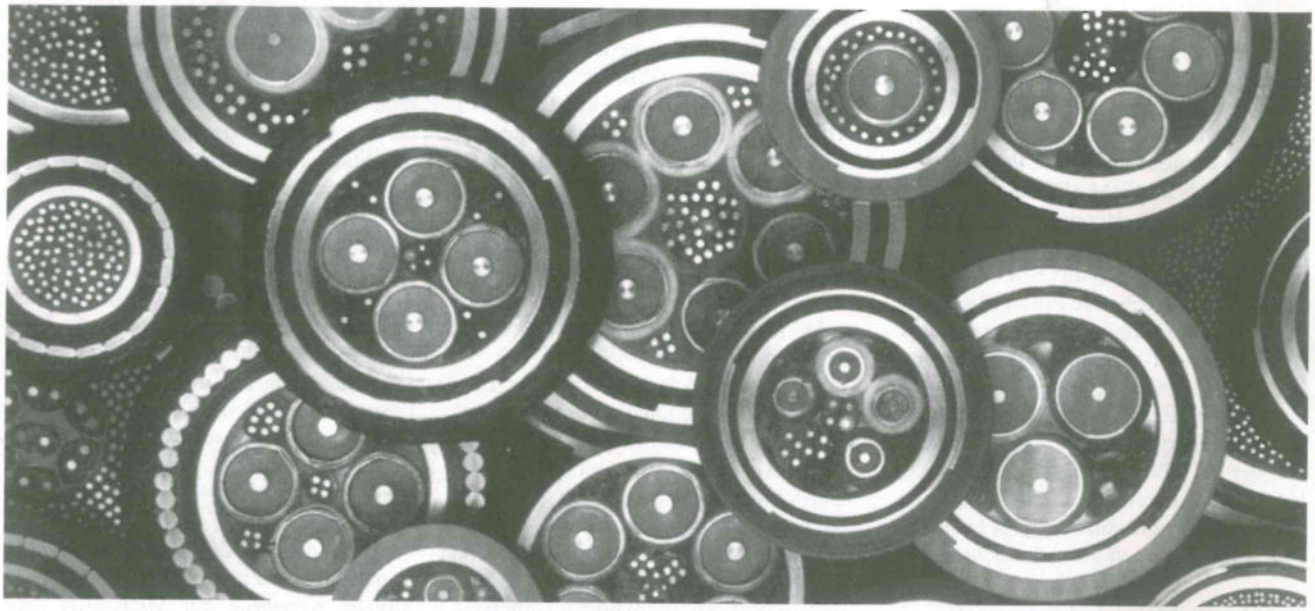

Datenflut und Normenebbe

Datenschutz in der Informationsgesellschaft

Marei Pelzer

Die neuen Informations- und Kommunikationstechnologien haben sich rasant entwickelt. Kann der Datenschutz die riesigen Datenfluten in den Griff bekommen? Die bisherigen Datenschutzreglungen reichen jedenfalls nicht mehr aus. Im Multimedia-Zeitalter sind neue Konzepte zur Datensicherung gefragt.

Während sich also die Mittel des Datenschutzes wandeln müssen, bleibt sein Ziel dasselbe. Nicht die Daten sollen geschützt werden, sondern die Menschen sollen vor nachteiligen Folgen der Datenverarbeitung bewahrt werden.

Im Volkszählungsurteil[1] von 1983 hat das Bundesverfassungsgericht (BVerfG) diesen Schutz mit Verfassungsrang ausgestattet. Aus dem allgemeinen Persönlichkeitsrecht gem. Artikel 2 Absatz 1 i. V. m. Artikel 1 Grundgesetz (GG) ergebe sich das Grundrecht auf „informationelle Selbstbestimmung". Dieses umfasse unter den modernen Bedingungen der Datenverarbeitung den Schutz des einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner Daten. Hieraus folgerte das BVerfG eine strikte Zweckbindung der Datenverarbeitung. Sie darf also nur erfolgen, wenn ein Gesetz das Verarbeitungsziel und den -umfang festlegt. Eine Verarbeitung auf Vorrat ist verfassungswidrig. Zudem stellt das Urteil die Bedeutung des Datenschutzes für die individuelle Selbstbestimmung und die Demokratie heraus. Das Individuum soll Schutz genießen gegen fremdes geheimes Wissen, welches zum Instrument von Manipulation und Erniedrigung werden kann. Als Sozialperson soll es vor der Gefahr geschützt werden, daß fremdes geheimes Wissen ihm den Mut nimmt, auch in der Öffentlichkeit für seine Meinung einzutreten.[2]

