Staatsvertrag (MDStV) der Länder[19]. Besondere Regelungen gelten für die Dienste, die Rundfunkanstalten anbieten.[20] Diese Aufspaltung auf der Diensteebene hat

aber keine große inhaltliche Bedeutung. Obwohl das TDG und das TDDSG im Rahmen des Elektronischen-Geschäftsverkehr-Gesetzes 2001[21] gründlich überarbeitet wurden, entsprechen deren Regelungsinhalte im Wesentlichen nach wie vor denjenigen des MDStV. Besondere Regelungen sind in diesem Gesetz besonders für die »kommerzielle Kommunikation« (»B2B«) geschaffen worden.

13. Telekommunikationsgesetz

Wer Telekommunikationsdienstleistungen anbietet, hat die Möglichkeit, von den übermittelten Nachrichten Kenntnis zu nehmen, wenn diese nicht verschlüsselt sind. Er erfährt insbesondere auch, wer wann mit wem und mit welchen Kommunikationsmitteln (»Diensten«) kommuniziert hat. Bereits seitdem Fernmeldeanlagen der Öffentlichkeit zur Verfügung stehen, wurden daher alle Personen, die Zugang zu diesen Informationen hatten, auf das Fernmeldegeheimnis verpflichtet. So wurde schon bei der Einführung der öffentlichen Telegrafie in Preußen festgelegt: »Sämtliche Telegrafenbeamte sind zur strengsten Geheimhaltung der telegrafischen Depeschen verpflichtet.«[22]

Diese Geheimhaltungspflicht ist mittlerweile in allen Verfassungen der Welt, aber auch im Vertragswerk der Internationalen Fernmeldeunion enthalten: »Die Mitglieder verpflichten sich, alle nur möglichen Maßnahmen zu treffen, die mit dem verwendeten Fernmeldesystem vereinbar sind, um die Geheimhaltung der Nachrichten im internationalen Verkehr zu gewährleisten.«[23]

Das Grundgesetz regelt dieses Grundrecht in Art. 10 Abs. 1 GG: »Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.« Das Telekommunikationsgesetz konkretisiert dieses Grundrecht. Das Geheimnis umfasst sowohl den Inhalt der Telekommunikation als auch deren Umstände, also etwa Daten über die Beteiligten oder deren Aufenthalt, insbesondere bei der Mobilkommunikation (Lokation). Die Verwertung dieser Daten ist nur zu Telekommunikationszwecken zulässig, es sei denn, ein Gesetz sieht eine anderweitige Verwendung vor. Der Verstoß gegen die Verpflichtungen aus dem Fernmeldegeheimnis ist nach § 206 StGB eine Straftat.

Die wichtigsten gesetzlichen Durchbrechungen des Fernmeldegeheimnisses betreffen die Befugnisse der Sicherheitsbehörden. Ihre materielle Grundlage finden sie in den Abhörvorschriften der Strafprozessordnung (für Staatsanwaltschaft und Polizei), im Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses – G-10-Gesetz – (für die Nachrichtendienste) und im Außenwirtschaftsgesetz für die Zollbehörden.

Die Betreiber von Telekommunikationsanlagen haben technische Einrichtungen zur Umsetzung von gesetzlich vorgesehenen Maßnahmen zur Überwachung auf eigene Kosten zu gestalten und vorzuhalten. Der Kreis der Verpflichteten, die Anforderungen an die Gestaltung der technischen Einrichtun-

gen und an die organisatorische Umsetzung von Überwachungsmaßnahmen sowie das Genehmigungsverfahren sind seit Dezember 2001 in der TKÜV festgelegt.

Neben diesen Vorschriften, die eine Überwachung der Inhalte der Telekommunikation gestatten, sind in strafrechtlichen Verfahren Richter und bei Gefahr im Verzug auch die Staatsanwaltschaft befugt, Auskunft über die Umstände der Telekommunikation zu verlangen, also darüber, wer mit wem wann kommuniziert hat, bei mobiler Kommunikation auch über den Standort des Handys. Diese Befugnis, die bis Ende 2001 im alten Fernmeldeanlagengesetz geregelt war,[24] ist nunmehr auch in die Strafprozessordnung übernommen worden.[25] Das Terrorismusbekämpfungsgesetz hat zusätzliche Befugnisse zur Erhebung von Lokationsdaten sowie zur Ermittlung von Geräte- (IMEI) und Kartennummern (IMSI) von Mobilfunkgeräten für Verfassungsschutz und MAD geschaffen. Der Einsatz so genannter »IMSI-Catcher«, die die Empfangsantenne simulieren und die dorthin gesendeten Signalisierungsdaten mithören, ist damit für die Nachrichtendienste erlaubt. Entsprechende strafprozessuale Befugnisse sollen noch geschaffen werden.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Anbieter von TK-Dienstleistungen sind entsprechend dem allgemeinen Datenschutzrecht grundsätzlich nur zulässig, soweit dies für die geschäftsmäßige Erbringung der Telekommunikationsdienste erforderlich ist. Die Einzelheiten werden in der TDSV geregelt, wobei das TKG selbst die wesentlichen Grundsätze vorgibt. Dies sind vor allem die folgenden:

