Bettina Sokol (Hrsg.)

Neue Instrumente im Datenschutz

Düsseldorf 1999

Herausgeberin:

Die Landesbeauftragte
für den Datenschutz
Nordrhein-Westfalen
Bettina Sokol
Reichsstraße 43

40217 Düsseldorf

Tel.: 0211/38424-0
Fax: 0211/3842410
E-mail: datenschutz@mail.lfd.nrw.de

Diese Broschüre kann unter www.lfd.nrw.de oder
www.nordrhein-westfalen.datenschutz.de abgerufen werden.

ISSN: 0179-2431
Druck: Klüsener-Druck, Wuppertal

Gedruckt auf chlorfrei gebleichtem Recyclingpapier

Vorwort

Die Professoren Dr. Thomas Hoeren und Dr. Bernd Holznagel, LL.M. vom Institut für Informations-, Telekommunikations- und Medienrecht der Westfälischen Wilhelms-Universität Münster und ich als Landesbeauftragte für den Datenschutz haben am 28. November 1998 gemeinsam das Symposium "Neue Instrumente im Datenschutz" veranstaltet. Mit dem vorliegenden Band werden die dort gehaltenen Vorträge dokumentiert. Die Vortragstexte sind zum Teil um Fußnoten ergänzt.

Das Symposium hätte in dieser Form nicht stattfinden können, ohne die freundliche Unterstützung der DaimlerChrysler AG, für die an dieser Stelle nochmals gedankt sei. Ebenfalls ist den Mitarbeiterinnen und Mitarbeitern sowohl des Instituts als auch meiner Dienststelle, die die Veranstaltungsorganisation und die Erstellung des Dokumentationsbandes in die Hand genommen haben, ein herzlicher Dank auszusprechen.

Düsseldorf 1999 *Bettina Sokol*

Inhaltsverzeichnis

Begrüßung

Peter Schüren

Meine sehr verehrten Damen und Herren, als Dekan der rechtswissenschaftlichen Fakultät dieser Universität habe ich die Ehre und Freude, Sie heute zum Symposium "Neue Instrumente im Datenschutz" zu begrüßen. Dieses Symposium wird von der Beauftragten für den Datenschutz unseres Bundeslandes und vom Institut für Informations-, Telekommunikations- und Medienrecht unserer Universität getragen. Dieses Institut, das die Veranstaltung mitträgt und das von Herrn Kollegen Holznagel und Herrn Kollegen Hoeren geleitet wird, manifestiert, daß sich unsere Fakultät den Entwicklungen der Rechtswissenschaft auf diesem Feld nicht nur geöffnet hat, sondern daß unsere Fakultät an der Gestaltung dieser Entwicklungen teilhaben will. Erlauben Sie mir aber eine Bemerkung zum Thema selbst: Der Datenschutz hat in meinem Fach, dem Arbeitsrecht, derzeit eine geringere Konjunktur als noch vor einigen Jahren. Vor einigen Jahren begegnete man den vorgetragenen Möglichkeiten und Gefahren der elektronischen Datenverarbeitung mit dem einer unverständlichen, jedenfalls aber unverstandenen Novität gebührenden Schrecken. Es gab Phantasien der vollkommenen Überwachung, vor denen die Arbeitnehmer bewahrt werden sollten. In der Folge erreichten die Betriebsräte ein umfassendes Mitbestimmungsrecht über den § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz bei allen Fragen der Personaldatenverarbeitung. Inzwischen ist die elektronische Datenverarbeitung Betriebsmittel nahezu aller ernsthaften markttätigen Unternehmen. Heute geht es eher darum, daß die Betriebsräte umfassenderen Netzzugang fordern und erhalten. Daten-, also Informationsverarbeitung in vernetzten Systemen ist Alltag. Damit reduziert sich der

Moment des Schreckens, der Beängstigung vor dem unverständlichen, unvertrauten Medium. 1984 ist 14 Jahre vorbei - übrigens ein wirklich gutes, wenig gelesenes Buch. Der Datenschutz heute kann mit mehr Realismus betrieben werden. Auseinandersetzungen wie im Vorfeld des berühmten Volkszählungsurteils sind nicht mehr zu erwarten. Uns interessiert eher, wie wir Daten vor wirtschaftlich gewichtigem Mißbrauch schützen. Genug davon, als Laie muß ich mich hierzu zurückhalten. Ich wünsche Ihrem Symposium, daß es im Geiste einer solchen realistischen Betrachtung und auf hohem Niveau an die Themen herangeht. Ich wünsche Ihnen allen gute Vorträge und spannende Diskussionen.

Eröffnung

Bettina Sokol

Meine sehr verehrten Damen und Herren, auch ich freue mich, Sie ganz herzlich bei unserem heutigen Symposium begrüßen zu können. Nach den freundlichen Worten unseres Gastgebers möchte ich mich mit meiner Eröffnung und den organisatorischen Hinweisen kurz fassen, um möglichst bald unserem ersten Referenten das Wort geben zu können.

Der Datenschutz steht vor enormen Herausforderungen. Insbesondere der technischen Entwicklung, aber auch anderen Veränderungen der tatsächlichen Situation ist unser Datenschutzrecht mittlerweile kaum noch gewachsen. Die Datenschutzbeauftragten fordern schon seit geraumer Zeit, die notwendige Umsetzung der Europäischen Datenschutzrichtlinie in nationales Recht zum Anlaß dafür zu nehmen, das Datenschutzrecht von Bund und Ländern umfassend zu modernisieren. Stichworte sind dabei insbesondere die Stärkung der Rechte der Bürgerinnen und Bürger hinsichtlich ihrer Informations- und Auskunftsrechte sowie ihrer Wahlmöglichkeiten. Es geht um den Grundsatz der Datenvermeidung, um die Forderung, Datenschutz auch und gerade durch Technik zu realisieren und außerdem darum, an dem Grundsatz der Zweckbindung - sowie es auch die Richtlinie vorschreibt - nach wie vor festzuhalten. Weitestgehend einheitliche Anforderungen des Datenschutzniveaus im öffentlichen wie im nicht-öffentlichen Bereich gilt es ebenso zu realisieren wie eine Aufsicht im nicht-öffentlichen Bereich, die aus dem Ministerialstrang ausgegliedert ist und insofern der Richtlinie entsprechend ihre

Tätigkeit tatsächlich in völliger Unabhängigkeit weisungsfrei wird ausüben können.

Auch der Deutsche Juristentag 1998 hat sich in seinen Beschlüssen für eine Neuorientierung des Datenschutzes ausgesprochen. Ideen und Vorschläge für einen neuen Datenschutz stehen zur Diskussion. Mit unserem Symposium möchten wir versuchen, einen Beitrag zu dieser Diskussion zu leisten, und wollen uns heute einigen Überlegungen, Elementen und neuen Instrumenten im Datenschutz widmen.

Die Erosion des Datenschutzes

- Von der Abstumpfung der alten Regelungen und den Schwierigkeiten, neue Instrumente zu entwickeln -

Spiros Simitis

I. Stand

"Was für eine Privatheit", meinte Umberto Eco im August 1998, "soll eigentlich noch verteidigt werden, wenn niemand mehr daran interessiert ist, daß sie verteidigt wird?" Zugegeben: eine zumindest auf den ersten Blick befremdliche, ja geradezu schockierende Frage. Fast ein Vierteljahrhundert nach den ersten, tastenden Versuchen des Hessischen Gesetzgebers, nahezu siebzehn Jahre nachdem das Bundesverfassungsgericht im Volkszählungsurteil jeden Zweifel am Verfassungsrang der informationellen Selbstbestimmung unmißverständlich zurückgewiesen hat und im vierten Jahr der durch die Richtlinie zum Schutz personenbezogener Daten illustrierten und besiegelten Europäisierung des Datenschutzes scheint schließlich alles für eine stete Konsolidierung und nichts für den Zerfall des Datenschutzes zu sprechen. Und doch hat Eco recht, nicht nur gerade jetzt, sondern überhaupt so vehement Zweifel anzumelden. Mindestens vier Gründe lassen sich dafür anführen:

1. Proliferation

Die Datenschutzgesetze haben, was zuweilen vergessen wird, von Anfang an ein doppeltes Ziel verfolgt. Sie wollten die Verarbeitung

personenbezogener Angaben keineswegs nur in geregelte, gesetzlich festgeschriebene Bahnen überführen, vielmehr ihr zunächst und vor allem Einhalt gebieten. Schon der Hessische Landtag hatte den primären Interventionszweck klar angesprochen, das Bundesverfassungsgericht hat ihn später noch deutlicher formuliert: Der Zugriff auf personenbezogene Daten bleibt solange versperrt wie die benötigte Information auch anders erlangt werden kann. Die Anonymität der Information ist, so gesehen, die Regel, ihre Personalisierung die Ausnahme. Verarbeitende Stellen unterliegen folglich einem zweifachen Begründungszwang. Reflexionen über Art und Umfang der zu verwendenden personenbezogenen Daten dürfen erst angestellt werden, wenn alternative Informationswege ausscheiden.

Doch genau diese Abfolge ist durch die anscheinend ebenso einleuchtende wie einprägsame Formel vom Verbot mit Erlaubnisvorbehalt vernebelt und unterlaufen worden. Sie hat sich zum Einfallstor einer Interpretation entwickelt, die sich fast ausschließlich auf eine mögliche Subsumtion unter die gesetzlich tolerierten Verarbeitungskonstellationen konzentriert, darüber aber die gesetzlich genauso geforderte Priorität entpersonalisierter Informationen aus dem Blickfeld nimmt. Die Datenschutzgesetze haben sich damit mehr und mehr in bloße Legitimationsinstrumente verwandelt, die nur dazu dienen, den Umgang mit personenbezogenen Daten zu ordnen, statt ihn auch und gerade in Frage zu stellen.

So konnte die Verarbeitung fast unbemerkt und ganz im Schatten der Gesetze von Höhepunkt zu Höhepunkt einer schier unaufhaltsamen Expansion eilen. Der Wandel der Technologie markiert deren Etappen. Den Anfang machten jene, Ende der sechziger und Anfang der siebziger Jahre eingerichteten "Datenzentralen", Symbol und Verkörperung der aufkommenden Computerisierung in einem. Den Zitadellen des Mittelalters gleich wurden Bund und Länder mit Megaspeichern überzogen, in denen sich schließlich sämtliche, die Bürgerinnen und Bürger betreffenden Daten wiederfinden sollten, um nicht zuletzt eine schnelle und reibungslose Gewährung der unterschiedlichsten Leistungen ebenso wie deren langfristige Planung sicherzustellen, die, so dachte man, allein der prospektiven Kosten willen, eigentlich nur vom Staat und allenfalls noch von einigen wenigen Großunternehmen aufgebaut werden könnten.

Keine zehn Jahre später verschob sich der Schwerpunkt vom Mega- auf den Microcomputer. Die Verarbeitung dezentralisierte sich, büßte jedoch zugleich ihre Exklusivität ein. Das vermeintliche Monopol des Staates und der Großunternehmen war endgültig gebrochen. Mittlere und kleinere Firmen profitierten davon genauso wie die öffentliche Verwaltung. Kunden-, Lieferanten- und Arbeitnehmerdaten konnten auf einmal ganz anders "erfaßt", übermittelt und in immer neuen Kombinationen zusammengestellt werden. Angaben von Antragstellern ließen sich sehr viel leichter überprüfen, potentielle Kaufinteressenten weitaus präziser festhalten und gezielter als bisher ansprechen, ein regulärer Informationsaustausch zur Abwehr gemeinsamer Risiken ungleich schneller und erfolgreicher durchführen. Der tragbare Personal-Computer der Außendienstmitarbeiter registrierte die Schadensquellen der je spezifischen Produkte, sorgte für eine rechtzeitige Bestellung von Ersatzteilen, hielt Arbeitszeit und Leistung der jeweiligen Mitarbeiter fest. Computergestützte Auswahllisten bei betriebsbedingten Kündigungen schirmten den Arbeitgeber gegen den Vorwurf der Einseitigkeit ab und begannen eine zunehmend wichtigere Rolle in Kündigungsschutzprozessen zu spielen. Mit den Laptops und Notebooks zog schließlich der Computer endgültig in den Alltag ein, wurde zu jedermanns Verarbeitungsinstrument.

Und wieder ließ der nächste qualitative und quantitative Sprung nicht lange auf sich warten. Diesmal waren es die Chipkarten, die den Wandel signalisierten. Ihre integrierten, fast beliebig ausbaufähigen Nanospeicher lösten einen ständig anschwellenden Informationsstrom aus. Vom stetig wachsenden Angebot an "intelligenten" Kreditkarten, über die zur selbstverständlichen Voraussetzung aller Arzt- und Apothekenbesuche avancierten Versichertenkarte bis hin zu der zum Mustermerkmal einer "Informationsgesellschaft" erklärten "Bürgerkarte", überall bahnen Chipkarten den Weg, um noch mehr und noch detailliertere Informationen über praktisch jeden Lebensaspekt der Kartennutzer zu sammeln. Vordergründig mögen zudem Kreditkarten nur ein zusätzliches Zahlungsmittel sein und auch Versicherungskarten lediglich eine Abrechnungsfunktion haben. In beiden Fällen zeigt sich freilich deutlicher denn je, daß die Verarbeitung keineswegs auf einzelne Personengruppen zugeschnitten oder bestimmten ebenfalls begrenzten Anlässen vorbehalten ist. Kreditkarten sind vielmehr universelle Zahlungsmittel und Versi-

chertenkarten genauso universell angelegt. Mit beiden universalisiert sich daher die Verarbeitung. Niemand bleibt letztlich ausgespart und alle tragen mit jeder neuen Verwendung ihrer Karten dazu dabei, mehr über sie zu wissen und ihr Profil schärfer zeichnen zu können.

Mit den Chipkarten rückt schließlich der nicht-öffentliche Bereich definitiv in den Mittelpunkt der Verarbeitung. Die Vision restlos "verdateter" und exakt "numerierter" Bürger hat zwar immer realere Züge angenommen, nur sind die privaten Unternehmen in die Rolle gewechselt, die einst den Behörden reserviert zu sein schien. Sie und nicht die öffentlichen Stellen sind es also, die vornehmlich registrieren und katalogisieren. In dem Maße freilich, in dem sich der Akzent auf die Datenbestände der privaten Unternehmen verschiebt, verwischen sich auch die Grenzen zwischen öffentlichen und nicht-öffentlichen Datensammlungen. Noch genauer: Die privaten Sammlungen verwandeln sich mehr und mehr in Informationsmittel, dem die öffentlichen Stellen eine mindestens genauso große Bedeutung beimessen. Steuererklärungen lassen sich nun einmal gerade mit Hilfe der über die Kreditkarten vermittelten und präzise aufgezeichneten Angaben vorzüglich überprüfen. Staatsanwaltschaft und Polizei können zudem mit eben diesen Daten Bewegungsbilder aufzeichnen, einen Verdacht erhärten oder gesuchte Personen ausfindig machen. Ähnlich ist die Lage bei Daten, die im Rahmen der Benutzung von Versichertenkarten anfallen. Nicht von ungefähr hat sich gerade die Bundesrepublik bei den Beratungen des Rates über die Europäische Datenschutzrichtlinie nachdrücklich für das Recht der Mitgliedstaaten eingesetzt, das angeblich so fundamentale Verbot, "sensitive" Daten zu verarbeiten (Art. 8 Abs. 1), jedenfalls dann zu durchbrechen, wenn es um die "Sicherung der Qualität und Wirtschaftlichkeit" von Verfahren geht, die dazu dienen, die Abrechnung von Leistungen in den sozialen Krankenversicherungssystemen zu überprüfen (Erwägungsgrund Nr. 34). Einen besseren Ansatz zu einer kontinuierlichen Kontrolle der Verhaltensweisen von Ärzten und Patienten sowie zur gezielten Revision genereller und individueller Maßnahmen gibt es in der Tat wohl kaum.

Internet beschleunigte und radikalisierte noch einmal den Wandel. Wo sich das "Netz der Netze" etabliert, globalisiert sich die Kommunikation. Räumliche und zeitliche Grenzen verkümmern. Doch die grenzenlose Kommunikation entgrenzt auch die Verarbeitung im

wahrsten Sinne des Wortes. Wer immer sich einklinkt, zahlt einen hohen Preis: Jede, aber auch wirklich jede Bewegung wird festgehalten. Dem virtuellen Kaufhaus gelingt so, was dem realen, trotz aller Anstrengungen, versagt geblieben ist: Es kennt nur gläserne Kunden. Je breiter sich überdies die Angebotspalette gestaltet, von den unterschiedlichsten Foren bis hin zu den immerfort wachsenden Dienstleistungs- und Warenangeboten, desto weniger läßt sich auf Navigationshilfen verzichten. Die Lotsen sind jedoch zumeist "Doppelagenten". Sie geleiten durchs Netz, melden aber zugleich denjenigen, von denen sie zur Verfügung gestellt werden, jeden Schritt der Surfer zurück. Und noch etwas: Internet vollendet jene schon von den Chipkarten forcierte Universalisierung der Verarbeitung. Weil das "Netz der Netze" ein dezidiert universales Kommunikationsmittel ist, das seiner ganzen Intention nach allen, die es nur möchten, offensteht, werden auch alle, die es nutzen, registriert. Auf den Beruf oder die soziale Stellung kommt es, so gesehen, ebensowenig an wie auf das Alter oder das Geschlecht. So gleichgültig allerdings jedes dieser Merkmale beim Zugang ist, so relevant sind sie, sobald die Spurenauswertung ansteht.

Kurzum, nie zuvor wurden derart viele und dermaßen verschiedene Daten für so unterschiedliche Zwecke verarbeitet. Formulierungen wie "Datamining" tauchen eben nicht zufällig auf. Ähnlich den Baggern in den Bergwerken treiben die Computer Stollen durch die Datenvorkommen auf der Suche nach bislang ungeahnten Verwertungsmöglichkeiten. Und wie in den Frühzeiten des "Goldfiebers" drängen sich immer neue "Mineneigentümer" auf den "Datenmarkt", stecken die "Datenbesitzer" ihren jeweiligen "Besitz" sorgfältig ab und versuchen, möglichst schnell möglichst viele weitere "Lagerstätten" aufzuspüren. Kein Wunder, wenn sich deshalb die Zahl der "Datawarehouses" in den letzten fünf Jahren verzehnfacht hat und mittlerweile bei über tausend liegt. Kein Wunder aber auch, daß es, wie allein das Beispiel von "Axciom" zeigt, fast keine Information mehr gibt, die nicht abgerufen werden kann. Ganz gleich, ob es darum geht, wer Katzen, Hunde oder Papageien hat, in einer gemieteten Dreizimmerwohnung oder in einem Eigenheim lebt, in Fast-Food- oder Drei-Sterne-Lokalen ißt, meistens mit der Bahn fährt oder überwiegend fliegt, Hemden, Schuhe oder Anzüge einer bestimmten Marke trägt, Western- oder Pornovideos ausleiht, die Bibel oder Groschenromane liest, allein oder mit Begleitung den Urlaub ver-

bringt, unter siebzig oder über hundert Kilo wiegt, hetero- oder homosexuell liiert ist, die Antwort erfolgt schnell, präzise und mit allen jeweils gewünschten Zusatzinformationen versehen. Ebensowenig überrascht es allerdings, daß sich unter diesen Umständen die Aufmerksamkeit mehr denn je darauf richtet, die Daten zu sieben, um sie auf jene Angaben zu reduzieren, die sich am ehesten dazu eignen, die direkt angesteuerten Betroffenen möglichst von der Unentbehrlichkeit der jeweiligen Offerte zu überzeugen. Mit den Worten des "Playboy": "We want to send customers the right message at the right time."