Neue Probleme des Datenschutzes

Zu Zeiten des Volkszählungsurteils standen noch die klassischen Gegensätze, BürgerInnenfreiheit und Staatskontrolle, beim Datenschutz im Vordergrund. Heute gehen Datenschutz-Gefahren immer mehr von den neuen Informationstechnologien aus, die die Privatwirtschaft ihren KonsumentInnen anbietet. Die Verwendung der Technologien hinterläßt fast immer Datenspuren, die die BetreiberInnen wirtschaftlich nutzen können. Muß der Datenschutz heute sein Augenmerk auch auf dieses Problemfeld richten, so hat er seine Abwehrfunktion gegen den Staat in keiner Weise verloren. Vielzählige nationale und länderübergreifende Fahndungs- und Überwachungssystem wurden geschaffen. Als Beispiele seien hier die beiden besonders „Großen Brüder" unter den Informationssystemen dargestellt: Schengen und EUROPOL.

Von den derzeitig in Betrieb befindlichen Fahndungsystemen in Europa ist wohl das Schengener Informationssystem (SIS) das einschneidendste. Durch das SIS wurden erstmals die Polizeizentralen der einzelnen EU-Staaten online miteinander verbunden. Als Relaisstation dient ein Zentralrechner in Straßburg. Über ein eigenes Datennetz sind Deutschland, Frankreich, Belgien, die Niederlande, Luxemburg, Portugal und Spanien angebunden. Anfang Mai1995 waren 2,5 Millionen Datensätze eingelesen, sieben bis acht Millionen soll die Gesamtkapazität des SIS ausmachen. Diese Zahlen dürften die Zahl aller wegen schwerer Delikte dringend Tatverdächtigen in ganz Europa um ein Vielfaches übersteigen.[3] Die riesigen Datenmengen des SIS bergen dementsprechend überdimensionale Gefahren für die informationelle Selbstbestimmung. Je umfangreicher eine Datensammlung ist, desto höher ist die Wahrscheinlichkeit, daß mehrere Personen mit dem gleichen Vor- und Familiennamen und anderen Identifizierungsmerkmalen in einer Datei erfaßt sind. Dies kann zu Verwechs-

lungen mit unerträglichen Folgen für die Betroffenen führen. Dabei gründen viele Daten nicht einmal auf einen dringenden Tatverdacht, sondern sind lediglich Verdachtsdaten. Es genügen persönliche Merkmale, die aus Polizeisicht „auffällig" sind, ohne direkt auf strafwürdiges Verhalten schließen zu lassen. Es werden also präventiv Daten gesammelt, was jedoch laut BVerfG verfassungswidrig ist. Außerdem wird das Datennetz gezielt gegen Flüchtlinge aus dem nichteuropäischen Ausland eingesetzt. Die Daten von AusländerInnen, die ausgewiesen oder an der Grenze zurückgewiesen werden sollen, sind online abrufbar.[4] Bei Abschiebungen leisten die Schengen-Staaten sich gegenseitig Amtshilfe. So legt das SIS den Grundstein für die Festung Europa.[5]

Überwachungssyssteme

Ähnliche Auswirkungen wird EUROPOL, das geplante Europäische Polizeiamt in Den Haag, haben. Ende Juli 1996 wurde nun die EUROPOL-Konvention von den EU-Mitgliedstaaten unterzeichnet. EUROPOL wird auf dem Gebiet „besonders schwerer Kriminalität" mit verschiedenen Dateien arbeiten. In einer sog. Basisdatei können nicht nur Strafverdächtige und Verurteilte, sondern auch diejenigen, „bei denen bestimmte Tatsachen die Annahme rechtfertigen, daß sie Straftaten begehen werden", erfaßt werden. In den sog. Analysedateien können mögliche Opfer von Gewalttaten und Personen, die Informationen über betreffende Straftaten liefern, gespeichert werden. Dies führt dazu, daß praktisch jede Person erfaßt werden kann. Die Speicherung setzt weder eine Einwilligung voraus, noch ist eine Betroffenheit, eine richterliche oder staatsanwaltliche Anordnung gefordert.[6]