- Bestandsdaten, Verbindungsdaten und Entgeltdaten dürfen nur verarbeitet werden, wenn dies zur betrieblichen Abwicklung der geschäftsmäßigen Telekommunikationsdienste erforderlich ist. Hierzu gehören auch Verfahren zum Erkennen und Beseitigen von Störungen oder zum Aufklären und Unterbinden von Leistungserschleichungen oder anderer rechtswidriger Inanspruchnahme.
- Mit Einwilligung des Anrufers und bei gleichzeitiger Anonymisierung der Daten des Angerufenen dürfen die Daten zur bedarfsgerechten Gestaltung der Telekommunikationsdienste genutzt werden.
- Auf schriftlichen Antrag des Nutzers dürfen eine Aufstellung von Leistungsmerkmalen gefertigt (Einzelentgeltnachweis) und bei bedrohenden oder belästigenden Anrufen Anschlüsse identifiziert werden (Fangschaltung).

Besondere Aufmerksamkeit widmen TKG und TDSV den Bestandsdaten. Diese dürfen grundsätzlich nur für die Vertragsabwicklung genutzt werden. Für Werbung, Kundenberatung oder Marktforschung ist eine ausdrückliche Einwilligung der Kunden erforderlich. Dies ist eine Umkehrung (opt-in) der allgemeinen datenschutzrechtlichen Widerspruchsklausel (opt-out). Diese Regelung will der ungehemmten Profilbildung bereits auf der Ebene der Bestandsdaten einen Riegel vorschieben. Bestimmte Bestandsdaten dürfen auf Antrag des Kunden in öffentliche gedruckte oder elektronische Verzeichnisse

aufgenommen werden, wobei diesem ein inzwischen auch im BDSG verankertes Auswahlrecht zusteht. Über diese Daten darf auch eine Telefonauskunft erteilt werden, wenn der Kunde nicht widerspricht.

Auch hinsichtlich der Bestandsdaten haben die Sicherheitsbehörden besondere Rechte: Sie sind ihnen im Einzelfall auf Ersuchen zu übermitteln, soweit dies für ihre Aufgabenerfüllung erforderlich ist. Darüber hinaus haben die Anbieter Kundendateien zu führen, in die Name und Anschrift der Inhaber von Rufnummern und Rufnummerkontingenten aufzunehmen sind. Diese Daten sind der Regulierungsbehörde für Post und Telekommunikation durch automatisierte Abrufverfahren zur Verfügung zu stellen, die die Daten ihrerseits an die Sicherheitsbehörden weiterübermittelt. Diese Bestimmung hat ihre Grenze da, wo die Telekommunikationsanbieter gegenüber ihren Kunden besondere Verpflichtungen haben (zum Beispiel Krankenhäuser, Arbeitgeber).

Anbieter von Telekommunikationsdienstleistungen unterliegen erhöhten Anforderungen an die technischen Schutzmaßnahmen. Nach dem Stand der technischen Entwicklung haben die Anbieter angemessene Vorkehrungen zum Schutz von Fernmeldegeheimnis und Datenschutz, zum Schutz gegen unerlaubte Zugriffe, zum Schutz gegen Störungen der Telekommunikationsnetze und zum Schutz gegen äußere Angriffe und Einwirkungen von Katastrophen zu treffen. Die Regulierungsbehörde erstellt hierzu nach Anhörung der beteiligten Kräfte einen Katalog von Sicherheitsanforderungen.

Der Bundesbeauftragte für den Datenschutz ist Kontrollstelle für alle Telekommunikationsdienstleistungsanbieter, obwohl nach der Privatisierung der Telekom diese ausschließlich Privatunternehmen sind und insoweit die Aufsichtsbehörden zuständig wären.