2. Routinisierung

Mit der Proliferation der Verarbeitung entwickelt sich der Zugriff auf personenbezogene Daten mehr und mehr zur Routine. Nur: Anders als es die massierten Hinweise auf den "numerierten Bürger" und erst recht die nicht minder häufigen Anspielungen auf "1984" suggerierten, wird die Verarbeitung den Betroffenen nicht aufgedrängt, sondern in einer immer größeren Anzahl von Fällen willentlich und wissentlich von ihnen ausgelöst. Indem sie sich dafür entscheiden, etwa Kreditkarten zu benutzen oder sich ins Internet einzuschalten, setzen sie selbst, um ihrer eigenen, je spezifischen Ziele willen jenen Prozeß in Gang, der dazu führt, ihre Daten zusammenzutragen und in Bausteine eines jederzeit abrufbaren Profils zu verwandeln.

Die "transparente Gesellschaft" ist, so gesehen, jedenfalls zu weiten und entscheidenden Teilen, das Produkt der für sie typischen Informations- und Kommunikationsmittel. Die Routinisierung der Verarbeitung ist folglich kein beliebig abstellbarer Vorgang, vielmehr inhärentes Merkmal einer Gesellschaft, in der sich individuelle Aktivitäten in einem generell akzeptierten und Tag für Tag sanktionierten technisch-organisatorischen Rahmen abspielen, der Personalisierung institutionalisiert und Anonymität verdrängt. Das strukturelle Dilemma der "Informationsgesellschaft" kommt damit deutlich zum Ausdruck. Einerseits maximiert just jene Technologie, die den einzelnen in die Lage versetzt, seine Informations- und Kommunikationschancen auf eine neue und bessere Grundlage zu stellen, seine Manipulierbarkeit und Verletzlichkeit. Andererseits legt eine Gesellschaft, die es, gerade wegen der unbestreitbaren Vorteile dieser

Technologie, als ihr ebenso selbstverständliches wie vordringliches Ziel ansieht, jede nur denkbare Zugangsbarriere, so schnell wie es nur geht, abzubauen und es deshalb als eine ihrer wichtigsten bildungspolitischen Aufgaben betrachtet, Jugendlichen so kurzfristig wie möglich die Fähigkeit zu vermitteln, mit dieser umzugehen, damit auch die Korrekturgrenzen fest. Korrekturen, die dazu führen könnten, die eigentliche Gefahrenquelle, also die Technologie selbst, in Frage zu stellen, scheiden von Anfang an aus.

3. Steigerung der Zugriffstiefe

Die Verarbeitung war lange Zeit weitgehend auf Daten beschränkt, die immer nur eine ganz bestimmte Information vermitttelten. Name, Adresse, Beruf, Ausbildung, Einkommen sind typische Beispiele dafür. Die Bedeutung der Information mag je nach dem Verwendungskontext oder in Verbindung mit zusätzlichen Daten variieren, ihr Inhalt bleibt trotzdem gleich. In dem Maße jedoch, in dem die Biotechnologie sich konsolidierte und expandierte, wurden Angaben in die Verarbeitung einbezogen, die ungleich mehr Informationen enthalten. Genetische Daten sind das Musterbeispiel dafür. Sie sind der Schlüssel zur genetischen Konstitution des einzelnen und erlauben es daher nicht nur, ihn so verläßlich wie noch nie zu identifizieren, sondern ermöglichen es ebenso, die für ihn typischen genetischen Defizite und Risiken auszumachen. Mit jeder Lücke freilich, die aus der in weltweiter Kooperation zusammengesetzten genetischen Charta verschwindet, tritt auch die Ambivalenz dieser bislang wohl einmaligen Kombination von Diagnose und Prognose und damit jeder Verarbeitung genetischer Daten noch deutlicher zutage. Sie ist Erkenntnis- und Steuerungsmittel in einem.

Beides ist sicherlich früh genug angesprochen worden. Doch die Steuerungsfunktion geriet, jedenfalls soweit es um die möglichen Gefährdungen der Betroffenen geht, zunehmend aus dem Blick. Von den Vorteilen, die eine Verarbeitung genetischer Daten auch und gerade für den einzelnen mit sich bringt, war dafür um so mehr die Rede. Tatverdächtige könnten zum ersten Mal ihre Unschuld wirklich einwandfrei beweisen, zu Unrecht in Anspruch genommene "Väter" sich besser denn je gegen unberechtigte Unterhaltszahlungen wehren, Beschäftigte gezielt und rechtzeitig vor dem Umgang mit

bestimmten, für sie schädlichen Substanzen bewahrt, potentielle Krankheitsursachen entschieden früher offengelegt und weitaus erfolgreicher bekämpft werden. Kaum verwunderlich, daß etwa der Bundesbeauftragte für den Datenschutz seine Bedenken gegen den "genetischen Fingerabdruck" im Interesse der Betroffenen zurückstellte. Ebensowenig überrascht es, daß Rat und Kommission, nicht zuletzt mit Rücksicht auf die Vorteile für die Betroffenen, ausdrücklich darauf verzichtet haben, die genetischen Daten in die Liste jener in Art. 8 Abs. 1 der EG-Datenschutzrichtlinie ausdrücklich aufgezählten Angaben aufzunehmen, deren Verwendung grundsätzlich untersagt ist. Die Verarbeitung genetischer Daten wurde damit im Ergebnis weitgehend freigegeben. Art. 8 kann nur noch über eine Subsumtion der genetischen Angaben unter die Gesundheitsdaten zum Zuge kommen und auch dann lediglich, soweit gesundheitsspezifische Aspekte zur Debatte stehen. Wohlgemerkt, bei den ständig wiederkehrenden Hinweisen auf ausgeprägt individuelle Interessen an der Verwendung genetischer Daten ist es keineswegs geblieben. Im Gegenteil, in der Argumentation für eine Verarbeitung wurden von Anfang an individuelle und öffentliche Belange gezielt miteinander verknüpft. Neben dem Nutzen für die Betroffenen wurden deshalb vor allem die Aufklärung und Prävention von Straftaten, die Verbesserung des generellen Gesundheitszustandes sowie die Senkung der Krankheits- und Pflegekosten mindestens genauso nachdrücklich betont, um das öffentliche Interesse an einer breit angelegten, kontinuierlich ausgebauten Erhebung genetischer Daten zu illustrieren.

Die Folgen ließen nicht lange auf sich warten. Die eine Zeit lang noch kritisch betrachteten "genetischen Fingerabdrücke" entwickelten sich schnell zur Grundlage eigens aufgebauter "genetischer Datenbanken" sowie zum Ansatzpunkt systematisch praktizierter "genetischer Rasterfahndungen" und die zunächst nur unter repressiven Gesichtspunkten angelegte Verwendung wurde durch immer konkretere Pläne für eine präventive Verarbeitung genetischer Daten ergänzt. Mindestens ebenso signifikant sind unternehmerische Aktivitäten, wie etwa die Operationen der isländischen Firma "Decode Genetics". Sie verfolgt zwei durchaus verschiedene, allerdings eng zusammenhängende Ziele. Das Unternehmen will nicht nur ein unter Forschungsgesichtspunkten in seiner, allein schon wegen der langen Isolation Islands, Kontinuität und Geschlossenheit einmaliges "gene-

tisches Material" sichern und verarbeiten, sondern zugleich die Forschungsergebnisse nutzen, um die Auswirkungen genetischer Defekte durch neue medizinische Präparate aufzufangen oder zumindest abzumildern. "Decode Genetics" möchte deshalb die genetischen Daten aller Isländer registrieren sowie die seit 1915 geführten umfassenden Krankheitsregister auswerten und ist zugleich eine enge Kooperation mit dem schweizerischen pharmazeutischen Unternehmen Hoffmann-La Roche eingegangen. Weder das Forschungs- noch das konkrete Auswertungsziel lassen sich allerdings nach Meinung des Unternehmens ohne ein Verarbeitungsmonopol und die damit verbundene Möglichkeit erreichen, Hoffmann-La Roche sowie einer Reihe weiterer Unternehmen, zu denen auch Versicherungsgesellschaften zählen, eine exklusive Verwertung der Forschungsergebnisse für ihre je spezifischen Zwecke zu garantieren. Die isländische Regierung reagierte durchaus positiv. Die angestrebte Verarbeitung und Verwertung der genetischen Daten bietet in ihren Augen einem Land, das über kaum andere Ressourcen verfügt, singuläre Chancen. Das isländische Parlament hat sich diesem Standpunkt weitgehend angeschlossen und ihn durch ein Ende 1998 verabschiedetes Gesetz bekräftigt.

Die Grundlage für ähnliche, sich bereits abzeichnende Projekte ist damit gelegt. Am schon deutlich erkennbaren Ende eines sorgfältig geplanten Weges stehen überall Datenbanken, die über ein in dieser Präzision bislang nie gebotenes Abbild ganzer Populationen verfügen. Sie wecken immer größere Erwartungen privater und öffentlicher Verarbeitungsinteressenten und drängen sich fast von selbst für eine Vielzahl von Verwendungen auf, die den Kreis der anfänglich verfolgten Verarbeitungsabsichten bei weitem überschreiten. Die Plausibilität der ursprünglichen, gleichsam eindimensionalen Verarbeitungszwecke versperrt freilich den Blick für die in der Erhebung und Konzentration genetischer Daten angelegte Mehrdimensionalität späterer Verwendungen. Datenschutz ist aber unverändert auch und gerade dezidierte Abwehr einer multifunktionalen Nutzung personenbezogener Angaben. Genau diese Gefahr vervielfacht sich durch die Verarbeitung genetischer Daten. Wo die Anzahl der Interessenten so sprunghaft ansteigt und sich ihre Erwartungen so ausfächern, nehmen nicht nur Diskriminierungen der Betroffenen schlagartig zu. Vielmehr weiten sich vor allem die zunehmend invasiveren Eingriffe in die Möglichkeiten der einzelnen aus, ihre Lebenswelt selbst zu

gestalten. Gemeint sind etwa die sich häufenden, unter anderem in der 1996 vorgelegten Studie der Universitäten Harvard und Stanford dokumentierten Fälle, in denen Arbeits- und Versicherungsverträge mit Rücksicht auf die genetischen Daten der Betroffenen entweder gekündigt oder gar nicht erst abgeschlossen wurden. Gemeint sind aber auch die vielfachen, sich ständig intensivierenden Bemühungen, die pränatale Diagnostik für eine auf ganz spezifische Eigenschaften bedachte Familienplanung zu verwenden, ebenso wie die mehr oder weniger offene Aufkündigung des "Paktes" der Molekularbiologen "zur Selbstbeschränkung", unter anderem im Zusammenhang mit den Auseinandersetzungen über die "met-machine" des Massachussets Institute of Technology, und die kaum verhüllten, besonders im Rahmen der "Soziogenetik" verfochtenen Projekte, Interventionen in die genetischen Daten als gesellschaftliches Korrektiv zu nutzen. Alles in allem, mit der Verarbeitung genetischer Daten erhöht sich die Verletzlichkeit des einzelnen, aber auch der Gesellschaft noch einmal beträchtlich. Soziale Exklusion und Manipulierbarkeit nehmen deutlicher denn je reale Züge an.

4. Kapitalisierung und Kommerzialisierung

Proliferation und Routinisierung wirken sich auch auf die Einschätzung personenbezogener Daten aus. Waren sie ursprünglich, in der Regel jedenfalls, nur Mittel, um im Einklang mit den Datenschutzgesetzen, bestimmte, konkret anzugebende Zwecke zu erreichen, so verwandeln sie sich in dem Maße, in dem die Datenbestände wachsen, in ein sich fortschreitend verselbständigendes Informationskapital. Unternehmen und Behörden werden sich mehr und mehr der Tatsache bewußt, daß die Daten für sie eine wichtige neue Einkommensquelle darstellen. Die Verarbeitung ist deshalb zunehmend von den Bemühungen geprägt, den Mehrwert der Daten zu kapitalisieren. So hat die EG-Kommission bereits Mitte der siebziger Jahre eine in den Vereinigten Staaten weit verbreitete Praxis aufgegriffen und begonnen, Vorschläge für gemeinschaftsweite Regeln zur Verwertung der von der öffentlichen Verwaltung gespeicherten Daten auszuarbeiten. Die Debatte ist, wie das 1999 verabschiedete Grünbuch zeigt, keineswegs versandet.

Am Grundsatz, daß der Erhebungsspielraum der öffentlichen Stellen beschränkt ist, ändert dies zwar nichts. Öffentliche Stellen müssen sich sowohl innerhalb der Europäischen Union als auch in den Vereinigten Staaten nach ihren je spezifischen Aufgaben richten und dürfen folglich nur die dafür jeweils erforderlichen Angaben erheben. In dem Augenblick aber, in dem die Daten in den Bereich der öffentlichen Stellen gelangen, werden auch Voraussetzungen und Grenzen der Dispositionsbefugnis neu bestimmt. Den öffentlichen Stellen wächst nach den bisher bestehenden oder vorgeschlagenen Regelungen das Recht zu, zumindest einen Teil der Angaben zu verwerten. Die Begründungen variieren. Sie reichen von einer wie immer definierten "Trivialität" der Daten bis zu einem durch die Erhebung ausgelösten "Eigentumsübergang". Das Ergebnis bleibt gleich: Die öffentlichen Stellen können mit dem Verkauf beginnen, die Betroffenen müssen sich damit abfinden.

Die Unternehmen haben ähnlich reagiert. Veräußerung und Leasing von Kundendaten sind weltweit die klassischen Beispiele einer direkten Verwertung. Die Vermarktung verläuft jedoch nicht immer reibungslos, allein schon im Hinblick auf die in den Datenschutzgesetzen, allerdings unterschiedlich scharf formulierte Zweckbindung der Verarbeitung. Die Generalklauseln des § 28 BDSG bieten aber genügend Schlupflöcher, um es doch noch zu versuchen. Selbst dort freilich, wo es, wie in den Vereinigten Staaten, an gesetzlichen Vorschriften zur Verarbeitung personenbezogener Daten weitgehend fehlt, regt sich, vor allem unter dem Eindruck der Erfahrungen mit Chipkarten und Internet, der Widerstand. So zwangen die öffentlichen Proteste gegen die Vermarktungsabsichten von American Express und Geocities beide Unternehmen dazu, ihre Pläne aufzugeben. Noch schärfer fiel die Reaktion beim Verkauf von Kundendaten der U.S. Bank an Telemarketing Unternehmen aus. Der Justizminister des Staates Minnesota leitete ein Verfahren gegen die Bank ein. Er berief sich dabei nicht nur darauf, daß unter den veräußerten Daten so sensitive Angaben wie etwa der Kontostand, die Sozialversicherungsnummer und der Kreditrahmen waren, sondern auch auf den eklatanten Widerspruch zwischen den fortwährenden Beteuerungen der Bank, das Interesse der Kunden an einer vertraulichen Behandlung ihrer Daten zu respektieren, und dem Verkauf der Daten.

Gleichviel jedoch, ob die Rücksicht auf bestehende gesetzliche Vorgaben oder der öffentliche Protest zur Zurückhaltung beim Verkauf zwingen, die Verwertungsabsichten werden keineswegs aufgegeben. Genaugenommen verschiebt sich nur der Akzent. So werden Patientendaten von Versicherungsgesellschaften oder von eigens mit der Verarbeitung von Rezeptdaten betrauten Unternehmen der pharmazeutischen Industrie überlassen. Der Vorteil für die Pharmaproduzenten ist leicht zu erkennen: Sie bekommen genau die Angaben, die sie für ein direktes, zudem eindeutig personalisiertes Gespräch mit Ärzten und Patienten brauchen. Die Gegenleistung variiert. Sie reicht von der Bereitschaft, die Werbung für einzelne, besonders kostspielige Präparate gezielt zurückzunehmen bis hin zu gemeinsam abgesprochenen Bemühungen, neue, die Kosten optimierende Produkte zu entwickeln. Das Begründungsspektrum ist einmal mehr weit gespannt. Von legitimen Eigenzwecken der Unternehmen ist ebenso die Rede wie von einer besseren Information der Patienten und ihrer finanziellen Entlastung oder auch von einem, etwa mit dem Versicherungsvertrag gleichsam zwangsläufig verknüpften Wechsel des "Eigentums" an den Daten.

Die Schwelle zur Kommerzialisierung ist damit überschritten. Ihren Höhepunkt erreicht sie freilich erst, wenn die Betroffenen unmittelbar in den Vermarktungsprozeß eingebunden werden. Der Grund liegt mehr oder weniger auf der Hand. Sobald sich die Kommerzialisierung nicht auf allen möglichen interpretatorischen Umwegen an den Betroffenen vorbei vollzieht, sondern unter ihrer Beteiligung, sind der Vermarktung tendenziell keine Grenzen mehr gesetzt. Die "informationelle Selbstbestimmung" geht im "property right" der Betroffenen auf, das den Ausschlag für alle weiteren Überlegungen gibt. Regulative Interventionen des Gesetzgebers weichen den Anforderungen des Marktes. Reflektiert wird folglich nur noch über die Verwertungsmöglichkeiten. Sie garantieren die Interessen der Betroffenen ebenso wie die Effizienz der Verarbeitung.

Die langwierigen Auseinandersetzungen zwischen John Moore einerseits sowie der Universität von Kalifornien, dem in Los Angeles angesiedelten Institut für Genetik und der Sandoz Pharmaceutical Corporation andererseits waren mit die ersten, in ihrer Bedeutung kaum zu unterschätzenden Vorzeichen dafür. John Moore litt an Leukämie und hatte deshalb im Oktober 1976 das Universitätsklini-

kum aufgesucht. Die Ärzte waren sich sehr bald darüber einig, daß sie es mit einem wahren "medizinischen Schatzkästchen" zu tun hatten. John Moores Blut enthielt Substanzen, die, nach Meinung der behandelnden Ärzte, ihnen genauso wie der Universität sowohl unter "Wettbewerbs-" als auch unter "kommerziellen und wissenschaftlichen Aspekten" beträchtliche Vorteile verschaffen könnten. Vor allem Blut, Rückenmark und die operativ entfernte Galle wurden deshalb in Unkenntnis des Patienten über Jahre intensiv für Forschungszwecke genutzt. Das Ergebnis waren zahlreiche Patente, die den Beteiligten einen Millionengewinn einbrachten. Als John Moore zufällig davon erfuhr, dachte er gar nicht daran, die Verwendung seiner Daten zu verbieten. Er verlangte vielmehr eine angemessene Beteiligung am bisherigen und künftigen Gewinn. Die Gerichte taten sich bis hin zum Supreme Court schwer. Statt auf die von John Moore explizit geltend gemachten "Verwertungsrechte" einzugehen, zogen sie es vor, sich nahezu ausschließlich mit möglichen Schadenersatzansprüchen zu beschäftigen.