Durch EUROPOL droht außerdem eine Umgehung des nationalen Datenschutzrechts. Werden unter strengen Voraussetzungen Daten von Länderpolizeien erhoben, so müssen sie diese auch über das Bundeskriminalamt (BKA) an EUROPOL weitergeben. EUROPOL nutzt diese dann für die Aufklärung jeder „schwerwiegenden Form der Kriminalität". Wurde im Einzelfall von der Länderpolizei Verwendungsbeschränkungen mitgeteilt, müssen die Daten nur mit anderen zusammengeführt werden, um daraus neue Daten entstehen zu lassen, die keiner Zweckbeschränkung mehr unterliegen. Weiterhin sind auch Datenübermittlungen an Drittstaaten vorgesehen. Der / die EmpfängerIn muß lediglich zusagen, daß er / sie die Daten nur zu dem Zweck nutzt, zu dem sie übermittelt worden sind. Die fatalen Folgen beispielsweise einer Datenübermittlung an die Türkei über kurdische „TerroristInnen" kann man sich leicht ausmalen.

Nicht weniger problematisch als die staatlichen Überwachungsbestrebungen ist der Umgang der Privatwirtschaft mit den neuen Medien. Die Angebote sind vielfältig: Telearbeit, Teleshopping, Telebanking, Video-on-demand, Internet-Nutzung. Immer mehr Dienstleistungen des alltäglichen Lebens werden nur noch elektronisch interaktiv über die Datenautobahn erreichbar sein. Dies bringt die informationelle Selbstbestimmung ins Wanken. Denn jede Aktivität „über das Netz" hinterläßt eine Datenspur. Durch die Zwischenspeicherung von Inhalten und Verbindungsdaten an jedem Netzknoten läßt sich alles, was unverschlüsselt über offene Netze übermittelt wird, problemlos mithören. Die Anonymität des Barkaufs, beim Fernsehkonsum oder beim Telefonieren wird nicht mehr gewährleistet sein.

Aus den anfallenden Daten können Persönlichkeits- und Nutzungsprofile erstellt werden. Aber Interessen, Kaufwünsche und Vorlieben können nicht nur registriert, sondern unter Umständen auch offengelegt werden. Dies kann besonders bei sensiblen Daten fatal sein, wie sie zum Beispiel bei personenbezogenen medizinischen Online-Diensten entstehen. Daß sich vor allem Online-Dienste ausgesprochen gut zur Profilbildung eignen, liegt daran, daß sie sowohl über bestimmte Grunddaten verfügen, Zugriff auf das Informationsverhalten der Betroffenen haben und diese Angaben mit registrierten Teleshopping-Aktivitäten abgleichen können.[7]

Aus Datenschutz-Sicht ist aber auch der Verkauf von CD-ROMs kritisch zu sehen. Typisches Beispiel für diese Sparte sind Telefonbücher auf CD-ROMs. Im Vergleich zum herkömmlichen Telefonbuch ist an der datenmäßigen Speicherung die vielfach erhöhte Selektionsmöglichkeit äußerst problematisch. Es kann nicht nur nach Nachname oder Stadt sortiert werden, sondern es stehen auch Vorname, Straße, Hausnummer, Branche, Berufsangaben und Telefonnummer zur Verfügung. Die Mißbrauchsgefahr liegt nahe. Es sind qualitativ völlig neue Suchaktionen möglich, die das Persönlichkeitsrecht bedrohen.[8] Außerdem besteht die Möglichkeit, daß sich CD-ROM-Angaben in elektronische Dateien überspielen und mit jeder sonstigen Datenbank kombinieren lassen, wodurch sich umfassende Persönlichkeitsprofile erstellen lassen.