14. Tele-, Medien- und Rundfunkdienste

Das Tele- und Mediendiensterecht gilt für alle Nutzer des Internets, die Inhalte in das Netz einstellen. Jeder Anbieter einer Website muss sich mit diesen Vorschriften vertraut machen, aber auch alle anderen Unternehmen oder Einzelpersonen, die Dienste über die Telekommunikationsnetze anbieten. Von besonderer Bedeutung für Tele- und Mediendienste ist die Transparenz der Angebote für die Nutzer. Die Anbieter sind verpflichtet, im Rahmen des Dienstes eine Reihe von Informationen leicht erkennbar, unmittelbar erreichbar und ständig zur Verfügung zu halten. Hierzu gehören unter anderem Name und Anschrift, Angaben zur elektronischen Kontaktaufnahme, bei zulassungsbedürftigen Aktivitäten auch Angaben zur Aufsichtsbehörde sowie Angaben zu Registern, in die der Anbieter eingetragen ist.

Im Sinne eines effektiven Verbraucherschutzes treffen Anbieter kommerzieller Kommunikation, die der Förderung des Absatzes von Waren und Dienstleistungen oder des Erscheinungsbildes eines Unternehmens dient, zu-

sätzliche Informationspflichten. So muss klar erkennbar sein, dass es sich um solche handelt, und die natürliche oder juristische Person, in deren Auftrag sie erfolgt, muss klar identifizierbar sein. Überdies sind die Angebote zur Verkaufsförderung wie Rabatte, Zugaben und Geschenke sowie Preisausschreiben oder Gewinnspiele unzweideutig zu kennzeichnen.

Der Mediendienste-Staatsvertrag (MDStV) sieht nur die Angabe von Name und Anschrift des Anbieters beziehungsweise des Vertretungsberechtigten vor. Für Angebote, die periodische Druckerzeugnisse vollständig oder teilweise wiedergeben oder in denen Texte in periodischer Folge erscheinen (Online-Zeitungen), kommen zusätzliche Angaben zum presserechtlich Verantwortlichen hinzu.

Vor dem Hintergrund der Verbreitung strafbarer oder sonst rechtswidriger Inhalte sind die Bestimmungen zur Verantwortlichkeit besonders wichtig. Je nach Rolle des Anbieters unterscheiden die Vorschriften mehrere Stufen der Verantwortlichkeit: Für eigene Informationen, die zur Nutzung bereitgehalten werden, sind die Anbieter nach den allgemeinen Gesetzen verantwortlich. Für fremde Informationen, die Diensteanbieter übermitteln oder zu denen sie den Zugang vermitteln, sind diese nicht verantwortlich, sofern sie den Dienst nur ermöglichen, also die Übermittlung nicht veranlassen, den Adressaten der übermittelten Informationen nicht auswählen oder die übermittelten Informationen nicht auswählen oder verändern. Werden fremde Informationen für einen Nutzer gespeichert, besteht diese Privilegierung auch, wenn der Diensteanbieter keine Kenntnis von der rechtswidrigen Handlung oder Information hat beziehungsweise wenn er unverzüglich nach Kenntnisnahme solcher Inhalte tätig geworden ist, um die Information zu entfernen oder den Zugang zu ihr zu sperren. Eine Überwachungs- oder Nachforschungspflicht hinsichtlich rechtswidriger Informationsverbreitung besteht aber nicht.

Der MDStV hat den gleichen Regelungsgehalt, wenn auch die Formulierung noch der einfacheren des ursprünglichen TDG entspricht. Die eigentlichen datenschutzrechtlichen Regelungen finden sich für die Teledienste in einem speziellen Gesetz, dem TDDSG, während sie für die Mediendienste im MDStV und für die Rundfunkdienste in den Rundfunkstaatsvertrag (RdfStV) integriert sind. Die Regelungen folgen der Dreiteilung des TKG, hier als Bestandsdaten, Nutzungsdaten und Abrechnungsdaten bezeichnet.

Bestandsdaten, die der Begründung, inhaltlichen Ausgestaltung oder Änderung eines Vertragsverhältnisses dienen, dürfen nur im hierzu erforderlichen Umfang verarbeitet werden. Jede weitere Verwendung bedarf der Einwilligung der Betroffenen (wie im TKG »opt-in« – im Gegensatz zu »opt-out«, bei dem der Betroffene einer Nutzung seiner Daten widersprechen muss). Lediglich der Rundfunkstaatsvertrag lässt die Verarbeitung von Bestandsdaten für Zwecke der Beratung oder zur bedarfsgerechten Gestaltung technischer Einrichtungen ohne Einwilligung zu, räumt jedoch ein Widerspruchsrecht ein.