Doch der Damm war gebrochen. Immer mehr "Data-Broker" schalten sich seither ein. Sie bieten den Betroffenen an, sie nicht nur vor unerwünschter Werbung zu bewahren, sondern auch einzelne Daten Interessenten gegen ein konkret zu vereinbarendes Entgelt zu überlassen. Die Betroffenen sollen damit die Chance erhalten, Angaben zu ihrer Person mit professioneller Unterstützung auf dem Informationsmarkt zu vertreiben, und zwar lediglich in dem jeweils gewünschten Umfang. Kaum jemand ist scheinbar bereit, sich dem zu entziehen. So verwundert es nicht, daß sich in Island Regierung und Parlament letztlich nur dazu bereit gefunden haben, die bereits erwähnten Verarbeitungspläne der "Decode Genetics" und deren Kooperation mit Hoffmann-La Roche zu billigen und gesetzlich abzusichern, nachdem Hoffmann-La Roche auf die besonders von der Regierung betonte "berechtigte Erwartung" der Betroffenen eingegangen ist, ihr Einverständnis nicht "umsonst" zu erteilen. Hoffmann-La Roche hat sich verpflichtet, die Einwilligung in die Verwertung ihrer Daten gleichsam in Naturalien, also mit firmeneigenen Medikamenten, zu honorieren.

Der Versuch, die informationelle Selbstbestimmung in ein "property right" umzudeuten, spielt im übrigen auch bei der Auseinandersetzung zwischen der Europäischen Union und den Vereinigten Staaten

über die Bedingungen der Übermittlung personenbezogener Daten eine wichtige Rolle. Einmal mehr wird die souveräne Verfügung der Betroffenen über ihr "property right" an den Daten in den Mittelpunkt gerückt. Verbindliche Anforderungen an den Datentransfer, wie sie in Art. 25 der EG-Datenschutzrichtlinie enthalten sind, werden deshalb in den Vereinigten Staaten zumeist genauso kategorisch verworfen wie die Forderung nach einer unabhängigen Kontrolle der Verarbeitung. "Selbstregulierung", "opt-out" und eine mögliche Kompensation für die Betroffenen wegen des Zugriffs auf ihre Daten scheinen statt dessen die einzig akzeptablen Regelungsgrundsätze zu sein.

Der Datenschutz wird so in die Hände der Beteiligten zurückverlegt. Die Betroffenen ebnen mit ihrem Verfügungsrecht den Weg für die Vermarktung ihrer Daten und können dafür einen "fairen Ausgleich" erwarten.

Kurzum, Einverständnis und Entgelt sind die Eckwerte eines Konzepts, das bewußt nahezu jede Schranke einer möglichen Verwertung der Daten beseitigt. Erst recht wird aber deutlich, daß Datenschutzgesetze unter diesen Umständen nur noch den Sinn haben, eine reibungslose Vermarktung sicherzustellen. Der Datenschutz reiht sich so nahtlos in jene Regelungen ein, deren Existenz und Ziel an der Funktionsfähigkeit des Marktes ausgerichtet sind und deshalb allein durch diese legitimiert werden.

II. Zerfall

1. Entwertung der Instrumente

Äußerlich hat sich am Instrumentarium des Datenschutzes wenig geändert. Gewiß, mancher Regelungsansatz wurde verfeinert und weiterentwickelt. Doch die Grundelemente des Datenschutzes sind auch dreißig Jahre nach der ersten gesetzlichen Regelung immer noch die gleichen. Kaum modifizierte phasenspezifische Verarbeitungsanforderungen werden nach wie vor durch altbekannte Rechte der Betroffenen und längst akzeptierte, durch die Aktivitäten eigens eingerichteter Instanzen geprägte und konkretisierte Kontrollstrukturen ergänzt. Die Kontinuität der Instrumente riskiert freilich, allzu

leicht als Bestätigung ihrer Effizienz aufgefaßt zu werden. Das Gegenteil ist der Fall. Die Beständigkeit kaschiert nur die schwindende Wirksamkeit. Wie brüchig die herkömmlichen Mittel sind, hatte sich schon an der on-line-Verarbeitung gezeigt. Die mühselige Uminterpretation der Übermittlungsbestimmungen übertünchte ebenso wie die wachsende Zahl von Spezialvorschriften allenfalls temporär die Risse im tradierten Regelungssystem.

Nicht anders ist es um die Kontrolle bestellt. Im Kontrollkonzept spiegelt sich die Annahme einer unausweichlichen Konzentration der Verarbeitung wider. Die Datenschutzbeauftragten sind das Gegengewicht zu einem scheinbar genauso expansiven wie zentralistisch angelegten Verarbeitungsprozeß. Ihre Rechte wurden daher vor dem Hintergrund einer so verstandenen Verarbeitung konzipiert und können sich unter diesen Umständen dann am besten entfalten, wenn sich die Verarbeitungsvorgänge möglichst zentral abspielen und sich daher nicht nur relativ schnell ausmachen, sondern auch weitaus leichter kontrollieren lassen. Je mehr daher Dezentralisierung und Vernetzung die Verarbeitungsmodalitäten von Grund auf veränderten, desto deutlicher geriet die Kontrolle an die Grenze ihrer Möglichkeiten. Doch die zunächst mühsam verleugneten Kontrolldefizite sind, seit Internet den Verarbeitungsprozeß dominiert, kaum zu übersehen. Die Kontrollinstanzen mögen deshalb unverändert weiterbestehen und ihre Bedeutung, wie erst jüngst durch die EG-Datenschutzrichtlinie, immer wieder bestätigt werden. Ihre Aktivitäten drohen trotzdem sich zunehmend als späte Illustration einer mittlerweile obsoleten Etappe der Verarbeitung zu erweisen.

Noch viel deutlicher fallen Erwartungen und Realität bei den individuellen Kontrollrechten auseinander. Die Diskrepanz zeichnete sich, genaugenommen, schon recht bald nach der Verabschiedung der ersten Datenschutzgesetze ab und verschärfte sich schnell. So läßt zwar kein Datenschutzgesetz das Auskunftsrecht aus. Im Gegenteil, ganz gleich, ob es um nationale, supranationale oder internationale Regelungen geht, das Auskunftsrecht wird überall in seltener Einmütigkeit zum harten, unverzichtbaren Kern des Datenschutzes gezählt. An Informationen über die faktische Bedeutung des Auskunftsrechts mangelt es dafür um so mehr. Nicht ohne Grund: Auskunft wird aller Erfahrung nach nur äußerst selten verlangt und wenn, fast ausschließlich im Gesundheits-, Sozial- und Sicherheits-

bereich. Beides, das evidente Desinteresse und die auffällige Zuspitzung auf bestimmte Verarbeitungen, spricht dafür, daß die Betroffenen solange nicht bereit sind, ihr Recht geltend zu machen, wie es an einem konkreten Anlaß fehlt oder es sich um einen aus ihrer Sicht besonders relevanten Verarbeitungsbereich handelt. Das Auskunftsrecht reicht also für sich genommen nicht aus. Soll es seiner Kontrollfunktion wirklich nachkommen, dann muß es um Vorkehrungen ergänzt werden, die gezielt die Aufmerksamkeit der Betroffenen auf die Verwendung ihrer Daten lenken.

Genau diesen Zweck erfüllt die oft geforderte, aber zumeist sorgfältig gemiedene Benachrichtigung. Sie konfrontiert die Betroffenen unmittelbar mit der Verarbeitung und bietet ihnen so die Möglichkeit, sich in Kenntnis der verarbeitenden Stelle, ihrer Aufgaben und der generell von ihr verwendeten Daten selbst darüber Gedanken zu machen, ob es sich lohnt, sich näher zu informieren. Selbst dort aber, wo eine Benachrichtigungspflicht ausdrücklich statuiert wird, herrscht offensichtlich die Tendenz vor, sie, soweit es nur geht, einzuschränken, indem man etwa schon eine direkte Erhebung der Daten bei den Betroffenen als Alternative gelten läßt, ohne Rücksicht im übrigen auf die Dauer oder den Umfang der Verarbeitung, und ansonsten darauf bedacht ist, sie bei der erstbesten Gelegenheit wieder abzuschaffen. Nur, selbst eine konsequente Verknüpfung von Benachrichtigung und Auskunft hilft nicht mehr weiter. Der Technologiewandel wirkt sich auch auf die Information der Betroffenen aus. Wo die Anzahl der verarbeiteten Daten unentwegt zunimmt, die Registrierung von Spuren zur Routine wird, räumliche und zeitliche Verarbeitungsgrenzen schwinden, fällt es schwer, Mechanismen aufrechtzuerhalten, die verläßliche Information sichern und es den Betroffenen zugleich ermöglichen, Korrekturen rechtzeitig anzumahnen und wirksam durchzusetzen. Das einst so gefeierte Auskunftsrecht droht vollends zu verkümmern, wie überhaupt Mechanismen, die den Verarbeitungsumfang einschränken und den Zugriff kanalisieren und transparenter gestalten sollten, mehr und mehr abstumpfen. Kurzum, die scheinbar so festen Fundamente des Datenschutzes zerbröseln.

2. Desintegration des Datenschutzes

Den Anfang machten Regelungen, die bewußt unpräzise und allgemein ausfielen. So deutlich Anlaß und Ziel waren, so tastend unsicher gestalteten sich die Reaktionen des Gesetzgebers. Anders und genauer ausgedrückt: Der radikale Technologiewandel bestimmte den Zeitpunkt der legislativen Intervention, die Sorge um die möglichen Auswirkungen der "Computerisierung" auf die Grundrechte und damit auf die Struktur von Staat und Gesellschaft die Tragweite des Eingriffs. Der zunächst so überschwenglich als Wegbereiter und Fundament einer vollendet rationalen Gesellschaft bejubelte Computer geriet plötzlich in ein ganz anderes Licht, als sich hinter dem einzigartigen Dokumentationsinstrument ein ebenso einmaliges Steuerungsmittel abzuzeichnen begann. Während die Ankündigung einer schier unbegrenzten Speicherung von Gesetzen, Entscheidungen, Verwaltungsakten oder Wirtschaftsdaten noch restloses Staunen erregte, schlug die Bewunderung in dem Augenblick in Beklemmung um, in dem mit demselben Aplomb die Absicht verkündet wurde, nun endlich alle an den unterschiedlichsten Orten befindlichen und von den verschiedensten Stellen gesammelten Daten der Bürgerinnen und Bürger zusammenführen zu können. Der Schatten des "numerierten" Bürgers legte sich mehr und mehr über den informierten Bürger.

Die Reflexionsebene veränderte sich. Die administrativen Probleme, wie etwa die Auseinandersetzungen darüber, nach welchen Kriterien die Auswahl der Dokumente erfolgen müßte, oder ob man tatsächlich den vollen Text aufnehmen sollte, statt sich mit Schlagworten zu begnügen, wichen einer dezidiert prinzipiellen Fragestellung. Verfassungsrechtliche und verfassungspolitische Aspekte rückten in den Vordergrund. Die Diskussion stand fortan unter dem Vorzeichen jener singulären Konstellation von Technologie und Grundrechten, die den Datenschutz begründet und seither begleitet und geprägt hat. Der lange und mühselige Weg von den Debatten des Hessischen Landtags über das Datenschutzgesetz von 1970, über die Verklammerung von "Informatik und Freiheitsrechten" in der Begründung und im Titel des französischen Gesetzes von 1976, die Entscheidung

des Bundesverfassungsgerichts vom Dezember 1983 zum Volkszählungsgesetz bis hin zum einleitenden Artikel der EG-Datenschutzrichtlinie von 1995 ist eine einzige Bestätigung der permanenten Präsenz dieser Konstellation und ihrer nachhaltigen Wirkung.

Der Gesetzgeber hatte, so gesehen, keine Wahl. Sein Eingriff ließ sich weder vermeiden noch vertagen. Die "Computerisierung" war kein diffuses, zeitlich höchst unbestimmtes Vorhaben. Die Pläne für die "Datenzentralen" waren längst konkretisiert, die erforderlichen gesetzlichen Vorschriften den Parlamenten, jedenfalls teilweise, bereits zugeleitet. Doch so seltsam es sich anhören mag: Die Technologie forderte nicht nur den Eingriff heraus, sie schränkte zugleich die Interventionsmöglichkeiten ein. Datenschutzgesetze sind ihrer ganzen Intention und Struktur nach nicht repressive, vielmehr eindeutig präventive Regelungen. Sie sollen die Technologie in grundrechtskonforme Bahnen lenken und nicht etwa nur Grundrechtsverletzungen korrigieren. Wie unverzichtbar Vorschriften sind, die gezielt auf die Technologiefolgen Einfluß zu nehmen suchen, sollte sich nur wenig später beim ersten französischen Großprojekt einer breit angelegten automatisierten Verarbeitung personenbezogener Daten zeigen. Schon dessen Name war, wenn auch ungewollt, prophetisch. "SAFARI" eröffnete in der Tat die Jagd auf die Daten. Gemeint waren im konkreten Fall Angaben zur sozialen und wirtschaftlichen Situation der Familien aller Neugeborenen, die in Kombination mit polizeilichen Daten dazu verhelfen sollten, Ansätze für "kriminogene Karrieren" zu diagnostizieren und ihnen rechtzeitig mit sozialtherapeutischen Maßnahmen zu begegnen.

Nur: Das Regelungsziel mag noch so klar gewesen sein, der Regelungsgegenstand war es, allem Anschein zuwider, nicht. Gewiß, von Computern und von der automatisierten Verarbeitung "persönlicher" Daten war viel die Rede. Doch an wirklich präzisen Aussagen fehlte es. Nicht von ungefähr. Verarbeitungsmodalitäten und Nutzungsmöglichkeiten begannen sich gerade erst abzuzeichnen. Die Folge war eine allen Datenschutzgesetzen der ersten Generation gemeinsame Regelungstechnik. Die mangelnde Detailkenntnis wurde durch das Zusammenspiel von Generalklauseln und organisatorisch-prozeduralen Vorschriften kompensiert. Dank der Generalklauseln standen die Chancen nicht schlecht, den Regelungsprozeß so anzugehen, daß möglichst viele bereits bestehende oder neu aufkommen-

de Verarbeitungskonstellationen einbezogen werden konnten. Eine besondere Kontrollinstanz und eine oft um eine Genehmigungspflicht ergänzte Meldepflicht automatisierter Verarbeitungsverfahren garantierten zudem einen immer besseren Einblick in Anlässe und Folgen der Verwendung personenbezogener Daten.

Die Strategien der Kompensation vermochten freilich nicht mehr als die Geltung der ersten Datenschutzgesetze temporär sicherzustellen. Generalklauseln und noch so vollständige, mit welchen administrativen Kompetenzen auch immer verbundene Register der Verarbeitungsaktivitäten sind kein Dauerersatz für mangelnde Präzision. Darüber können selbst kunstvolle Exkurse über die lange Tradition und die Unentbehrlichkeit von Generalklauseln nicht hinwegtäuschen. Gerade dort, wo, wie bei den Datenschutzgesetzen, die Grundrechte auf dem Spiel stehen und deren Wahrnehmung Existenz und Ziel der gesetzlichen Regelung bestimmt, ist Genauigkeit unverzichtbar. Nicht umsonst hat das Bundesverfassungsgericht im Volkszählungsurteil "Normenklarheit" angemahnt. Sie ist die Gewähr dafür, daß die informationelle Selbstbestimmung nicht zum Appell degeneriert, sondern sich als reale, konsequent beachtete Vorgabe jeder Verarbeitung personenbezogener Daten erweist. In dem Maße daher, in dem die zunächst überaus abstrakte Reflexion über die Verarbeitung und ihre Folgen einer durchaus konkreten, nicht zuletzt durch die Erfahrungen der Datenschutzbeauftragten und der Aufsichtsbehörden untermauerten sowie ständig weiter angereicherten Betrachtung wich, schwand die Legitimation der für die frühen Datenschutzgesetze charakteristischen Regelungstechnik.

Die Alternative zeichnete sich schon relativ bald nach der Verabschiedung des ersten Bundesdatenschutzgesetzes ab. Sie wurde zunächst von den Datenschutzbeauftragten angesprochen und später vom Bundesverfassungsgericht im Volkszählungsurteil als zwingende Konsequenz der Normenklarheit apostrophiert: Normative Anforderungen, die gezielt auf genau definierte Verarbeitungsbereiche zugeschnitten sein müssen. Und in der Tat: Bereichsspezifische Regelungen markieren den Schritt aus der ersten in die zweite Generation der Datenschutzgesetze. Wohl kein anderes Beispiel ist so bezeichnend für deren Bedeutung wie die fortschreitende Präzisierung des Auskunftsrechts. Alle Gesetze der ersten Generation haben sich emphatisch dafür ausgesprochen. Alle haben es aber auch genauso

dezidiert in Generalklauseln eingebettet, mit deren Hilfe die Bereitschaft, es allgemein anzuerkennen, ebenso allgemein wieder in Frage gestellt wurde. Die Folgen sind unschwer auszumachen. Das Regel-Ausnahme-Verhältnis droht gerade in besonders sensiblen Verarbeitungssektoren, wie etwa dem Sicherheitsbereich, auf den Kopf gestellt zu werden. Das Recht der Betroffenen zu erfahren, was mit ihren Daten geschieht, läuft also Gefahr, sich in eine Konzession zu verwandeln, die jederzeit unter Bedingungen widerrufen werden kann, die für die Betroffenen undurchschaubar sind. Erst die Revision der Polizeigesetze hat die Regelungsprämissen wieder zurechtgerückt. Ausnahmen gibt es zu Recht nach wie vor. Doch die Definitionsmacht wird nicht mehr, auf dem Umweg über Generalklauseln, ohne weiteres den Polizeibehörden zugestanden. Eigens eingefügte und in Kenntnis der spezifischen Anforderungen polizeilicher Arbeit entwickelte Vorschriften versuchen jedenfalls, die Ausnahmetatbestände einzugrenzen und präziser zu umschreiben. Sie sehen zudem ausdrücklich vor, daß die Verweigerungsgründe das Auskunftsrecht lediglich suspendieren, die Betroffenen also unverändert das Recht haben, eine Auskunft, allerdings zu einem späteren Zeitpunkt, zu bekommen. Schließlich: Die Betroffenen müssen sich selbst dann, wenn eine Auskunft unterbleibt, nicht einfach damit abfinden. Sie können die Datenschutzbeauftragten einschalten und sie bitten, zu überprüfen, ob ihnen die Informationen über den Umgang mit ihren Daten zu Recht vorenthalten worden sind.

Genauso ist es übrigens bei den Sozialdaten. Wiederum gibt der Verarbeitungskontext den Maßstab für die Verarbeitungsvoraussetzungen ab. Erneut modifiziert und präzisiert deshalb der Gesetzgeber die allgemeinen Regeln und knüpft etwa die Übermittlung an entschieden enger formulierte Bedingungen. Ganz in diesem Sinn haben, um ein letztes Beispiel zu nennen, die Landesgesetzgeber ihre Datenschutzgesetze nach und nach um eindeutig bereichsspezifische Teile ergänzt, die unter anderem Sondervorschriften für die Verarbeitung von Arbeitnehmerdaten enthalten.