Multimediale Verantwortungslosigkeit

Ob das Individuum mit seinen Daten in der zukünftigen Informationsgesellschaft geschützt werden kann, hängt vor allem von der Entwicklung im Datenschutz ab. Dabei kann auf das geltende Recht aufgebaut werden, wobei weiterführende Konzepte dringend notwendig sind.

Zentrale Regelung des Datenschutzes ist das Bundesdatenschutzgesetz (BDSG). Während das BDSG den behördlichen Bereich des Bundes und das Gebiet der Privatwirtschaft regelt, sind Landesdatenschutzgesetze für den behördlichen Bereich der Länder zuständig. Letztere stimmen weitgehend mit dem BDSG überein. Das BDSG ist nur auf personenbezogene Daten anwendbar, obwohl auch Sachdaten nie völlig losgelöst von personellen Bezügen sind. Sie aus dem Datenschutz auszuklammern, geht also fehl. Kritikwürdig ist auch, daß eine Zweckbindung der Datenerhebung nur für den öffentlichen und nicht für den privaten Bereich vorgeschrieben ist. Das BDSG regelt auch die Betroffenen-Rechte. Betroffene haben ein Auskunftsrecht über ihre Daten. Unrichtige Daten müssen berichtigt werden, unzulässigerweise gespeicherte Daten müssen gesperrt und gelöscht werden. Der oder die Bundesbeauftragte für den Datenschutz soll die Einhaltung des BDSG bei Behörden und sonstigen öffentlichen Stellen kontrollieren. Neben dem allgemeine Datenschutz bestehen bereichsspezifische Schutzgesetze. Für den Bereich der Telekommunikation ist der Bund datenschutzrechtlich zuständig. Die Datenschutzregelungen der Medienangebote fallen in die Zuständigkeit der Länder. Diese traditionelle Abgrenzung der beiden Rechtsgebiete er-

Anmerkungen:
1 BVerfGE 65, 1 ff.
2 Hassemer *DuD* 1996, 195, 198.
3 Leuthardt 1996, 43.
4 Busch, in: Roth (Hrsg.) 1996, 21.
5 Siehe dazu auch Kunzmann *FoR* 1/96, 21.
6 Weichert, in: Roth (Hrsg.) 1996, 26.
7 Schaar *DuD* 3/96, 134, 135.
8 Weichert *RDV* 1995, 202, 203.

scheint unter Multimedia-Voraussetzungen jedoch nicht mehr sinnvoll. Beispielsweise kann man das interaktive Angebot der Fernsehanstalten dem Rundfunkrecht (rundfunkähnliche Dienste), aber auch der individuellen Telekommunikation zuordnen.

Neue Entwicklungen im deutschen Datenschutzrecht werden in nächster Zeit wohl vor allem durch die Harmonisierung des Datenschutzrechts in der Europäischen Union (EU) vorangetrieben werden. Durch die Vereinheitlichung der Datenschutzstandards soll die Abwanderung von Unternehmen in „Datenschutzoasen" verhindert werden und so der grenzüberschreitende freie Wettbewerb unterstützt werden. Der im Juli 1995 verabschiedete EU-Datenschutzrichtlinie[9] steht nun die Umsetzung durch die Mitgliedstaaten bevor, was für einige europäische Länder, z. B. für Italien und Griechenland, die erstmalige Normierung des Datenschutzes bedeutet. Abweichend vom BDSG ist in der EU-Datenschutzrichtlinie keine Trennung zwischen dem öffentlichen und privaten Bereich vorgesehen. Eine unterschiedliche Behandlung der beiden Bereiche durch das deutsche Datenschutzrecht ist schon längst nicht mehr haltbar, da die Privatsphäre durch die auf den Multimedia-Markt drängenden Privaten nicht mehr weniger bedroht wird als durch den Staat. Die für den Datenschutz wichtige Bestimmung des oder der Verantwortlichen wird durch die Richtlinie wesentlich erleichtert. Danach ist verantwortlich, wer über die Zwecke der Verarbeitung entscheidet, z. B. bei E-Mail im Internet der / die AbsenderIn. Hingegen ist der / die NetzwerkbetreiberIn für die Verarbeitung der Zugangsdaten verantwortlich. Weiterhin wird die Pflicht, die Betroffenen über die Datenerhebung, bzw -verarbeitung zu informieren, ausgebaut.