Die im internationalen Vergleich datenschutzfreundlichste Regelung betrifft die Verarbeitung von *Nutzungsdaten*. Sie darf nur solange erfolgen, wie

sie für die Inanspruchnahme von Diensten erforderlich ist. Darüber hinausgehende Verarbeitungswünsche der Diensteanbieter bedürfen der ausdrücklichen Einwilligung der Nutzer. Daraus folgt, dass die Erstellung von Nutzungsprofilen aus dem Clickstream nach deutschem Recht nur mit ausdrücklicher Einwilligung der Betroffenen zulässig ist. Bei Verwendung von Pseudonymen dürfen vom Diensteanbieter für eigene Zwecke Nutzungsprofile erstellt werden. Die Nutzer haben hiergegen ein Widerspruchsrecht, auf das sie der Diensteanbieter hinzuweisen hat.

Abrechnungsdaten dürfen über das Ende des Nutzungsvorganges bearbeitet und genutzt werden, soweit dies für die Abrechnung erforderlich ist. Im Gegensatz zum TKG ist keine ausdrückliche Frist für die Speicherungsdauer im Zusammenhang mit der Abrechnung vorgesehen. Das TDDSG enthält jedoch die Regelung, dass zur Erfüllung bestehender gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen, die über das Ende der Abrechnung hinausgehen, der Diensteanbieter die Daten zu sperren hat. Diese Bestimmung ist eine mittelbare Befugnis zur Aufbewahrung der Daten zum Beispiel im Hinblick auf handels- oder steuerrechtliche Vorschriften. Wünscht der Nutzer einen Einzelnachweis über die Inanspruchnahme bestimmter Angebote, dürfen allerdings diese Daten ausdrücklich bis zum Ablauf des sechsten Monats nach Versendung der Rechnung gespeichert werden. Angesichts der derzeit noch bestehenden weitgehenden Kostenfreiheit beziehungsweise Pauschalentgeltung der Tele- und Mediendienste (»Flatrate«) stellen diese Vorschriften allerdings in den weitaus meisten Fällen keine Rechtsgrundlage für die Verarbeitung von Nutzungsdaten dar.

In vielen Fällen, insbesondere wenn die Weiterverarbeitung von Nutzungsdaten nach Ende der Verbindung beispielsweise für Werbezwecke (zum Beispiel individualisierte Bannerwerbung) erwünscht wird, spielt die Einwilligung der Nutzer als Rechtsgrundlage eine sehr wichtige Rolle. Die Neufassung des TDDSG hat die Anforderungen an die elektronische Einwilligung gegenüber der vorherigen Vorschrift deutlich abgesenkt. Nach der alten TDDSG-Fassung hatte der Diensteanbieter sicherzustellen, dass die Einwilligungserklärung nicht unerkennbar verändert und der Urheber erkannt werden konnte (was nur unter Zuhilfenahme einer digitalen Signatur möglich ist). Diese strengen Verpflichtungen sind entfallen. Es reicht nunmehr aus, dass die Einwilligung durch eine eindeutige und bewusste Handlung des Nutzers erfolgt, die Einwilligung protokolliert wird und ihr Inhalt jederzeit vom Nutzer abgerufen werden kann. Im MDStV ist es bislang bei den höheren Anforderungen an die elektronische Einwilligung geblieben.

Die Dienstevorschriften räumen dem Nutzer einen Anspruch auf unentgeltliche und unverzügliche Auskunft über die zu seiner Person oder zu seinem Pseudonym gespeicherten Daten ein. Für die Neuen Medien ist besonders relevant, dass diese Auskunft auf Verlangen des Nutzers auch elektronisch erfolgen kann.

15. Was ist strafbar?

Bis das neue Bundesdatenschutzgesetz (BDSG) in Kraft trat, waren die wesentlichen Verstöße gegen das Gesetz Straftaten. Es handelte sich allerdings um Antragsdelikte, das heißt die Betroffenen mussten einen Strafantrag stellen, was in der Regel daran scheiterte, dass die Betroffenen von rechtswidrigen Handlungen der Datenverarbeiter gar nichts wussten. Insbesondere wenn die Aufsichtsbehörden bei Kontrollen auf Verstöße gegen das BDSG stießen, konnte eine Bestrafung nur erreicht werden, wenn die Betroffenen zu einem Strafantrag gebracht werden konnten. Und dann mussten Gerichte in aufwändigen Verfahren über die Strafbarkeit entscheiden.

Durch das neue BDSG wurden die meisten Verstöße zu Ordnungswidrigkeiten gemacht. Hierzu gehören beispielsweise die unbefugte Erhebung oder Verarbeitung nicht allgemein zugänglicher Daten, die unbefugte Bereithaltung zum Abruf der Daten (zum Beispiel im Internet), aber auch der unbefugte Abruf nicht allgemein zugänglicher Daten (beispielsweise durch Hacker) sowie die Erschleichung von Daten durch unrichtige Angaben (zum Beispiel durch Detekteien). Für Verstöße dieser Art können nun durch die Aufsichtsbehörden von Amts wegen Bußgelder bis zu einer Höhe von 250 000 Euro verhängt werden.