Die Präzisierung kann allerdings leicht in Desintegration umschlagen. Anders und genauer ausgedrückt: Der Übergang von generellen auf bereichsspezifische Vorschriften macht nur solange einen Sinn, wie diese Teil eines einheitlichen, konsistent aufgebauten Regelungssystems bleiben, sich also darauf beschränken, gemeinsamen

Grundsätzen eine besondere, am jeweiligen Verarbeitungskontext orientierte Ausprägung zu verleihen. Bereichsspezifische Regelungen sind, so gesehen, nicht dazu bestimmt, die allgemeinen Datenschutzgesetze zu substituieren. Ihre Aufgabe besteht im Gegenteil darin, bereits formulierte Vorgaben aufzugreifen und zu verdeutlichen und damit Geltung und Effizienz des Datenschutzes zu maximieren. Allein deshalb ist es mit simplen, wenngleich kontextkonformen Wiedergaben bereits vorhandener Regeln nicht getan. Der Rückgriff auf einen besonderen Verarbeitungsbereich führt vielmehr dazu, sich auch und gerade mit neuen, bislang nicht bedachten Verarbeitungsaspekten auseinanderzusetzen. Jede bereichsspezifische Anpassung schreibt deshalb tendenziell die Anforderungen des Datenschutzes fort. Eine konsequente Integration bereichsspezifischer Vorschriften ist folglich kein einseitiger, ausschließlich auf die bereichsspezifischen Regelungen bezogener, sondern ein wechselseitiger, sich auf deren Leitprinzipien genauso auswirkender Vorgang. Der Datenschutz kann mit anderen Worten seine Ziele nur erreichen, wenn er als ein reflexives Regelungssystem verstanden wird, in dem bereichsspezifische Präzisierung und Revision der Ausgangsgrundsätze einander fortwährend ergänzen.

Doch statt einer sorgfältigen Abstimmung beherrscht offene Auflösung das Feld. Schon die weit verbreitete, etwa durch die Krankenhausgesetze exemplifizierte Restriktion bereichsspezifischer Regelungen auf eine schlichte Wiederholung der allgemeinen Bundes- und Landesvorschriften stimmt bedenklich. Wirklich gefährlich ist allerdings erst der manifeste Zerfall des Datenschutzes. Längst wird auf eine Verknüpfung der verschiedenen Regelungen nicht mehr geachtet. Was bleibt, sind gelegentliche Verweisungen, die allerdings noch keineswegs eine in sich geschlossene, widerspruchsfreie Anwendung sichern. Die Unstimmigkeiten und die Unübersichtlichkeit nehmen vielmehr gleichermaßen zu. Je neuartiger zudem der Regelungsgegenstand ist, desto deutlicher zeichnen sich die Verselbständigungstendenzen ab.

Mit das beste Beispiel dafür sind die Sondervorschriften zur Telekommunikation. Zentrale Grundsätze des Datenschutzes werden gleichsam neu entdeckt und dementsprechend zu genuinen Komponenten einer für den Informations- und Kommunikationsbereich typischen und deshalb ihm auch vorbehaltenen Regelung erklärt. So

ist plötzlich nicht mehr von der informationellen, sondern nur noch von der kommunikativen Selbstbestimmung die Rede, obwohl es wie bisher um nichts anderes als um die Kommunikationsfähigkeit der einzelnen geht und damit um deren Recht, selbst darüber zu befinden, wer wann und unter welchen Bedingungen auf ihre Daten zugreifen darf. Und so wird die "Datenvermeidung" als Grundstein eines anderen, wirklich modernen Datenschutzes präsentiert, obgleich die Minimierung der Verarbeitung personenbezogener Angaben von Anfang an Kernstück aller Regelungsbestrebungen war. Mehr noch: Selbst dann, wenn, wie bei der Revision etwa der Datenschutzgesetze, die Vorschriften aus dem Telekommunikationsbereich mit in die Reflexion über mögliche Änderungen einbezogen werden, kommt es lediglich zu einer weitgehend wörtlichen Übernahme der Bestimmung über die "Datenvermeidung". Die Frage, ob es sich nicht um einen immer schon akzeptierten allgemeinen Grundsatz handelt, der daher keineswegs in seiner sektoralen Form aufgenommen werden kann, wird gar nicht erst gestellt. Die Revision gerät so zur Illustration der Zersplitterung des Datenschutzes. Das Datenschutzgesetz gibt nicht mehr die Grundlage für alle weiteren Regelungen ab. Es reduziert sich auf eine Zusammenstellung unterschiedlicher, weder auf ihre Tragweite noch auf ihre Konsistenz wirklich geprüfter Elemente. Besser läßt sich das geschwundene Bewußtsein für die Einheit des Datenschutzes kaum veranschaulichen.

3. Das Ende der rein normativen Konzepte

Die beiden ersten Generationen der Datenschutzgesetze haben eines gemeinsam: Sie beruhen auf der Vorstellung, daß normativ abgesicherte Verhaltensvorgaben ebenso notwendig wie ausreichend sind. Ganz in diesem Sinn stellen alle Gesetze Regeln auf, die in gleichsam klassischer Manier die Rechtmäßigkeitsvoraussetzungen der Verarbeitung genauso definieren wie etwa die Rechte der Betroffenen oder die Kontrollbedingungen. Dahinter steht die schon für die frühen Debatten über einen legislativen Eingriff charakteristische Kontrastierung von Datenschutz und Datensicherung. Die Forderung nach Datenschutz wurde mit anderen Worten als klare Absage an die vor allem von den Computerherstellern vertretene Annahme verstanden, technische Vorkehrungen reichten völlig aus, um die Verarbeitung personenbezogener Daten in einer die Interessen der Betroffe-

nen berücksichtigenden und ihnen gerecht werdenden Art und Weise einzugrenzen. Keine noch so ausgefeilte technische Vorkehrung kann in der Tat bestimmen, welche Daten überhaupt erhoben oder übermittelt werden dürfen. Ziel und Einsatz der technischen Vorkehrungen sind vielmehr normativ prädeterminiert. Nicht von ungefähr listen deshalb das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze technisch-organisatorische Maßnahmen lediglich in einem Anhang auf und geben sich im übrigen mit einer Generalklausel zufrieden, die es letztlich offen läßt, wie die Vorkehrungen auszusehen haben. Deutlicher hätte deren ausgeprägt akzessorische Funktion kaum zum Ausdruck gebracht werden können.

So einsichtig, ja berechtigt es zunächst erschien, sich für einen entschieden normativen Ansatz auszusprechen, so wenig hilft eine so konzipierte Regelung bei einer konsequent dezentralisierten, an keine räumliche oder zeitliche Grenzen gebundenen Verarbeitung weiter. On-line, Chipkarten und Internet sind Stationen eines Weges, auf dem sich die Einflußmöglichkeiten normativer Konzepte zunehmend verflüchtigten. Wo Anonymität zur Fiktion gerät, Datensammlung zur Routine wird, Verarbeitungsvorgänge von beliebigen Stellen aus zu ebenso beliebigen Zeiten durchgeführt werden können und sich die Spuren der Betroffenen zwar immer weiter verdichten, die Spuren des Zugriffs auf ihre Daten aber immer mehr verlieren, lassen sich mit rein normativen Vorgaben bestenfalls Intentionen umschreiben. Ihre Realisierung ist dagegen fraglicher denn je.

Solange, beispielsweise, personalisierte Zahlungsmodalitäten nach wie vor, auch und gerade im Internet, an Bedeutung gewinnen, Bewegungsprofile weiterhin zu den fast selbstverständlichen Nebenprodukten der veränderten Verarbeitungstechnologie zählen, Spuren nicht gezielt eingedämmt werden können und Nutzer außerstande sind, Inhalte und Sendeaktionen verläßlich zu steuern, schwindet die von den Datenschutzgesetzen nachdrücklich geforderte Transparenz und bleiben fundamentale Grundsätze wie die Verpflichtung, von einer Verwendung personenbezogener Daten möglichst abzusehen oder eine strikte Zweckbindung sicherzustellen, wirkungslos. Die Betroffenen mögen nominell noch über eine verfassungsrechtlich abgesicherte Entscheidungsprärogative verfügen, sie sind aber in Wirklichkeit längst Objekte eines vom Gesetzgeber nicht mehr kontrollierbaren Prozesses.

Keines dieser Beispiele signalisiert allerdings Einzeldefizite bestehender Regelungen. Jedes von ihnen ist, im Gegenteil, symptomatisch für die strukturelle Insuffizienz exklusiv normativer Regelungskonzepte. Sie sind an der Grenze ihrer Möglichkeiten angelangt. Anders als seinerzeit beim Übergang von den allgemeinen zu den bereichsspezifischen Gesetzen kann es daher nicht mehr darum gehen, den Geltungsanspruch der normativen Konzepte neu zu begründen. Die Realität der Verarbeitung hat sie endgültig überholt. Sie sind deshalb nur noch mühsam konservierbare Relikte einer anderen Verarbeitungsepoche und nicht etwa reparierbare Regelungsmechanismen.

III. Rekonstruktion

1. Technisierung des Datenschutzes

Die Chance des Datenschutzes liegt, so paradox es klingen mag, in der Verarbeitungstechnologie. Sie war es, die ihn destabilisierte, sie ist es aber auch, die ihm die Möglichkeit bietet, seinen Geltungsanspruch wieder durchzusetzen. Sicher, der Datenschutz wird durchaus zu Recht als eine gezielte Restriktion der Verarbeitung personenbezogener Angaben und damit zwangsläufig als Technologiebarriere wahrgenommen. Doch die Erfahrung hat schon relativ früh gezeigt, daß sein Gegenstand genauso gut sein Instrument sein kann. Gemeint sind etwa die ersten Versuche, Telefonkarten einzuführen. Keiner der immer wieder vorgebrachten Einwände war, genaugenommen, schlüssig. Was an den vorausbezahlten Wertkarten wirklich störte, waren nicht die vielzitierten organisatorischen, technischen und finanziellen Schwierigkeiten, sondern die berechtigte Befürchtung, daß ihre Einführung eine neue und zudem höchst profitable Informationsquelle verschütten würde. In einer Zeit, in der sich Kreditkarten anschickten, das Bargeld mehr und mehr zu verdrängen, erschienen ganz nach dem Muster der Kreditkarten konzipierte Zahlungsmodalitäten für Telefongespräche als die ideale Ergänzung, sei es der ohnehin systematisch ausgewerteten Daten aus den Telefonbüchern, sei es der ansonsten über die Kreditkarten erhobenen Angaben. Kein Wunder, daß die potentiellen Nutznießer nur Nachteile aufzuzählen wußten, die Datenschutzbeauftragten aber dafür die Vorteile der

Telefonkarten entdeckten. Sie stellen eine verlorengegangene Anonymität wieder her und dämmen die scheinbar unaufhörliche Ausweitung der Verarbeitung personenbezogener Daten wenigstens in einem unstreitig besonders empfindlichen Sektor ein.

Eine zweite, ganz andere Erfahrung brachte die Technologie ebenfalls, allerdings auf Umwegen, ins Spiel. Die heftigen Diskussionen über den Einfluß des Fernsehens auf das Verhalten von Jugendlichen lösten in den Vereinigten Staaten die Forderung nach technischen Hilfsmitteln aus, die es den Eltern erlauben würden, den Zugang zu einzelnen Sendungen oder Kanälen zu sperren. Nichts lag unter diesen Umständen näher als auch im Internet ähnlich zu verfahren. Wiederum ging es um technische Instrumente, die Unzugänglichkeit garantieren sollten und erneut war die Technologie Ansatzpunkt von Bestrebungen, den Betroffenen die Entscheidungsmacht über die Preisgabe ihrer Anonymität wiederzugeben.

Das Fundament für eine eigens auf den Datenschutz zugeschnittene Technologie war damit gelegt. Die Beispiele häuften sich. Ganz gleich, ob man die immer weiter verfeinerten Spezialfilter, das breite Angebot von "Pretty-Good-Privacy", den "Identity-Protector" oder die "MixMaster-Remailer" nimmt, eines bestätigt sich: Der Datenschutz ist, soll er wirklich auf die Verarbeitung einwirken, auf die Technologie angewiesen. "Privacy-enhancing technology" ist deshalb mittlerweile zum Schlagwort für ein neues, die Technologie gezielt instrumentalisierendes Verständnis des Datenschutzes geworden. Der Wandel wird freilich eher verhüllt als verdeutlicht, wenn von "datenschutzfreundlichen" Technologien die Rede ist. Allzu leicht entsteht der Eindruck als ginge es lediglich um eine generelle Kategorisierung. Akzeptable, ja wünschenswerte, "freundliche" Technologien sollen eben von inakzeptablen "feindlichen" unterschieden werden. In Wirklichkeit steht entschieden mehr zur Debatte: Eine gesetzlich abgestützte, aktive Technologiepolitik. "Freundlich" beschreibt, so gesehen, die Erwartungen nur unzureichend. Notwendig sind vielmehr Technologien, die den Datenschutz ebenso gezielt fördern wie garantieren. Die Technologie muß, mit anderen Worten, aus der Peripherie in den Mittelpunkt der legislativen Intervention rücken.

Damit bahnt sich zugleich der Übergang zu einer neuen, dritten Generation von Datenschutzgesetzen an. Deren hervorstechendes, ureigenstes Merkmal sind Regelungsmechanismen, die bewußt auf die Technologie setzen und sie konsequent einbeziehen. Wohlgemerkt, der Gesetzgeber schreibt nicht näher spezifizierte und womöglich in allen Einzelheiten definierte Vorkehrungen, sondern nur Vorgaben fest. Wie die jeweiligen Vorkehrungen konkret auszusehen haben, ist infolgedessen ausschließlich Sache der Industrie. Um so deutlicher konzentriert sich die Aufmerksamkeit auf das Ergebnis: Es ist nur solange hinnehmbar, wie es den Maßstäben voll genügt, die der Gesetzgeber formuliert hat. Der Datenschutz geht so den Weg, den vor allem das Umweltrecht längst eingeschlagen hat. Genau wie dort wird das Regelungsziel gleich doppelt abgesichert. Zwingende rechtliche Anforderungen werden in genauso verbindliche technische Erwartungen umgesetzt. Wie beim Umweltschutz dürfen zudem die je spezifischen Vorkehrungen nicht Teil einer unverbindlich angebotenen Sonderausstattung sein. Die Marktfähigkeit des Informations- und Kommunikationsinstrumentariums muß vielmehr von der Existenz solcher Vorkehrungen abhängen.

Kurzum, der Aufbau einer gesetzlich initiierten und implementierten datenschutzgerechten Technologie ist Grund- und Prüfstein aller Bemühungen, den Datenschutz aus der gegenwärtigen Sackgasse herauszuführen. Er wird, dank der Technisierung seiner Regelungsansprüche, in den Verarbeitungsprozeß hineinverlegt. Die Verarbeitungsgrenzen werden folglich nicht mehr durch externe und deshalb sehr viel leichter umgehbare Barrieren bestimmt, sondern durch technikimmanente Schranken, die den gesamten Ablauf des Verarbeitungsprozesses steuern. Soll aber dieses Ziel wirklich erreicht werden, dann bedarf es einer datenschutzgerechten Technologie, die sich auch und vor allem durch ein Höchstmaß an Flexibilität auszeichnen muß. Noch so überzeugende Reaktionen auf den jeweiligen Stand der Informations- und Kommunikationstechnologie genügen daher nicht. Gesetzliche Vorgaben und konkrete technische Vorkehrungen können vielmehr ihrer Aufgabe nur gerecht werden, wenn sie das hohe Veränderungspotential der Verarbeitungstechnologie durch eine genauso ausgeprägte Adaptationsfähigkeit aufzufangen vermögen. Der Schlüssel dazu ist nicht anders als bei allen Überlegungen zur Effizienz des Datenschutzes eine permanente, konsequent betriebene Technikfolgenabschätzung. Sie liefert den letztlich entschei-

denden Maßstab dafür, ob die gesetzlichen Vorgaben und deren technische Umsetzung nach wie vor ausreichen. Bewertung und Antizipation der Technikfolgen sind deshalb eine genauso unabdingbare Voraussetzung des Datenschutzes wie die gesetzliche Regelung selbst.

2. Revision der rechtlichen Regelungselemente

So wichtig, ja unentbehrlich die Technisierung des Datenschutzes ist, so wenig gilt es, darüber Klarheit und Konsistenz der rechtlichen Regelungselemente zu vernachlässigen. Mehr denn je kommt es, allein schon mit Rücksicht auf die Intensität der Verarbeitung und die wachsende Proliferation der Daten, darauf an, doch noch zu versuchen, jene Hoffnung auf Übersichtlichkeit und Präzision zu erfüllen, die nicht zuletzt an der bereichsspezifischen Zersplitterung des Datenschutzes zerschellt ist. Das Rezept scheint in Zeiten der Deregulierung denkbar einfach zu sein: Eine radikale Entrechtlichung des Datenschutzes verbunden mit einer konsequenten Konzentration der rechtlichen Anforderungen auf eine bewußt gering gehaltene Anzahl leicht auffindbarer und möglichst einfacher Bestimmungen. Alles spricht, so gesehen, für eine Rehabilitierung der Generalklauseln.

Ihr spätes Lob verkennt freilich dreierlei Zunächst: Bereichsspezifische Regelungen sind, um noch einmal daran zu erinnern, nicht zufällig entstanden oder gar Produkte einer willkürlichen "Überregulierung". Sie sollten vielmehr dem Datenschutz die Glaubwürdigkeit und Verläßlichkeit zurückgeben, die ihm die mangelnde Präzision der Generalklauseln genommen hatte. Wer deshalb so vehement für Generalklauseln plädiert, muß auch und gerade auf die Frage eingehen, wie es, anders als bisher, gelingen kann, Genauigkeit dort sicherzustellen, wo Ungenauigkeit systemimmanentes Element der angestrebten Regelung ist. Solange jedoch eine Antwort darauf fehlt, bleibt es dabei: Die Unübersichtlichkeit wird durch die Rückkehr zu den Generalklauseln nicht korrigiert, sondern nur unter einem anderen Vorzeichen fortgesetzt und zementiert.

Im übrigen: Vagheit der Erwartungen und Undurchschaubarkeit der gesetzlichen Regelung lassen sich nicht mit einem Gewinn an Spielraum für die "Rechtsanwender" rechtfertigen. Soweit damit auch die

verarbeitenden Stellen gemeint sein sollten, haben die bisherigen Erfahrungen nur zu gut gezeigt, welche Folgen für die Betroffenen ein nicht von Anfang an strikt begrenzter Interpretationsradius nach sich zieht. Sie werden mit dem Risiko einer Auslegung belastet, die den Datenschutz möglichst beschränkt, also jeden sich bietenden Ansatz nutzt, um die Verarbeitungschancen auszuweiten. Nicht zuletzt davor sollten die Betroffenen durch entschieden präzisere bereichsspezifische Vorschriften geschützt werden. Zu den "Rechtsanwendern" zählen allerdings auch die Datenschutzbeauftragten und die für den nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden. Weder deren Kontrollfunktion noch die explizit garantierte Unabhängigkeit der Datenschutzbeauftragten legitimieren jedoch einen Verzicht auf Exaktheit und Transparenz. Eine breite, bewußt unklar gehaltene Interpretationsmarge beschwört Divergenzen förmlich herauf, die einmal mehr zu Lasten der Betroffenen gehen. Daß es sich dabei um eine durchaus realistische Annahme handelt, zeigt sich an manchen, in den Tätigkeitsberichten der Datenschutzbeauftragten angesprochenen und verschieden bewerteten Alltagsproblemen des Datenschutzes ebenso wie an prinzipiellen Auseinandersetzungen. Mit eines der wichtigsten Beispiele dafür ist die unterschiedliche Einschätzung des später, jedenfalls partiell, für verfassungswidrig erklärten Volkszählungsgesetzes von 1983. Genauso bezeichnend sind aber auch Entscheidungen wie jenes Urteil des Conseil d'État, das der französischen Datenschutzkommission vorwarf, das Datenschutzgesetz unnötig eng und für die Betroffenen viel zu nachteilig interpretiert zu haben.