Auch die Betroffenenrechte werden durch die Richtlinie verbessert. Es wird für jedermann / jedefrau ein allgemeines Informationsrecht über das Bestehen von Verarbeitungen, für Betroffene ein qualifiziertes Widerspruchsrecht gegen Verarbeitungen aller Art sowie ein Recht auf Auskunft über den logischen Aufbau der Verarbeitungen, und schließlich für jedermann / jedefrau das Recht, nicht einer Entscheidung unterworfen zu werden, die ausschließlich auf der Grundlage automatisierter Verarbeitungen erfolgt, die eine Bewertung der Persönlichkeit enthalten.

Fazit

Die Vereinheitlichung des Datenschutzes in Europa weist in die richtige Richtung. Da die Online-Nutzung jedoch global ist, müßte ein wirksamer Datenschutz international harmonisiert werden.

Außerdem muß sich ein moderner Datenschutz am Prinzip der Datenvermeidung orientieren: Wo anonyme Zugangs- und Nutzungsformen für Online-Dienste technisch möglich sind, müssen diese auch angeboten werden. Wo Verbindungsdaten technisch zwangsläufig gespeichert werden müssen, muß das Verbot der Herstellung von Nutzungsprofilen sowie die Garantie der Zweckbindung und der umgehenden Löschung gelten.

Gegen den Einsatz von wirksamen Verschlüsselungsprogrammen und anonymen Chipkarten wird oft das Kostenargument vorgebracht. Datenschutzstandards seien gegen den Markt nicht durchsetzbar. Aber gerade das Gegenteil trifft zu. Letztendlich werden nur die Techniken wirtschaftlich erfolgreich sein, die mit wenigen personenbezogenen Daten auskommen. Denn diesen werden die KonsumentInnen den Vorzug geben.

Marei Pelzer studiert Jura in Freiburg.

Anmerkungen:

9 Richtlinie 95/46/Eg v. 24.10.1995, ABI. der EG vom 23. 11. 1995. L 281.

Literatur:

Brühann, Ulf, EU-Datenschutzrichtlinie–Umsetzung in einem versetzten Europa, *Datenschutz und Datensicherheit (DuD)* 2/96, 66.

Garstka, Hansjürgen, „http://www.Datenschutz-berlin.de/", Schriftenreihe „Materialien zum Datenschutz", Zusammenfassung eines Symposiums „Multimedia und Datenschutz", Gesetzestexte zum Thema Datenschutz im Internet.

Hack, Sophie, „Haben Sie Ihre Karte dabei?" in: *Forum Recht (FoR)* 2/96, 57.

Hassemer, Winfried / Möller, Klaus Peter, 25 Jahre Datenschutz, 1996.

Hassemer, Winfried, Über die Zukunft des Datenschutzes, in: *DuD* 1996, 195.

Kunzmann, Tobias, Datenschutz-auch für AusländerInnen?, in: *FoR* 1/96, 21f.

Leuthardt, Beat, Leben online, 1996.

Pfeiffer, Christian, Telefongespräche im Visier der elektronischen Rasterfahndung, in: *Zeitschrift für Rechtspolitik (ZRP)* 1994, 253.

Roth, Claudia (Hrsg.), Mit EUROPOL grenzelnlos sicher?, Hearing zu Europol (Bezug über: Bündnis 90/Die Grünen, Versand, Heerstr. 172, D-53111 Bonn).

Schaar, Peter, Datenschutzrechtliche Probleme von Online-Diensten, in: *DuD* 1996, 134.

Weichert, Thilo, Personenbezogene Daten auf CD-ROM, in: *Recht der Datenverarbeitung (RDV)* 1995, 202.

Weichert, Thilo, EUROPOL-Konvention und Datenschutz, in: *DuD* 1995, 450.