Bereits bisher konnten Verstöße gegen die formellen Bestimmungen des BDSG mit Bußgeld geahndet werden, zum Beispiel wenn kein Datenschutzbeauftragter benannt ist oder Anordnungen der Aufsichtsbehörde nicht nachgekommen wird. Einige neue Bestimmungen kamen hinzu, etwa wenn der Betroffene über die Widerspruchsmöglichkeit bei Werbung nicht informiert wird. Bußgelder können in diesen Fällen bis zu einer Höhe von 25 000 Euro verhängt werden.

Straftaten sind nach wie vor Verstöße gegen eine Reihe von materiellen Regelungen des BDSG, wenn sie gegen Entgelt oder in Bereicherungs- oder Schädigungsabsicht erfolgen. Sie werden nur auf Antrag der Betroffenen, der verantwortlichen Stelle, des Bundesbeauftragten für den Datenschutz oder der Aufsichtsbehörden verfolgt.

Auch mit dem neuen TDG wurden Bußgeldvorschriften eingeführt. Verstöße gegen die allgemeinen Informationspflichten stellen eine Ordnungswidrigkeit dar und können mit einer Geldbuße bis zu 50 000 Euro geahndet werden. Ebenso können bei Verstößen von Telediensteanbietern gegen datenschutzrechtliche Bestimmungen des TDDSG wie zum Beispiel die Verarbeitung oder Nutzung von Daten ohne die notwendige Einwilligung des Betroffenen oder die unzulässige Anfertigung eines Nutzungsprofils Bußgelder verhängt werden.

Einen weitaus ausführlicheren Ordnungswidrigkeitenkatalog enthalten der MDStV und der RdfStV. Die Obergrenzen für Bußgelder liegen im MDStV bei 250 000 Euro, im RdfStV sogar bei 500 000 Euro.

Anmerkungen

1 Empfehlungen des Rates über Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten vom 23. September 1980.
2 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (Konvention Nr. 108).
3 Richtlinien betreffend personenbezogene Daten in automatisierten Dateien vom 14. Dezember 1990.
4 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.
5 Charta der Grundrechte der Europäischen Union, proklamiert in Nizza am 7. Dezember 2000.
6 Privacy Act vom 31. Dezember 1974; Public Law 93-579.
7 Entscheidungen des Bundesverfassungsgerichts (BVerfGE), Band 65, S. 1 ff.
8 Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18. Mai 2001.
9 Alexander Rossnagel/Andreas Pfitzmann/Hansjürgen Garstka, Modernisierung des Datenschutzrechts, Berlin 2001.
10 Samuel D. Warren/Louis D. Brandeis, The Right to Privacy, Harvard Law Review 1890, S. 193 ff.
11 Ebd., S. 198.
12 In Deutschland: Gesetz zur Bekämpfung des internationalen Terrorismus vom 14. Dezember 2001.
13 Vgl. hierzu die Beiträge Goltzsch und Hansen/Krause in diesem Band.
14 Der Zugang zu den Websites der Datenschutzbeauftragten ist am einfachsten über das Virtuelle Datenschutzbüro, http://www.datenschutz.de, möglich.
15 Telekommunikationsgesetz vom 25. Juli 1996.
16 Telekommunikations-Datenschutzverordnung vom 18. Dezember 2000.
17 Teledienstegesetz vom 22. Juli 1997 in der Fassung des EGG (vgl. Anm. 20) vom 9. November 2001.
18 Teledienstedatenschutzgesetz vom 22. Juli 1997 in der Fassung des EGG (vgl. Anm. 20) vom 9. November 2001.
19 Staatsvertrag über Mediendienste vom 20. Januar bis 12. Februar 1997.
20 Rundfunkstaatsvertrag vom 31. August 1991 in der Fassung des Vierten Staatsvertrages zur Änderung rundfunkrechtlicher Staatsverträge vom 16. Juli 1999 bis 24. August 1999.
21 Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr vom 9. November 2001.
22 Preußisches Regulativ über die Benutzung der elektromagnetischen Staatstelegraphen seitens des Publikums vom 6. August 1849.
23 Art. 37 der Konstitution der Internationalen Fernmeldeunion.
24 Gesetz über Fernmeldeanlagen vom 14. Januar 1928, zuletzt neu bekannt gemacht am 3. Juli 1989.
25 Gesetz zur Änderung der Strafprozessordnung vom 20. Dezember 2001, §§ 100 g, 100 h.