Schließlich: Die Normenklarheit bleibt auch unter den veränderten, primär durch das Internet bestimmten Informations- und Kommunikationsbedingungen verbindliche Regelungsprämisse. Kompromisse, die früher noch möglich und vertretbar erschienen, scheiden freilich von vornherein aus. Wo die Verarbeitung zur Routine gerät, die Datenbestände fortwährend ausgeweitet und ergänzt werden, sich mehr oder weniger lückenlose Profile jederzeit anfertigen lassen und sich die Grenzen zwischen öffentlicher und nicht-öffentlicher Verarbeitung verwischen, geraten Generalklauseln zu Generalschlüsseln. Wer sich auf Generalklauseln berufen kann, hat es dank ihrer Unbestimmtheit in der Hand, sich einen tendenziell schrankenlosen Zugang zu einer sowohl dem Umfang als auch der Art nach unbeschränkten Anzahl von Daten zu verschaffen. Von einer auch und

vor allem für die Betroffenen überschaubaren und kontrollierbaren Verarbeitung läßt sich unter diesen Umständen kaum noch ernsthaft sprechen. Im Gegenteil, deutlicher kann die Verletzung der Normenklarheit nicht mehr ausfallen.

Beim Übergang zur dritten Gesetzesgeneration stellt sich also, wenngleich sehr viel schärfer, genau die Frage, die bei der Überleitung von der ersten auf die zweite ebenfalls im Mittelpunkt aller Überlegungen gestanden hatte. Anders als damals geht es freilich nicht mehr an, sich mit Generalklauseln abzufinden. Sie müssen vielmehr einer möglichst präzisen und abschließenden Umschreibung der Verarbeitungsgründe weichen. Im Grunde genommen keine völlig neue und allein schon deshalb nur schwer erfüllbare Erwartung. Ein Vorbild gibt es durchaus: Die strikte Abschottung der Protokolldaten. Sie ist gerade vor dem Hintergrund der im Sicherheitsbereich besonders verbreiteten Generalklauseln entstanden und soll die mit der Zweckbindung verknüpften inhaltlichen und zeitlichen Verarbeitungsschranken absichern. Einfach ist es trotzdem nicht. Jeder Verzicht auf Generalklauseln löst unweigerlich Zugriffsrestriktionen aus, die zumindest solange erträglich erscheinen, wie nicht feststeht, ob sich wirklich Daten finden lassen, die für die jeweils am Zugang interessierte Stelle von Bedeutung sein könnten. Genau diese Ungewißheit hat spätestens seit den Chipkarten und erst recht, seitdem sich der Kommunikationsschwerpunkt zunehmend auf das Internet verschiebt, wenn nicht ganz, so doch weitgehend aufgehört zu bestehen. Der Datenfundus enthält so gut wie jede Information. So gesehen spricht nahezu alles dafür, daß es durchaus gelingen dürfte, die jeweils benötigten Angaben aufzuspüren. In einer Gesellschaft, in der sich Informationsbarrieren immer niedriger gestalten, gilt es deshalb, diese umgekehrt dort fortlaufend zu erhöhen, wo es um personenbezogene Daten geht. Je deutlicher somit Allwissenheit faktisch reale Züge annimmt, desto stärker muß rechtlich Nichtwissen als Leitprinzip aller Verarbeitung gewährleistet, also selbst dann garantiert werden, wenn Wissen durchaus möglich wäre.

3. Gegenkräfte

An Möglichkeiten, die Effizienz des Datenschutzes zurückzugewinnen, fehlt es zwar nicht. Sie stehen aber durchweg unter dem mitt-

lerweile klar erkennbaren Vorbehalt einer Kommerzialisierung der Verarbeitung, die sich mehr und mehr im Zeichen einer Akquisition der Daten bei den Betroffenen selbst vollzieht. Sie werden direkt angesprochen und sie sind es auch, die ihre Daten verkaufen. Der rechtliche Ansatz ist allem Anschein nach einwandfrei. Kein Gesetzgeber hat schließlich bei der Frage nach der Rechtfertigung der Verarbeitung gezögert, die Einwilligung auf eine Stufe mit gesetzlichen Verarbeitungsanforderungen zu stellen. Sämtliche Gesetze gehen zudem wie selbstverständlich davon aus, daß die Betroffenen frei entscheiden können, welche ihrer Daten wem überlassen werden dürfen. Einschränkungen gibt es nicht einmal bei besonders "sensitiven Daten". Die Verarbeitung muß sich zwar im Prinzip nach deutlich restriktiveren Vorschriften richten, Zweifel sind trotzdem ausgeschlossen. Die Einwilligung der Betroffenen reicht, wie sich etwa an der EG-Datenschutzrichtlinie (Art. 8 Abs. 2 Buchst. a) zeigt, einmal mehr aus.

Bedenken hat es trotzdem gegeben. Vor allem bei der Verarbeitung von Arbeitnehmerdaten zeigte sich sehr schnell, daß es kaum angeht, sich so vorbehaltlos auf die Einwilligung zu verlassen. Allein schon die längst von der Rechtsprechung festgeschriebenen Grenzen des Arbeitgeberfragerechts illustrieren die Notwendigkeit genauso klarer wie verbindlicher Einschränkungen. Genau diesem Ziel dient auch das im Betriebsverfassungsgesetz (§ 94 Abs. 1) vorgesehene Mitbestimmungsrecht der Arbeitnehmervertretungen bei Fragebögen. In ihren ausdrücklich auf die Verarbeitung von Arbeitnehmerdaten bezogenen Empfehlungen hat sich schließlich die Internationale Arbeitsorganisation ebenfalls für eine strikte Begrenzung ausgesprochen. Ähnlich ist übrigens die Diskussion bei den für Versicherungsverträge typischen Datenschutzklauseln verlaufen. Sie waren zunächst ganz auf die Informationserwartungen der Versicherungsgesellschaften abgestellt und durch die Einwilligung der Versicherungsnehmer abgedeckt. Doch die ursprüngliche Fassung scheiterte sehr bald am Widerstand der Datenschutzbeauftragten und des Bundesaufsichtsamts für das Versicherungswesen. Der neue Text begrenzt den Verarbeitungsspielraum der Versicherungen verbindlich und ist mit beiden Kontrollinstanzen abgesprochen. Der Einwilligung kommt, so gesehen, nur noch eine rein formale Funktion zu. Sie wirkt sich also keineswegs auf Inhalt und Tragweite der Klausel aus,

sondern manifestiert und bekräftigt lediglich die Bereitschaft der Versicherungsnehmer, eine ohnehin feststehende Regelung zu akzeptieren.

Aber auch die Datenschutzgesetze sind, allem Anschein zum Trotz, nicht frei von Zweifeln. Die Landesdatenschutzgesetze und das Bundesdatenschutzgesetz betonen zwar den Vorrang der Einwilligung, knüpfen ihn allerdings an zwei Bedingungen. Einwilligungen müssen grundsätzlich schriftlich erteilt werden. Die Betroffenen dürfen überdies nicht auf ihre Kontrollrechte verzichten. Beides soll mögliche negative Folgen einer beliebigen Freigabe der eigenen Daten kompensieren. Die Schriftform verzögert den Entscheidungsprozeß, das Verzichtverbot sichert eine nachträgliche Überprüfung der Einwilligungsfolgen. Anders ausgedrückt: Die Einwilligung wird vordergründig nicht angetastet, in Wirklichkeit jedoch in ein Regelsystem eingefügt, das ihre Gefahren zumindest vermindern soll. Noch deutlicher reagiert die Richtlinie, wenngleich nur bei der Verarbeitung sensitiver Daten. Sie räumt den Mitgliedstaaten das Recht ein, die Einwilligung auszuschließen (Art. 8 Abs. 2 Buchst. a).

Skepsis und Kritik sind allerdings, sieht man von den wenigen punktuellen Korrekturen einmal ab, folgenlos geblieben. Die Gleichstellung von Einwilligung und gesetzlicher Regelung hat alle Reformen der Datenschutzgesetze überstanden. Mehr noch, die Einwilligung ist als ideale Alternative zu den immer komplizierteren und kaum noch überschaubaren gesetzlichen Bestimmungen angepriesen worden. Je geringer freilich die Vorbehalte gegenüber der Einwilligung sind, desto leichter fällt es, die Entscheidungsbefugnis der Betroffenen zu nutzen, um den Datenschutz zu unterlaufen.

So hat sich der Gesetzgeber bei der 1990 verabschiedeten Novellierung des Bundesdatenschutzgesetzes ausgerechnet auf die informationelle Selbstbestimmung berufen, um mit die wichtigste Voraussetzung eines wirklich wirksamen Datenschutzes auszuhebeln, eine konsequente, auf Prävention bedachte Kontrolle der Verarbeitung. Bei bestimmten "besonders sensiblen Daten", also etwa bei Angaben, die dem Arztgeheimnis unterliegen oder in Personalakten enthalten sind, zwingt der Respekt vor der Entscheidungsprärogative der Betroffenen, nach Meinung des Gesetzgebers, dazu, sie darüber befinden zu lassen, ob der Bundesbeauftragte für den Datenschutz ihre

Daten einsehen darf. Sicher, der Gesetzgeber gibt sich mit einem Widerspruchsrecht zufrieden (§ 24 Abs. 2 Satz 4), bleibt mithin auf halbem Wege stehen und beeilt sich zudem unter dem Eindruck der sich verschärfenden Kritik zu versichern, nichts habe ihm ferner gelegen als eine "Einwilligungslösung". Was aber auf den ersten Blick ganz nach einem Kompromiß aussieht, der das Entscheidungsrecht der Betroffenen wenigstens partiell aufrechtzuerhalten sucht, läßt in Wirklichkeit, genauso übrigens wie die Kontroverse über Bedeutung und Tragweite der Feststellung, die Betroffenen müßten selbstverständlich "Gelegenheit" haben, ihr Widerspruchsrecht auszuüben, das eigentliche Motiv des Gesetzgebers aufscheinen. Die gesetzliche Regelung spiegelt eben nicht den Wunsch wider, die Einwirkungschancen der Betroffenen zu garantieren. Deren Entscheidungsbefugnis wird, im Gegenteil, gezielt instrumentalisiert, um die auch und gerade vom Bundesverfassungsgericht im Volkszählungsurteil nachhaltig geforderte umfassende Kontrolle der Verarbeitung zu konterkarieren. Mit der Widerspruchsmöglichkeit wird ein Hindernis aufgebaut, das die Überwachung keineswegs bloß verzögert, sondern letztlich leerlaufen läßt. Eine Kontrolle, die nicht nur darauf ausgerichtet ist, Einzelverstößen gegen die Verarbeitungsanforderungen nachzugehen, vielmehr vor allem Verhaltensmuster und Verarbeitungstendenzen offenlegen soll, bleibt solange illusorisch wie sie in zentralen Verarbeitungsbereichen lediglich auf ein gleichsam willkürlich zerstückeltes Material zurückgreifen kann.

Wohl in keinem anderen Fall wird freilich die informationelle Selbstbestimmung so nachhaltig instrumentalisiert wie bei der fortschreitenden Kommerzialisierung der Verarbeitung personenbezogener Daten. Wiederum scheint alles dafür zu sprechen, sich an die Betroffenen zu halten. Schließlich geht es um ihre Daten. Sie müßten daher, so meint man, auch darüber selbst entscheiden können, ob ihre Daten vermarktet werden sollen und erst recht berechtigt sein, sich über den Preis zu verständigen. So gesehen käme es in der Tat einer Mißachtung ihrer informationellen Selbstbestimmung gleich, sie davon abzuhalten oder es ihnen gar zu verbieten. Einmal mehr verbirgt sich jedoch hinter der vermeintlich so engagierten Verteidigung der informationellen Selbstbestimmung eine zielstrebige Demontage des Datenschutzes.

Ein besseres Mittel als die Einwilligung, um die jeweils gewünschten Daten schnell und möglichst an allen Datenschutzhindernissen vorbei systematisch zu verwerten, gibt es nicht. Dank der Einwilligung erwirbt der Käufer mit den Daten auch das Recht, diese grundsätzlich für seine Zwecke, und zwar ganz nach seinen Vorstellungen zu verwenden. Letztlich kommt es deshalb nur darauf an, die Einwilligung so zu formulieren, daß Zweifel an der Fortgeltung gerade jener gesetzlichen Verarbeitungsbedingungen gar nicht erst auftauchen, die den Vermarktungsprozeß besonders erschweren. Nicht von ungefähr sind die Auseinandersetzungen über die Auswirkungen der EG-Richtlinie auf die Übermittlung personenbezogener Daten in die Vereinigten Staaten von den Bemühungen begleitet und geprägt worden, auf die Einwilligung und die Information der Betroffenen zurückzugreifen, um die Zweckbindung, so weit es nur geht, auszuschalten. Je deutlicher sich allerdings solche Bestrebungen durchsetzen, desto janusköpfiger erweist sich die informationelle Selbstbestimmung. Sie soll einerseits die Herrschaft der Betroffenen über ihre Daten sichern, schafft jedoch andererseits die Voraussetzungen, um ausgerechnet die Verarbeitungseinschränkungen zu überwinden, die um der informationellen Selbstbestimmung willen entwickelt und gesetzlich verankert worden sind.

Die informationelle Selbstbestimmung ist freilich weit mehr als ein personalisiertes Entscheidungs- und Verfügungsrecht. Sie ist auch und gerade konstitutives Merkmal der Kommunikations- und Partizipationsfähigkeit des einzelnen, damit aber, um noch einmal an die Aussage des Bundesverfassungsgerichts im Volkszählungsurteil zu erinnern, "elementare Funktionsbedingung einer freiheitlich-demokratischen Gesellschaft". Erst die Verknüpfung beider Aspekte macht die Bedeutung der informationellen Selbstbestimmung aus und begründet zugleich die Notwendigkeit, die Verarbeitung personenbezogener Daten gesetzlich zu regeln. Anerkennung und Wahrnehmung der Entscheidungsprärogative der Betroffenen gehen deshalb keineswegs lediglich die Betroffenen etwas an, sondern wirken sich genauso auf die Struktur der Gesellschaft aus.

Steuerbarkeit und Anpassungszwang gefährden allerdings die Kommunikations- und Partizipationsfähigkeit der Betroffenen keineswegs nur, solange sie nicht wissen, wer ihre Daten wofür nutzt, vielmehr ebenso dann, wenn die Daten mit Wissen und Billigung der Betrof-

fenen vermarktet werden. Dort, wo die Einwilligung zum Vehikel der Kommerzialisierung wird, fördert und potenziert sie das Instrumentarium einer Verarbeitung, deren Anlaß und Ziel eine möglichst wirksame Einflußnahme auf das Verhalten der Betroffenen ist. Eine, gerade dank der Kommerzialisierung, sich ständig weiter verdichtende, eindeutig personalisierte, in Profile umgesetzte Information erlaubt es, die günstigsten Ansatzpunkte für eine Beeinflussung der Betroffenen auszumachen, deren Reaktionen, jedenfalls partiell, besser zu antizipieren und deren Verhalten prädefinierten, am Waren- und Dienstleistungsabsatz orientierten Erwartungen anzupassen. Keine der ansonsten immer wieder beschworenen Gefahren fällt also deshalb weg, weil die Betroffenen sich mit der Verarbeitung einverstanden erklärt haben.

Sicher, ein Gegenmittel drängt sich fast von selbst auf. Die Schranken der Monetarisierung der Daten und ihrer Kommerzialisierung hängen auch und vor allem von der Schärfe der Zweckbindung ab. Eine Vermarktung lohnt erst, wenn der Verarbeitungsspielraum weit genug ist, um eine hinreichend große Zahl an Interessenten anzusprechen. Je enger daher die Verwendungsgrenzen gezogen werden und je klarer die Verpflichtung ist, sie zu respektieren, desto nachhaltiger wird allen Kommerzialisierungsbestrebungen der Boden entzogen. Eine strikte Begrenzung reduziert die Verarbeitungsmöglichkeiten zwangsläufig auf den explizit formulierten, verbindlich umschriebenen Erhebungszweck und entwertet damit das potentielle Informationskapital. Genau diese Konsequenz hat die vielfachen Versuche ausgelöst, die Zweckbindung wenigstens aus dem nicht-öffentlich Bereich herauszuhalten. Doch weder die wieder und wieder behauptete Unvereinbarkeit der Zweckbindung mit dem "Wesen" der Verarbeitungsaktivitäten nicht-öffentlicher Stellen, noch deren zuweilen kategorisch postulierte Verfassungswidrigkeit haben letztlich etwas genutzt.

Spätestens seit der EG-Datenschutzrichtlinie ist jede weitere Diskussion überflüssig. Sie reiht die Zweckbindung ausdrücklich in die Leitprinzipien jeder Verarbeitung personenbezogener Daten ein (Art. 6 Abs. 1 Buchst. b) und ist zudem die erste umfassende Verarbeitungsregelung, die primär den nicht-öffentlichen Bereich anspricht. Wie groß der Widerstand gegen die Zweckbindung trotzdem noch ist, zeigt sich an den Vorschlägen zur Novellierung des Bundesda-

tenschutzgesetzes. Die Zweckbindung wird zwar nicht mehr grundsätzlich verworfen, aber mit Hilfe einer Vielzahl von Einzelvorschriften heruntergespielt. Gemeinschaftskonform ist jedoch nur eine Regelung, die nicht darauf abzielt, die Zweckbindung zu entkräften, sondern diese, im Gegenteil, uneingeschränkt bestätigt.

Die Zweckbindung kann freilich letztlich nur weiterhelfen, wenn sie nicht zur Disposition steht. Ob sie also eine wirklich taugliche Kommerzialisierungsbarriere ist, entscheidet sich am Stellenwert der Einwilligung. Solange das Einverständnis der Betroffenen ausreicht, um die gesetzlichen Verarbeitungsvorgaben, damit aber auch die Zweckbindung, jedenfalls weitgehend abzulösen, bleibt die Einwilligung ein ebenso naheliegendes wie einfaches Mittel, um den vom Gesetz versagten Verarbeitungsspielraum zurückzugewinnen. Deutlicher denn je zeigt sich daher, daß kein Weg mehr an einer Auseinandersetzung mit Bedeutung und Tragweite der Einwilligung vorbeiführt. Die Kommerzialisierung zwingt, so gesehen, eine längst fällige Debatte nachzuholen. Arbeitnehmer und Arbeitnehmerinnen sind, um noch einmal daran zu erinnern, genausowenig wie Bank- oder Versandhauskunden nur deshalb plötzlich in der Lage, ihre Interessen geltend zu machen, weil nicht der Abschluß von Verträgen, sondern die Verwendung ihrer Daten auf dem Spiel steht.

Die Erfahrungen im Versicherungsbereich oder bei der Verarbeitung von Arbeitnehmerdaten lassen sich allerdings nicht kurzerhand auf die Veräußerung der eigenen Daten übertragen. Zur Diskussion steht eben nicht, wie die Betroffenen am ehesten vor der Gefahr einer Übervorteilung geschützt, also ihre Chancen auf einen "angemessenen" Preis für ihre Daten gesichert werden können. Der Akzent liegt vielmehr ganz auf den Folgen der Vermarktung für die Funktionsfähigkeit der informationellen Selbstbestimmung. Noch genauer: Maßstab aller Überlegungen zur Zulässigkeit der Kommerzialisierung und die Rolle der Einwilligung müssen die strukturellen Konsequenzen einer durch die Einwilligung legitimierten Veräußerung der eigenen Daten für eine Gesellschaft sein, die sich auf die Kommunikations- und Partizipationsfähigkeit auch und gerade der Betroffenen gründet.

Die Zukunft der informationellen Selbstbestimmung und damit des Datenschutzes entscheiden sich mithin an der Bereitschaft, der

Kommerzialisierung Grenzen zu setzen und sich zugleich von der Vorstellung einer tendenziell unbeschränkten Legitimationswirkung der Einwilligung zu lösen. Eine Alternative zu einer strikten Zweckbindung, die mit einer ebenso strikten Einschränkung der Einwilligung in die Veräußerung der eigenen Daten verknüpft werden muß, gibt es infolgedessen nicht. Genauso steht allerdings der Preis für jede weitere Verzögerung oder Verwässerung der Revision der Datenschutzgesetze fest. Wo die Veräußerlichkeit der Daten widerspruchslos akzeptiert wird, endet auch der Datenschutz. Oder, um noch einmal auf Eco zurückzukommen: Wenn Reflexionen zur Verarbeitung personenbezogener Daten auf Überlegungen über ihre bestmögliche Vermarktung reduziert werden, ist es sinnlos, sich mit der informationellen Selbstbestimmung und dem Datenschutz weiter zu beschäftigen. Beide sind dann endgültig obsolet und beide nur noch Erinnerungsposten an eine abgeschlossene Epoche.

Datenschutz-Audit

Alexander Roßnagel

1. Die Idee eines Datenschutz-Audits

Das Datenschutz-Audit ist ein neues Instrument des Datenschutzes: Durch die abgesicherte Möglichkeit, mit seinen Datenschutzanstrengungen werben zu können, soll der Datenverarbeiter veranlaßt werden, freiwillig ein Datenschutz-Managementsystem zu errichten, das zu einer kontinuierlichen Verbesserung des Datenschutzes beiträgt.

Das Datenschutz-Audit ist eine Antwort auf das gestiegene Datenschutzbewußtsein bei der Verarbeitung personenbezogener Daten bei Anwendern und Nutzern. Datenschutz ist ein entscheidender Akzeptanzfaktor für alle Formen des elektronischen Handels und der elektronischen Verwaltung. Nach einer repräsentativen Umfrage, die das Freizeit-Forschungsinstitut in Hamburg bei 3000 Personen über 14 Jahren zum Thema Multimedia und Datenschutz durchgeführt hat, würden gern 46% aller Befragten und 57% der Berufstätigen behördliche Teledienste in Anspruch nehmen.[1] Ein Drittel der Bevölkerung (33% der Befragten) würde gern online Informationen über Produkte und Dienstleistungen erhalten und eventuell auch kaufen und in Anspruch nehmen. Mehr Bürger sogar (37% der Befragten) würden auf diese Weise Reiseinformationen abrufen und Reisen organisieren. Allerdings sind 47% der Bevölkerung der Ansicht, es werde derzeit zu wenig für den Datenschutz getan. Diese Einschät-

[1] Die folgenden Angaben stammen aus Opaschowski/Duncker, Der gläserne Konsument? Multimedia und Datenschutz, Hamburg 1998.

zung nimmt mit steigender Schulbildung zu und wird unter den Personen mit Hochschulabschluß sogar von 60% vertreten. Für die Zukunft fordern sie - auch angesichts der neuen Möglichkeiten der Multimediatechnik - eine Verbesserung des Datenschutzes. Mit 55% von allen Befragten votiert die Mehrheit für einen Ausbau des Datenschutzes. Weitere 30% würden ihn zumindest auf dem Niveau von heute halten und lediglich jeder Zwölfte (8% der Befragten) meint, dem Datenschutz könnte gern weniger Bedeutung beigemessen werden. Aus diesen Ergebnissen ist zu schließen: "Wer mit den ihm anvertrauten Informationen nicht sorgsam umgehen kann, wird in der Informationsgesellschaft des 21. Jahrhunderts einen schweren Stand haben". Es wird vor allem eine Aufgabe der Anbieter von Telediensten sein, "alle wirksamen Schutzmaßnahmen für ihre Konsumenten zu treffen, um die Akzeptanz der neuen Medienwelt nicht durch eine wie auch immer geartete Datenunsicherheit im Keim zu ersticken". Und - so ist zu ergänzen - angesichts der großen Unkenntnis und Verunsicherung wird es auch darauf ankommen, die Anstrengungen für den Datenschutz zu vermitteln. Für beides - für die Datenschutzanstrengungen und deren Vermittlung - könnte das Datenschutz-Audit ein hilfreiches Instrument sein.

2. Ziele eines Datenschutz-Audits

Entsprechend seinem Vorbild, dem Umweltschutz-Audit, sollte das Datenschutz-Audit vier zentrale Ziele verfolgen, die vorab zum besseren Verständnis der nachfolgenden Erörterung von Einzelaspekten des Datenschutz-Audits genannt werden:

2.1 Stärkung der Selbstverantwortung und Stimulierung von Wettbewerb

Das Datenschutz-Audit sollte in erster Linie ein geeignetes Instrument sein, die Selbstverantwortung des Datenverarbeiters für den Datenschutz zu fordern und zu fördern. Datenschutz ist ein immer wichtiger werdendes Qualitätsmerkmal für Anwendungen der Informations- und Kommunikationstechniken, das als Wettbewerbsvorteil verstanden wird. Das Datenschutz-Audit sollte daher in nachprüfbarer Weise ermöglichen, mit Datenschutz und Datensicherheit

zu werben. Um ein hohes Datenschutzniveau kontinuierlich sicherzustellen, ist ein Datenschutz-Managementsystem einzurichten. Dessen wiederkehrende Überprüfung und Verbesserung wird durch rechtliche Verfahrensregeln abgesichert. Für den Datenverarbeiter ist entscheidend, daß das Datenschutz-Audit sich den Besonderheiten seines Betriebes anpaßt und ihm Möglichkeiten eröffnet, mit dem positiven Ergebnis der Überprüfung die Kommunikation mit der Öffentlichkeit zu suchen und mit ihm zu werben. Das Datenschutz-Audit soll die datenverarbeitenden Stellen belohnen, die bei der Konzeption ihres Angebots datenschutzrechtliche Belange berücksichtigen, und für alle anderen marktgerechte Anreize schaffen, dies ebenso zu tun.[2]

2.2 Verringerung des Vollzugsdefizits

Nicht nur im Umweltschutzrecht, auch im Datenschutzrecht besteht ein erhebliches Vollzugsdefizit. Die öffentlichen Datenschutzbeauftragten und die Aufsichtsbehörden sind durch die weltweite Vernetzung und die ubiquitäre Verwendung von Informations- und Kommunikationstechniken überfordert. Hier könnte das Datenschutz-Audit zu einer Entlastung beitragen. Mit dem von ihm geschaffenen Anreiz zur Selbstkontrolle verringert das Datenschutz-Audit Defizite in der Einhaltung des geltenden Datenschutzrechts. Es etabliert neue Formen und Instanzen der Datenschutzkontrolle, indem es interne Kontrollverfahren vorsieht, externe private Gutachter einbezieht und der kritischen Öffentlichkeit Kontrollinformationen bietet und Bewertungsmöglichkeiten eröffnet. Maßstab der Prüfung dieser Kontrollinstanzen sind die für die Datenverarbeitung geltenden Anforderungen des Datenschutzrechts. Da das Datenschutz-Audit andere Voraussetzungen[3] und Folgen[4] aufweist als die behördliche Datenschutzkontrolle, vermag es diese sehr wohl zu ergänzen, nicht aber zu ersetzen.

---

2 Begründung zu § 17 des MDStV; ebenso Engel-Flechsig, DuD 1997, 15; Roßnagel, DuD 1997, 507.

3 Z.B. die freiwillige Teilnahme versus die Durchsetzung von Kontrollen nach §§ 24, 38 Abs. 1 - 4 BDSG.

4 Z.B. Nichtzertifizierung der Datenschutzerklärung versus Beanstandungen und Anordnungen nach §§ 25, 38 Abs. 5 BDSG.

2.3 Kontinuierliche Verbesserung des Datenschutzes und der Datensicherung

Beim Umweltschutz-Audit haben die teilnehmenden Unternehmen nicht nur die einschlägigen Vorschriften einzuhalten, sondern auch auf eine angemessene kontinuierliche Verbesserung des betrieblichen Umweltschutzes hinzuwirken, wie sie sich mit der wirtschaftlich vertretbaren Anwendung der besten verfügbaren Technik erreichen läßt.[5] Ebenso sollte das materielle Hauptziel des Datenschutz-Audits die kontinuierliche Verbesserung des Datenschutzes und der Datensicherung sein.[6] Bisher bestehen für die Datenverarbeiter keine Anreize, eigene Anstrengungen zur Verbesserung des Datenschutzes und der Datensicherung zu ergreifen. Das Datenschutz-Audit ermöglicht, solche Anstrengungen zu dokumentieren, zu prüfen und zu prämieren und schafft dadurch einen Marktanreiz, diese zu unternehmen. Es sollte sich daher nicht darauf beschränken, nur die Einhaltung der Datenschutzregelungen zu überprüfen. Diese einzuhalten, ist ohnehin jeder verpflichtet. Zwar wird diese Einhaltung im Datenschutz-Audit erstmals durchgängig extern kontrolliert, doch darf das Bestehen dieser Kontrolle allein noch nicht zu einer besonderen Auszeichnung des kontrollierten Unternehmens führen. Die Auszeichnung ist gerechtfertigt durch überobligationsmäßige Anstrengungen, die das Unternehmen über den gesetzlichen Minimalstandard hinaus unternimmt.

2.4 Datenschutz-Audit als Lernsystem

Das Ziel einer kontinuierlichen Verbesserung kann das Datenschutz-Audit nur erreichen, wenn es als ein Lernsystem verstanden wird. Wie beim Umweltschutz-Audit sollte auch im Datenschutz der Regelungsschwerpunkt auf der Normierung des "Lernprozesses" des Datenschutzmanagementsystems liegen.[7] Dieser Lernprozeß wird dadurch strukturiert, daß der Datenverarbeiter in einer umfassenden Betriebsprüfung eine Bestandsaufnahme der Verarbeitung personen-

---

5 Art. 3 lit a) der EG-UAVO.

6 So auch Berliner Datenschutzbeauftragter, Datenschutz-Bericht 1996, Berlin 1997, 134; Roßnagel, DuD 1997, 507; Königshofen, DuD 1999, 266 ff.

7 S. für das Umweltschutz-Audit z.B. Hemmelskamp/Neuser/Zehnle, ZEW-Wirtschaftsanalysen 1994, 207; Köck, JZ 1995, 646.

bezogener Daten erstellt und die hierfür relevanten Anforderungen des Datenschutzrechts zusammenträgt. Schon allein die dadurch angestoßene Vermehrung und Verbreitung des Wissens um die organisatorischen, technischen und gesetzlichen Rahmenbedingungen, in denen sich die Datenverarbeitung vollzieht, stellt einen positiv zu wertenden Erfolg dar.[8] Die Erkenntnisse aus dieser Bestandsaufnahme fließen in Datenschutzprogramme ein, für die konkrete Ziele, Maßnahmen und Fristen festzulegen sind. Nach Ablauf der Frist wird die Umsetzung dieser Programme überprüft und führt zu deren Fortschreibung. In diese gehen positive und negative Erfahrungen mit der Umsetzung bisheriger Datenschutzmaßnahmen ein, die in reflektierter Form die nächsten Verbesserungsschritte bestimmen. Mit der Strukturierung eines solchen Lernprozesses würde in den Datenschutz ein neues förderliches Element eingefügt. Zwar kann auch der betriebliche Datenschutzbeauftragte als Teil eines betrieblichen Lernsystems verstanden werden. Doch beschränkt sich bei ihm die rechtliche Normierung auf die Institutionalisierung (Bestellungspflicht). Nach der gesetzlichen Zielsetzung bleibt es dem Innenverhältnis zwischen dem Unternehmen und dem Betriebsbeauftragten überlassen, sowohl das Verfahren als auch den Erfolg des innerbetrieblichen Lernprozesses selbst auszugestalten. Das Datenschutz-Audit müßte darüber deutlich hinausgehen, indem es den Lernprozeß strukturiert und über die Belohnung eines bestimmten "Lernerfolgs" diesen indirekt mitnormiert.

3. "Ideengeschichte" des Datenschutz-Audits

Die Programmnorm für ein Datenschutz-Audit im späteren Mediendienste-Staatsvertrag (MDStV) geht zurück auf einen Vorschlag der "Projektgruppe verfassungsverträgliche Technikgestaltung (provet)", den diese im Rahmen eines Gutachtens "Vorschläge zur Regelung von Datenschutz und Rechtssicherheit in Online-Multimedia-Anwendungen" für das Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie unterbreitet hat.[9] Aufgrund die-

---

[8] S. für das Umwelt-Audit ähnlich Führ, Eigenverantwortung oder Öko-Staat? Sicherung der Selbstverantwortung in Unternehmen, in: Roßnagel/Neuser (Hrsg.), Reformperspektiven im Umweltrecht, Baden-Baden 1996, 247.

[9] Das Gutachten stammt vom 15.2.1996 - s. provet, Vorschläge zur Regelung von Datenschutz und Rechtssicherheit in Online-Multimedia-Anwendungen, Gut-

ses Vorschlags war das Datenschutz-Audit in den ersten Entwürfen[10] (§ 13 Teledienstegesetz - TDG)[11] des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) enthalten. Auch der parallel zum IuKDG erarbeitete MDStV sah wortgleich in § 17 die Möglichkeit eines Datenschutz-Audits vor. Während der MDStV diese Vorschrift beibehielt, war sie in der am 15.12.1996 von der Bundesregierung beschlossenen Fassung des IuKDG[12] überraschender Weise[13] nicht mehr zu finden. Eine offizielle Begründung hierfür fehlt. Der MDStV[14] hat das Datenschutz-Audit in seinem § 17 wie folgt geregelt:

> *"Zur Verbesserung von Datenschutz und Datensicherheit können Anbieter von Mediendiensten ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt."*

---

achten für das Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie, Darmstadt 1996, <http://www.provet.org/bib/mmge> oder <http://www.iid.de/iukdg>; der Vorschlag eines Datenschutz-Audits befand sich bereits in einem Eckwerte-Papier zu dem Gutachten vom 15.12.1995. Eine JURIS-Recherche ergab keine Erwähnung des Datenschutz-Audits vor diesem Zeitpunkt. Etwa zur gleichen Zeit wurde auch von Königshofen eine ähnliche Idee ("Datenschutz-Gütesiegel") entwickelt - s. Königshofen, DuD 1999, 267 -, ohne sie allerdings zu publizieren. Der Hinweis von Königshofen, die Idee des "Datenschutz-Gütesiegels" sei schon früher z.B. bei Hassemer, DuD 1995, 449 diskutiert worden, ist unzutreffend. Dort heißt es lediglich: "Es ist jetzt auch die 'Akzeptanz' der neuen Technologien bei Käufern und Wählern, welche auf die datenschutzrechtliche Unbedenklichkeit wie ein Gütesiegel aufmerksam machen könnte".

10 S. den ersten Referentenentwurf vom 28.6.1996.

11 Die Datenschutzvorschriften waren damals noch nicht in einem eigenen Teledienstedatenschutzgesetz (TDDSG) zusammengefaßt, sondern Teil des TDG.

12 BR-Drs. 966/96; BT-Drs. 13/3385.

13 Bachmeier, DuD 1996, 672, stellte noch im November 1996 darüber "keinen politischen Streit" fest und rechnete fest mit der Verabschiedung der Vorschrift im IuKDG. Unverständnis über die Streichung äußert der Berliner Datenschutzbeauftragte (Fn. 5), 135.

14 Der MDStV ist am 1.8.1997 in Kraft getreten.

Ein Gesetz, wie es § 17 Abs. 2 MDStV ankündigt, ist bisher noch nirgendwo erlassen worden. Auch ist bisher weder der Entwurf eines solches Gesetzes noch gar die Arbeit an einem solchen Entwurf bekannt. Zur Etablierung des Datenschutz-Audits wurden neben der erfolgten Regulierung im MDStV drei weitere Regelungsinitiativen unternommen und in Brandenburg sogar eine Initiative umgesetzt:

Am 14.11.1997 hat die Fraktion BÜNDNIS 90/DIE GRÜNEN einen Gesetzentwurf zu einem neuen Bundesdatenschutzgesetz in den Bundestag eingebracht,[15] in dem in § 17 ein Datenschutz-Audit vorgesehen war. Diese Vorschrift ist nahezu wortgleich mit § 17 MDStV. Am 30.10.1998 legte der Landesbeauftragte für den Datenschutz in Schleswig-Holstein den Entwurf eines neuen Landesdatenschutzgesetzes vor, in dessen § 34 Abs. 3 ein Datenschutz-Audit vorgesehen ist. Die Vorschrift lautet:

> *"Datenverabeitende Stellen können ihr Datenschutzkonzept durch die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz prüfen und beurteilen lassen. Das Nähere regelt die Verordnung nach § 5 Absatz 4."* [16]

In Brandenburg ist am 21.12.1998 eine Programmnorm zum Datenschutz-Audit sogar Gesetz geworden.[17] Die Vorschrift des § 11c des neuen Landesdatenschutzgesetzes lautet:

> *"Die öffentlichen Stellen können zur Verbesserung von Datenschutz und Datensicherheit sowie zum Erreichen größtmöglicher Datensparsamkeit ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten sowie das Ergebnis der Prüfung veröffentlichen lassen. Sie können auch bereits geprüfte und bewertete Datenschutzkonzepte und -programme zum Einsatz bringen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt."*

---

15 BT-Drs. 13/9082.

16 Landesbeauftragter für den Datenschutz Schleswig-Holstein, LT-Drs. 14/1738, 80.

17 GVBl. I, 243.

Umsetzungsregelungen, die erst eine Durchführung von Datenschutz-Audits ermöglichen, fehlen aber auch hier.

Von besonderer Bedeutung für die Realisierung eines Datenschutz-Audits dürfte sein, daß das Bundesinnenministerium am 11.3.1999 einen Entwurf eines neuen BDSG vorgelegt hat, der eine Programmnorm für ein Datenschutz-Audit vorsieht. § 9a BDSG-E lautet:

> *"Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt."*

Die Idee eines Datenschutz-Audits stieß von Anfang auf viel Sympathie.[18] Ausgearbeitete Konzepte jedoch fehlten. Ein solches wurde erstmals im September 1997 konkretisiert[19] und inzwischen in einem Gutachten für das Bundesministerium für Wirtschaft und Technologie ausgearbeitet.[20]

4. Vorbild Umweltschutz-Audit

Die Idee eines Datenschutz-Audits geht zurück auf das Umweltschutz-Audit, das in Form einer Verordnung der Europäischen Ge-

---

[18] S. z.B. Ulrich, DuD 1996, 668; Bachmeier, DuD 1996, 673; Engel-Flechsig, DuD 1997,15; Engel-Flechsig, RDV 1997, 66; Berliner Datenschutzbeauftragter (Fn 5), 134 f.; Bizer 1997, 149; Bundestags-Fraktion BÜNDNIS 90/DIE GRÜNEN, BT-Drs. 13/9082; Landesbeauftragter für den Datenschutz Schleswig-Holstein, LT-Drs. 14/1738, 13; Vogt/Tauss, Entwurf für ein Eckwerte Papier der SPD-Bundestagsfraktion: Modernes Datenschutzrecht für die (globale) Wissens- und Informationsgesellschaft, Bonn Oktober 1998, 19; kritisch zum Datenschutz-Audit Drews/Kranz, DuD 1998, 94.

[19] Roßnagel, DuD 1997, 505.

[20] Roßnagel, Datenschutz-Audit, Konzept und Entwurf eines Datenschutz-Audit-Gesetzes, Rechtsgutachten für das Bundesministerium für Wirtschaft und Technologie, 1999.

meinschaft[21] und in Form einer Techniknorm der International Standardization Organisation (ISO)[22] geregelt ist. Die unmittelbar geltende EG-Verordnung wird ergänzt durch das Umweltauditgesetz (UAG)[23] und vier Rechtsverordnungen[24], die zur deren innerstaatlichen Umsetzung ergangen sind.

Durch das Umweltschutz-Audit sollen die Eigenverantwortung des Unternehmens für dessen Umweltauswirkungen und Umweltmanagement gestärkt und Vollzugsdefizite verringert werden. Die Teilnahme an dem Verfahren ist freiwillig. Als Anreiz wird dem erfolgreich teilnehmenden Unternehmen ermöglicht, mit der zertifizierten Umwelterklärung Image-Werbung in der Öffentlichkeit zu betreiben und sich im Wettbewerb von anderen, nicht oder nicht erfolgreich teilnehmenden Unternehmen zu unterscheiden.

Gegenstand des Umweltschutz-Audits sind die Aktivitäten eines Unternehmens an einem Standort. Für diesen Standort geht das Unternehmen eine Selbstverpflichtung ein, die einschlägigen Umweltrechtsvorschriften einzuhalten und das bestehende betriebliche Umweltschutzniveau kontinuierlich zu verbessern. Als anzustrebender Umweltschutzstandard gilt die jeweils wirtschaftlich vertretbare Anwendung der besten verfügbaren Umwelttechnik. Zur Umsetzung der Selbstverpflichtung wird ein Umweltmanagementsystem eingerich-

---

21 EG-Verordnung "über die freiwillige Beteiligung gewerblicher Unternehmen an einem Gemeinschaftssystem für das Umweltmanagement und die Umweltbetriebsprüfung" (EG-UAVO), Nr. 1836/93 des Rates vom 29.6.1993, EG-ABl. Nr. L 168/1.

22 ISO EN DIN 14.001 vom Oktober 1996 sowie weitere Normen der 14.000er Reihe.

23 Gesetz vom 7.12.1995, BGBl I, 1591.

24 Verordnung über das Verfahren zur Zulassung von Umweltgutachtern und Umweltgutachterorganisationen sowie zur Erteilung von Fachkenntnisbescheinigungen nach dem Umweltauditgesetz (UAG-Zulassungsverfahrensverordnung - UAGZVV) vom 18.12.1995, BGBl I, 1841; Verordnung über die Beleihung der Zulassungsstelle nach dem Umweltauditgesetz (UAG-Beleihungsverordnung - UAGBV) vom 18.12.1995, BGBl I, 2013; Verordnung über Gebühren und Auslagen für Amtshandlungen der Zulassungsstelle und des Widerspruchsausschusses bei der Durchführung des Umweltauditgesetzes (UAG-Gebührenverordnung - UAGGebV) vom 18.12.1995, BGBl I, 2014; Verordnung nach dem Umweltauditgesetz über die Erweiterung des Gemeinschaftssystems für das Umweltmanagement und die Umweltbetriebsprüfung auf weitere Bereiche (UAG-Erweiterungsverordnung - UAG-ErwV) vom 3.2.1998, BGBl I, 338.

tet, das in regelmäßigen Abständen in einer von dem Unternehmen selbst durchgeführten Umweltbetriebsprüfung auditiert wird. Die daraus entstehende Umwelterklärung wird von einem externen Gutachter überprüft. Im Falle einer positiven Validierung durch den externen Gutachter wird die Umwelterklärung veröffentlicht und an die zuständige Behörde zur Standortregistrierung im Verzeichnis der am Umweltschutz-Audit teilnehmenden Unternehmen weitergeleitet. Aufgrund der Standortregistrierung ist das Unternehmen dann berechtigt, eine Teilnahmeerklärung für Werbezwecke zu nutzen.

Die bisherigen Erfahrungen mit dem noch jungen Umweltschutz-Audit sind differenziert, aber überwiegend positiv. Es wird von vielen Unternehmen akzeptiert, verändert die unternehmensinternen Strukturen und Aufmerksamkeiten und zeigt erste Verbesserungsergebnisse.[25] Ende 1998 waren 1734 Standorte in Deutschland eingetragen.[26] Die Zugänge zum Standortregister belaufen sich auf circa 40 Neueinträge pro Monat. Aufgrund der UAG-Erweiterungsverordnung ist mit einer weiteren Steigerung der Neuteilnahmen zu rechnen, da durch diese weiteren Branchen die Teilnahme ermöglicht wurde. Als Kosten für die Einführung des Umwelt-Managementsystems einschließlich der betriebsinternen Kosten wurden zwischen 6.000 DM und 800.000 DM angegeben. Als arithmetisches Mittel ergab sich ein Betrag von 102.241 DM.[27] Bezieht man die Einspareffekte auf die Auditkosten, ergibt sich eine Amortisationszeit von durchschnittlich weniger als 1,5 Jahren. Bis Ende 1998 wurden bei einer Durchfallquote von 59,5% 229 Umweltgutachter, davon 33 Umweltgutachterorganisationen zugelassen.

Insgesamt kann das in der gesamten EU geltende Verfahren des Umweltschutz-Audits als Vorbild für die Konzeption eines Datenschutz-Audits genommen werden. Allerdings muß immer wieder geprüft werden, inwieweit es im Detail für die völlig andere Zielsetzung des Datenschutzes als tauglich erscheint.

5. Das Konzept eines Datenschutz-Audits

---

[25] S. "Bericht der Bundesregierung über die Erfahrungen mit dem Vollzug des Umweltauditgesetzes (UAG)" vom 18.6.1998- BT-Drs. 13/11127.

[26] S. Lütkes/Ewer, NVwZ 1999, 20.

[27] S. hierzu die Zusammenfassung im Evaluationsbericht der Bundesregierung, BT-Drs. 13/11127, 7.

Das entscheidende Mittel, um die genannten Ziele zu erreichen, ist die Einführung eines Datenschutz-Managementsystems und dessen wiederkehrende interne und externe Überprüfung und Verbesserung.

5.1 System-Audit

Das Datenschutz-Audit sollte daher als ein System-Audit konzipiert werden. Dagegen griffe ein reines Produkt-Audit viel zu kurz, um die genannten Zielsetzungen erfüllen zu können. Denn dieses setzt eine abschließende Qualifizierung des Produkts voraus. Die Prüfung wäre auf einen ganz spezifischen Gegenstand bezogen, für ein abschließendes Urteil sehr voraussetzungsvoll und müßte bei jeder neuen Version des geprüften Gegenstandes erneut durchlaufen werden.[28] Eine solche Prüfung ist statisch und objektbezogen. Dagegen soll das Datenschutz-Audit prozeßbezogen sein und einen dynamischen Lernprozeß initiieren. In ihm soll die Fähigkeit eines Unternehmens überprüft und prämiert werden, flexibel auf die rasanten Veränderungen der Informations- und Kommunikationstechniken zu reagieren und die sich dadurch immer wieder neu stellenden Herausforderungen für den Datenschutz zu meistern. Daher zielt das Datenschutz-Audit nicht auf die einmalige Evaluierung eines Produkts, sondern auf die Fähigkeit, immer wieder neue Lösungen zu generieren und daher auf die kontinuierliche Verbesserung eines Datenschutz-Managementsystems. Gegenstand des Datenschutz-Audits ist die Funktionsfähigkeit und Zweckmäßigkeit des unternehmensinternen Datenschutz-Managements.[29] Das Datenschutz-Audit soll eine Ressource nutzen, die für den Datenschutz bisher noch nicht genutzt

---

[28] S. für die Datensicherheit z.B. die Produktzertifizierung durch das BSI nach dem BSIG.

[29] So Kothe, Das neue Umweltauditrecht, München 1996, 5 für das Umweltschutz-Audit; für das Datenschutz-Audit Roßnagel, DuD 1997, 509; so dürfte wohl auch die Enquete-Kommission "Zukunft der Medien in Wirtschaft und Gesellschaft - Deutschlands Weg in die Informationsgesellschaft", BT-Drs. 13/11002, 104, zu verstehen sein, wenn sie einen Vorteil des Datenschutz-Audits darin sieht, "dem Nutzer die Überprüfung des Umgangs eines Unternehmens mit personenbezogenen Daten ermöglichen".

wird, nämlich die Möglichkeiten eines Datenschutzmanagements. Dementsprechend ist das Datenschutz-Audit als System-Audit zu konzipieren.

5.2. Freiwilligkeit

Das Datenschutz-Audit sollte freiwillig sein.[30] Für die Unternehmensvertreter, die sich bisher zum Datenschutz-Audit geäußert haben, ist dies eine essentielle Voraussetzung für die Akzeptanz des Datenschutz-Audits.[31] Die Freiwilligkeit führt zwar dazu, daß möglicherweise gerade die Unternehmen nicht am Verfahren teilnehmen, für deren Datenverarbeitung ein großer Verbesserungsbedarf und ein besonderes Interesse in der Öffentlichkeit besteht.[32] Für eine freiwillige Teilnahme sprechen jedoch vor allem zwei Erwägungen: Zum einen läßt die Freiwilligkeit der Beteiligung einen wesentlich größeren Raum für die Formulierung anspruchsvoller Vorgaben, die zu erreichen tatsächlich nicht alle Unternehmen in der Lage sind. Zum anderen widerspräche eine verpflichtende Teilnahme der Systematik des Instruments. Denn wenn die Eigenverantwortlichkeit der Unternehmen gestärkt werden soll, so wäre hierfür kein Raum, wenn die Teilnahme verpflichtend ist. Außerdem kommt der Öffentlichkeit eine entscheidende Rolle zu, indem sie über die Marktnachfrage die Unternehmen zu einer Teilnahme veranlassen soll. Als marktorientiertes Instrument kann das Datenschutz-Audit aber nur funktionieren, wenn die Teilnahme an ihm freiwillig ist. Das Datenschutz-Audit ist gerade kein "Ansatz einer externen Fremdregulierung"[33], sondern ein Instrument der unternehmensinternen Selbstregulierung mit öffentlicher Anerkennung.

---

30 Ebenso Entschließungsantrag der SPD-Bundestagsfraktion, BT-Drs. 13/7936, 5; Vogt/Tauss (Fn 18), 19; Bachmeier, DuD 1996, 680; Roßnagel, DuD 1997, 509; kritisch gegenüber der freiwilligen Teilnahme am Umweltschutz-Audit Führ, EuZW 1992, 471, und ders., NVwZ 1993, 860.

31 S. z.B. VDMA/ZVEI, Schriftliche Stellungnahme zur Anhörung zum IuKDG am 14.5.1997; Arbeitskreis "Datenschutzbeauftragte" im Verband der Metallindustrie Baden-Württemberg (VMI), s. DuD 1999, 281 ff.; Königshofen, DuD 1999, 266 ff.

32 Aus diesem Grund enthält § 14 des Allgemeinen Teils des vorgeschlagenen Umweltgesetzbuchs eine Verpflichtung für Großbetriebe, eine Öko-Bilanz durchzuführen.

33 So aber Drews/Kranz, DuD 1998, 94.

5.3 Angebot an die "Datenschutzvorreiter"

Das Datenschutz-Audit ist ein Angebot zur Auszeichnung der Besten. Zwar wäre es schön, wenn sehr viele datenverarbeitende Stellen zu diesen Besten gehören würden. Doch darf dieses Ziel nicht durch eine Reduzierung der Anforderungen erkauft werden. Das Datenschutz-Audit wird von den "Anspruchsgruppen" - wie Kunden, Vertragspartner, Mitarbeiter, Banken, Versicherungen, Anteilseigner, Behörden, Presse, Parteien und die interessierte Öffentlichkeit - nur dann akzeptiert werden, wenn es ein verläßliches Unterscheidungsmerkmal zwischen hohem und niedrigem Datenschutz- und Datensicherheitsniveau ist. Die bestätigte Datenschutzerklärung muß einen diskriminierenden Aussagewert haben. Die Bestätigung muß zwar grundsätzlich von jedem Unternehmen - bei entsprechenden Anstrengungen - erreicht werden *können*, darf aber nicht von jedem "Datenschutznachzügler" auch tatsächlich erreicht *werden*, sondern muß die "Datenschutzvorreiter" von diesen unterscheiden. Das Datenschutz-Audit setzt daher hohe Anforderungen voraus. Es muß am Markt als Auszeichnung derer verstanden werden, die diesen hohen Maßstab erreichen.

5.4 Umsetzung der Programmnorm des § 9a BDSG-E

Ein Datenschutz-Audit-Gesetz muß die Programmnorm des § 9a BDSG-E beachten. Diese ermöglicht für sich genommen noch kein Datenschutz-Audit, weil die Ausführungsregelungen erst noch durch ein Gesetz geregelt werden müssen. Mit ihr schließt der Gesetzgeber allerdings die Diskussion über das "Ob" eines Datenschutz-Audits ab, setzt sich mit ihr selbst ein Ziel und deutet die Art und Weise der Erfüllung des Programms an. Damit setzt er rechtspolitisch ein Zeichen, an dem sich die interessierten Kreise orientieren können.

Für das eigentliche Datenschutz-Audit-Gesetz ist die Programmnorm rechtlich in keiner Weise bindend. Auch wenn sie dieses ankündigt, ist sie ihm nicht übergeordnet. Es ist wie die Programmnorm im rechtlichen Rang ein Gesetz, das ihr sogar aus zwei Gründen vorgeht: Es ist zum einen ein Spezialgesetz, das nach § 1 Abs. 4 Satz 1 BDSG den Regelungen des BDSG vorgeht. Zum anderen hat es al-

lein schon nach der Lex-Posterior-Regel im Konfliktfall Vorrang vor dem älteren Gesetz.

Allerdings stellt die Formulierung des § 9a BDSG-E einen Kompromiß zwischen den an seiner Entstehung beteiligten Interessen dar und entfaltet damit gewisse politische Bindungswirkungen. Daher sollte diese Grundlage nicht ohne Not verlassen werden. Bei richtiger Interpretation kann diese Vorschrift auch ein passender Anknüpfungspunkt für die Umsetzung des hier entworfenen Konzepts eines Datenschutz-Audits sein.

Die Vorschrift unterscheidet zwei Adressatengruppen und zwei Gegenstandsbereiche. Entscheidend ist der Unterschied zwischen technischen Einrichtungen und Datenschutzkonzepten. Denn deren Überprüfung fordert ganz unterschiedliche Konzepte der Auditierung: Für technische Einrichtungen ist ein Produkt-Audit und für Datenschutzkonzepte, die von einem Datenschutzmanagement umzusetzen sind, ist ein System-Audit erforderlich. Daher müssen zur Umsetzung der Programmnorm des § 9a BDSG-E zwei unterschiedliche Wege verfolgt werden: die Regelung eines Produkt-Audits und die Regelung eines System-Audits.

Beiden Auditformen sind die unterschiedlichen Adressatengruppen zuzuordnen - wenn auch nicht ausschließlich, so doch schwerpunktmäßig. Die Anbieter von Datenverarbeitungssystemen und -programmen bieten technische Einrichtungen an, die in einem Produkt-Audit auf ihren Beitrag zur Verbesserung des Datenschutzes überprüft werden können. Für datenverarbeitende Stellen ist es zwar nicht ausgeschlossen, aber doch eher seltener, daß sie technische Einrichtungen entwickeln, die sie auditieren lassen wollen. Personenbezogene Daten werden dagegen von den datenverarbeitenden Stellen verarbeitet, die für deren Erhebung, Verarbeitung und Nutzung ein Datenschutzkonzept erarbeiten, das in einem System-Audit überprüft werden kann. Auch die Anbieter von Datenverarbeitungssystemen und -programmen können für ihre technischen Einrichtungen ein Datenschutzkonzept entworfen haben. Dieses ist aber in die technische Einrichtung eingegangen und nicht Gegenstand einer gesonderten Prüfung. Es wird im Produkt-Audit mitevaluiert.

Beide Formen des Audits sollten getrennt werden. Es macht wenig Sinn, wenn die vielen tausend Anwender eines Datenverarbeitungssystems oder -programms dieses viel tausendfach auditieren lassen. Vielmehr sollte allein der jeweilige Anbieter für das System oder Programm ein einziges Produkt-Audit durchführen. Die datenverarbeitenden Stellen sollten sich dagegen im Rahmen ihres System-Audits verpflichten, - soweit vorhanden - auditierte Datenverarbeitungssysteme und -programme in ihrer Datenverarbeitung einzusetzen. Das System-Audit wiederum zielt auf eine Überprüfung und Bewertung des Datenschutzmanagementsystems einer datenverarbeitenden Stelle und ist ungeeignet, verläßliche Aussagen über eine technische Einrichtung zu generieren. Das Produkt-Audit für Datenverarbeitungssysteme und -programme kann daher nicht durch ein System-Audit ersetzt werden.

Aus dieser Interpretation der Programmnorm des § 9a BDSG-E ergibt sich folgende Regelungsstrategie: Die Anbieter von Datenverarbeitungssystemen und -programmen sollten die gesetzliche Möglichkeit erhalten, ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten zu lassen sowie das Ergebnis der Prüfung zu veröffentlichen. Zu diesem Zweck sollte das BSIG um den Aspekt des Datenschutzes erweitert werden. In § 4 BSIG ist bereits die Möglichkeit für eine Zertifizierung der Datensicherheit eröffnet. Für den Aspekt des Datenschutzes müßten konkrete Prüfkriterien erarbeitet werden. Zu diesem Zweck könnte in einer Novelle des BSIG eine Ermächtigung zum Erlaß eines Kriterienkatalogs vorgesehen werden. Diese könnte sich an § 16 Abs. 6 SigV orientieren.[34] Danach wäre in der Ermächtigung festzuhalten, daß das Bundesamt für Sicherheit in der Informationstechnik einen Katalog geeigneter Kriterien erstellt und fortführt, anhand derer die Gewährleistung von Datenschutz und Datensicherheit technischer Einrichtungen bewertet werden kann. An der Erstellung und Fortführung des Katalogs sind Experten aus Wirtschaft und Wissenschaft zu beteiligen. Die jeweils gültige Fassung wird im Bundesanzeiger veröffentlicht.

---

[34] S. zu dieser Vorschrift Roßnagel/Pordesch in: Roßnagel (Hrsg.), Recht der Multimedia-Dienste, Kommentar zum Informations- und Kommunikationsdienste-Gesetz und zum Mediendienste-Staatsvertrag, München 1999, § 16 SigV, Rn. 111.

Datenverarbeitende Stellen sollten entsprechend § 9a BDSG-E die gesetzliche Möglichkeit erhalten, ihre Datenschutzkonzepte durch unabhängige und zugelassene Gutachter prüfen und bewerten zu lassen sowie das Ergebnis der Prüfung zu veröffentlichen. Da ein Datenschutzkonzept allein als Papierdokument wenig aussagekräftig ist, kann der Begriff des Datenschutzkonzepts zur Verbesserung von Datenschutz und Datensicherheit nur so gemeint sein, daß er neben der programmatischen Formulierung des Konzepts auch dessen organisatorische Ausprägung und Umsetzung durch konkrete Maßnahmen beinhaltet. In diesem Sinn entspricht das Datenschutzkonzept der Formulierung einer Datenschutzpolitik, deren Konkretisierung in einem Datenschutzprogramm und organisatorischen Umsetzung in einem Datenschutzmanagementsystem. Die Auditierung dieses Datenschutzkonzepts kann in der Form erfolgen, daß die datenverarbeitende Stelle eine interne Datenschutzbetriebsprüfung durchführt, als deren Ergebnis sie eine Datenschutzerklärung erstellt und diese von einem unabhängigen und zugelassenen Datenschutzgutachter prüfen und bewerten läßt.

6. Kriterien

Ziel der Prüfung ist es, das Datenschutzmanagement danach zu bewerten, ob es für die jeweilige Anwendung geeignet und effektiv ist, die Einhaltung des geltenden Datenschutzrechts sicherzustellen und eine kontinuierliche Verbesserung des Datenschutzes zu erreichen. Die Prüfung verwendet also zwei Maßstäbe: einen objektiven, für alle gleichen Maßstab und einen subjektiven, den der einzelne Anbieter nach seinen individuellen Möglichkeiten bestimmt.

6.1 Objektive Kriterien

Der objektive Maßstab, der für alle Unternehmen und Anwendungen gleichermaßen als Minimalstandard zugrunde gelegt wird, sind die Vorschriften des Datenschutzrechts. Da diese für alle Teilnehmer gleich sind, wird ein hohes Maß an Vergleichbarkeit und Wettbewerbsgerechtigkeit sichergestellt. Durch diesen Maßstab wird das Datenschutz-Audit zu einem Instrument innerbetrieblichen Gesetzesvollzugs.

Viele Vorschläge wollen die Datenschutzprüfung auf die Rechtmäßigkeitskontrolle beschränken.[35] Dies kann aber nicht das einzige Kriterium für ein freiwilliges, wettbewerbsorientiertes öffentliches Datenschutz-Audit sein. Allein für die Erfüllung der ohnehin bestehenden Pflicht, die Datenschutzgesetze einzuhalten, kann es keine besondere Anerkennung geben. Das Datenschutz-Audit soll die besonderen Anstrengungen eines Anbieters von Telediensten mit einer Werbemöglichkeit prämieren. Es darf keine Auszeichnung für Selbstverständliches sein. Die Rechtmäßigkeitskontrolle ist daher ein notwendiger Bestandteil eines jeden Datenschutz-Audits. Denn die Bestätigung für besondere Anstrengungen im Datenschutz setzt voraus, daß die geltenden Datenschutzanforderungen eingehalten werden. Die Gesetzeskonformität des Angebots ist aber noch kein hinreichender Maßstab für ein Datenschutz-Audit. Hinzu kommen müssen freiwillige, individuell festgelegte, aber über das Normale hinausgehende Anstrengungen zur Verbesserung des Datenschutzes.

Soweit das Datenschutzrecht klare Anforderungen an die datenverarbeitende Stelle enthält, ist die Feststellung des objektiven Prüfungsmaßstabs kein Problem. Wie aber ist zu verfahren, wenn das Datenschutzrecht keine klaren und eindeutigen Anforderungen enthält? Was soll objektiver Maßstab sein, wenn das Recht etwa statt präziser Handlungs- oder Gestaltungsanforderungen nur ein Optimierungsziel nennt und dies gar noch unter den Vorbehalt der Zumutbarkeit stellt. Ein solches Ziel ist zum Beispiel in § 3 Abs. 4 TDDSG und § 12 Abs. 5 MDStV - und ähnlich in § 3a BDSG-E - formuliert: "Die Gestaltung und Auswahl technischer Einrichtungen für Teledienste hat sich an dem Ziel, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen, auszurichten."

Die abstrakt rechtsdogmatisch zutreffende Feststellung, daß es rechtlich ein richtiges Ergebnis in der Konkretisierung dieser Norm geben muß, wird den Bedingungen der vollzugspraktischen Durchsetzung

---

[35] So z.B. der Arbeitskreis "Datenschutzbeauftragte" im Verband der Metallindustrie Baden-Württemberg (VMI), DuD 1999, 281 ff. und der Entwurf des Landesdatenschutzbeauftragen Schleswig-Holstein - s. zu diesem Kap. 2. Für die Vorabüberprüfung von Verfahren in der Landesverwaltung mag die Beschränkung einen Sinn machen, wenn auch für diese eine kontinuierliche überobligationsmäßige Verbesserung des Datenschutzes erstrebenswert wäre.

der Optimierungen und Abwägungen nicht gerecht. Über die für die Feststellung der Belange und deren Gewichtung notwendigen Informationen verfügt fast ausschließlich allein die datenverarbeitende Stelle. Diese wird der Gutachter nicht gegen die datenverarbeitende Stelle in ausreichendem Maß erheben können. Er ist auf die Informationen angewiesen, die die datenverarbeitende Stelle ihm präsentiert. Diese Informationen werden in der Regel die Konkretisierung des Optimierungsziels oder der Abwägung durch die Stelle und nicht mögliche Alternativkonkretisierungen des externen Gutachters stützen. Ohne umfangreiche eigene Aufklärungen wird der Datenschutzgutachter deren Feststellungen und Gewichtungen selten widerlegen können. Dem Charakter des Datenschutz-Audits als eines freiwilligen Instruments zur Stärkung der Selbstverantwortung des Datenverarbeiters würde es jedoch nicht entsprechen, dem Datenschutzgutachter richterliche Aufklärungs- und Entscheidungskompetenzen zuzuschreiben. Vielmehr ist für das Datenschutz-Audit das Zusammenspiel von objektiven Mindestkriterien und subjektiven Kriterien einer kontinuierlichen Verbesserung des Datenschutzniveaus fruchtbar zu machen.

Wenn auf diese Weise im Rahmen des objektiven Kriteriums letztlich nur ein Mindeststandard an Optimierung und Abwägung durchgesetzt werden kann, ist dies im Rahmen des Datenschutz-Audits kein Nachteil. Denn eine Optimierung des Datenschutzes oder eine Abwägung zugunsten von mehr Datenschutz wird beim subjektiven Kriterium berücksichtigt. Diese hängen ohnehin von der Zumutbarkeit, von der subjektiven Möglichkeit, letztlich von den individuellen Umständen ab. Wenn diese nach subjektiver Leistungsfähigkeit befördert werden, entspricht dies genau dem Charakter und der Zielsetzung des Datenschutz-Audits.

6.2 Subjektive Kriterien

Der subjektive, auf dem objektiven aufbauende Maßstab ist die Selbstverpflichtung zur kontinuierlichen Verbesserung des Datenschutzes oberhalb datenschutzrechtlicher Pflichten. In Orientierung am Umweltschutz-Audit müßte sich das Unternehmen zwar zum Einsatz der besten, verfügbaren Technik und Organisation verpflichten. Durch die Anbindung dieser Verpflichtung an die "wirt-

schaftliche Vertretbarkeit" ist die jeweilige Verbesserung des Datenschutzes jedoch in die Verantwortung des Unternehmens gestellt. Im einzelnen stellt das Unternehmen im Datenschutzprogramm einen Maßnahmenkatalog auf und legt für die einzelnen Maßnahmen Durchführungsfristen fest. Der Prüfungsmaßstab besteht dann darin festzustellen, wie hoch der Grad der Übereinstimmung zwischen geplanten und durchgeführten Maßnahmen ist. Für die "Übererfüllung" der gesetzlichen Anforderungen wird also gerade kein objektiver Maßstab angelegt.[36] Vielmehr bestimmen die Unternehmen selbst, um wieviel sie ihre Datenschutzanstrengungen über das rechtlich geforderte Minimum hinaus verbessern wollen.

Ziele, die durch solche Anstrengungen immer besser erreicht werden können, sind etwa die datenschutzgerechte Organisation von Abläufen wie die organisatorische Trennung von Zahlung, Lieferung und Service oder der Verarbeitung von Verbindungs-, Nutzungs- und Abrechnungsdaten, der Schutz vor übereilter Einwilligung, die Unterrichtung der Betroffenen, die Organisation von Auskunft, Berichtigung, Sperrung und Löschung, die Verwendung als datenschutzkonform zertifizierter technischer Einrichtungen, die Erforschung und Fortentwicklung von datenschutzgerechten Dienstleistungen und Produkten oder die Integration von Datenschutz und Datensicherheit in Produkten.

Als solche Anstrengungen im Rahmen einer zusätzlichen kontinuierlichen Verbesserung des Datenschutzes sind auch Verbesserungen anzuerkennen, datenschutzrechtliche Zielbestimmungen und Optimierungsgebote besser zu erfüllen oder Abwägungen stärker zugunsten des Datenschutzes ausfallen zu lassen. Diese Zielsetzungen und ihre Konkretisierung in Form von Prinzipien für die Systemherstellung, Systemauswahl, Systemkonfiguration und Anwendung sind zwar rechtlich vorgegeben und fallen somit unter die Einhaltung von Datenschutzregelungen. Sie können aber im Rahmen des Datenschutzrechts mehr oder minder gut erreicht werden. Ihre optimale Erfüllung sicherzustellen, sollte eine Hauptfunktion des Datenschutz-Audits sein.[37]. Wer hier einen höheren Aufwand betreibt als andere,

---

[36] Dies jedoch unterstellen Drews/Kranz, DuD 1998, 94, und kritisieren diese falsche Annahme.

[37] S. hierzu für § 3 Abs. 4 TDDSG Bundesrat, BT-Drs. 13/7385, 57; s. allgemein Roßnagel, DuD 1997, 508.

verdient eine Auszeichnung. Insgesamt sollte diese Funktion des Datenschutz-Audits darin gesehen werden, "die Ziele der Dateneinsparung und eines hohen Datenschutzniveaus durch Stärkung der unternehmerischen Selbstverantwortung, der Transparenz und des Wettbewerbs zu erreichen".[38]

Der konkrete subjektive Maßstab ergibt sich aus der Datenschutzpolitik und deren Konkretisierung in einem Datenschutzprogramm. Für die Formulierung der Datenschutzpolitik ist es nicht notwendig, daß jeder Anbieter die Prinzipien und Leitlinien, denen er sein Unternehmen verpflichten will, jeweils immer wieder selbst erarbeitet. Vielmehr wäre dies der geeignete Ort für eine Selbstregulierung der Branchen. Für den Bereich der Multimediadienste könnten etwa die "Prinzipien und Leitlinien zum Datenschutz bei Multimediadiensten" des Arbeitskreises "Datenschutz-Audit Multimedia" als Vorbild dienen.[39] Jeder einzelne Anbieter könnte diese als Datenschutzpolitik seines Unternehmens übernehmen oder sie seinen spezifischen Verhältnissen anpassen. Er könnte sie weiter zur Orientierung wählen, wenn er in seinem Datenschutzprogramm für einen bestimmten Zeitraum die Maßnahmen festlegen muß, mit denen er selbstgesteckte Ziele erreichen will.

Bei der Prüfung des subjektiven Maßstabs ist in der Datenschutzbetriebsprüfung zu kontrollieren, ob die im Datenschutzprogramm selbstgesteckten Ziele erreicht werden konnten, festzustellen, an welchen Gründen eine Erfüllung der Ziele scheiterte, und ein Datenschutzprogramm für die nächste Audit-Periode aufzustellen. Dieses Datenschutzprogramm muß ein in sich geschlossenes Konzept enthalten, wie das Datenschutzmanagementsystem die selbstgewählten Prinzipien und Leitlinien für den Datenschutz umsetzt. Es darf sich an der individuellen Leistungsfähigkeit der datenverarbeitenden Stelle ausrichten, muß aber als Entwicklungskonzept einer kontinuierlichen Verbesserung des Datenschutzes überzeugen. Dies festzu-

---

[38] S. provet (Fn 9), Begründung zu § 11 des vorgeschlagenen Multimedia-Datenschutz-Gesetzes; ebenso Begründung zu § 17 MDStV; Bachmeier, DuD 1997, 680; Engel-Flechsig, DuD 1997, 15; Vogt/Tauss (Fn 18), 19.

[39] S. die Dokumentation der Prinzipien und Leitlinien in DuD 1999, 285 ff., i.E.; s. auch <http://www.gdd.de> und <http://www.oetb.de/ mulimed. htm> die Prinzipien und Leitlinien können in der Newsgroup <d.soc. datenschutz> diskutiert werden.

stellen, ist eine Aufgabe des Datenschutzgutachters. Ihm kommt daher eine besondere Bedeutung für die Vertrauenswürdigkeit des gesamten Auditsystems zu.

7. Verfahren

Das Verfahren des Datenschutz-Audits kann weitgehend entsprechend dem Vorbild des Umweltschutz-Audits bestimmt werden. In Anlehnung an dieses sollte das Datenschutz-Audit in neun Schritten durchgeführt werden:

1. Das Unternehmen beginnt das Datenschutz-Audit damit, daß es eine *Datenschutzprüfung* durchführt. Diese erbringt für jeden Teledienst eine Bestandsaufnahme des Status der Verarbeitung personenbezogener Daten und des Status geltender Datenschutzregeln.

2. Nach dieser Bestandsaufnahme verpflichtet sich der Anbieter schriftlich zu einer das gesamte Unternehmen betreffenden *Datenschutzpolitik.*

3. Auf dieser Grundlage erstellt der Anbieter ein *Datenschutzprogramm* mit den konkreten Datenschutzzielen und dem Katalog konkreter Maßnahmen und dem Fristenplan zur Umsetzung der Datenschutzpolitik für die jeweilige Anwendung.

4. Parallel zum Datenschutzprogramm wird ein *Datenschutzmanagementsystem* eingerichtet, das die Organisationsstruktur, die Zuständigkeiten sowie die Verfahren, Abläufe und Mittel zur Verwirklichung der Datenschutzpolitik festlegt.

5. In periodischen Abständen führt das Unternehmen selbst eine *Datenschutzbetriebsprüfung* als systematische und dokumentierte Analyse durch, ob Organisation, Management und Betriebsabläufe mit der Datenschutzpolitik und dem Datenschutzprogramm übereinstimmen und die angestrebte Verbesserung des Datenschutzes erreicht haben.

6. Als Ergebnis der jeweiligen Betriebsprüfung verfaßt das Unternehmen eine *Datenschutzerklärung*.
7. Anschließend prüft und zertifiziert ein zugelassener unabhängiger *Datenschutzgutachter* die Datenschutzerklärung.

8. Im Falle einer positiven Validierung durch den externen Datenschutzgutachter wird die Datenschutzerklärung veröffentlicht und an die zuständige Behörde zur *Registrierung* im Verzeichnis der am Datenschutz-Audit teilnehmenden Unternehmen weitergeleitet.

9. Aufgrund der Registrierung ist das Unternehmen berechtigt, eine *Teilnahmeerklärung* und ein Datenschutzzeichen für Werbezwecke zu nutzen.

Um die Kosten eines Datenschutz-Audits in Grenzen zu halten, bietet es sich an, die Fachkompetenz im eigenen Unternehmen für die Durchführung des Audits zu nutzen. Vor allem drängt es sich auf, dem betrieblichen Datenschutzbeauftragten hierbei eine zentrale Rolle einzuräumen.[40] Denn zwischen seinen Aufgaben und denen des Datenschutz-Audits bestehen viele Parallelen.[41] Das Unternehmen muß sich in seiner Datenschutz-Politik verpflichten, die einschlägigen Datenschutz-Vorschriften einzuhalten und den Datenschutz kontinuierlich zu verbessern. Die zentrale Aufgabe des betrieblichen Datenschutzbeauftragten gemäß § 37 BDSG ist es, die Einhaltung datenschutzrechtlicher Vorschriften sicherzustellen.[42] Viele Teilaufgaben, die er in diesem Rahmen zu erfüllen hat, können auch für die Vorbereitung des Audits und die interne Betriebsprüfung genutzt werden.

8. Fazit

Das Datenschutz-Audit ist ein neues, hoffnungsvolles Instrument des Datenschutzes. Über den Anreiz der Werbung ("Tue Gutes und rede darüber") und den Wettbewerbseffekt der Teilnahme von Konkur-

---

40 Ebenso der Arbeitskreis "Datenschutzbeauftragte" im Verband der Metallindustrie Baden-Württemberg (VMI), DuD 1999, 281 ff.

41 S. hierzu ausführlich Roßnagel, DuD 1997, 513 f.

42 S. Engel-Flechsig, DuD 1997, 15; ders., RDV 1997, 67.

renten könnte eine Selbstverpflichtung und Selbstkontrolle der Unternehmen zu einer kontinuierlichen Verbesserung des Datenschutzes genutzt werden. Dadurch könnte die behördliche Kontrolle durch Datenschutzbeauftragte und Aufsichtsbehörden unterstützt und entlastet werden. Eine rechtliche Regelung des Datenschutz-Audits versucht, im Rahmen einer Kontextsteuerung das Ziel einer kontinuierlichen Verbesserung des Datenschutzes nicht durch Ge- und Verbote, sondern mit leichter Hand durch die freiwillige Selbstregulation der Wirtschaftseinheiten zu erreichen. Die rechtliche Rahmensetzung schafft die Voraussetzungen für die Zielgerechtigkeit des Verfahrens und die Vergleichbarkeit der Kriterien und Ergebnisse. Das Datenschutz-Audit ist ein Instrument zur Erfüllung der Strukturverantwortung des Staates.[43] Dieser könnte er gerecht werden, ohne öffentliche Haushalte zu belasten.[44]

[43] S. hierzu näher Roßnagel, ZRP 1997, 26 ff.

[44] Soweit öffentliche Aufgaben wie die Zulassung der Gutachter und die Registrierung der Teilnehmer nicht auf private Träger übertragen werden, können die dadurch entstehenden Kosten durch Gebühren voll abgedeckt werden.

Vorabkontrolle durch behördliche und betriebliche Datenschutzbeauftragte

Hansjürgen Garstka

Mit der Vorabkontrolle, die nach Art. 20 der Europäischen Datenschutzrichtlinie bei "Verarbeitungen mit spezifischen Risiken für die Rechte und Freiheiten der Personen" durchgeführt werden muß, erhalten die behördlichen und betrieblichen Datenschutzbeauftragten, aber auch der Bundesbeauftragte und die Landesdatenschutzbeauftragten sowie die Aufsichtsbehörden neue Aufgaben, die geeignet sind, sie aus ihrer in letzter Zeit (auch bei dieser Veranstaltung) heftig kritisierten reaktiven Rolle herauszuführen. Bei der Umsetzung stellen sich allerdings schwierige, insbesondere die Reichweite und die einzusetzenden Methoden betreffende Fragen.

Gesetzlicher Ausgangspunkt

Die Vorabkontrolle ist die "kleine Münze" der Auditierung. Es geht hierbei nicht um die Auszeichnung positiver Aspekte der geplanten Verarbeitungen, sondern um die Überprüfung, ob sich die Vorhaben im gesetzlich vorgegebenen Rahmen unter Einbeziehung der möglichen Grundrechtsgefährdungen halten. Im Gegensatz zur "Kür" des Audits stellt die Vorabkontrolle die Pflichtübung dar.

Nach Art. 20 der Richtlinie legen die Mitgliedsstaaten fest, welche Verarbeitungen spezifische Risiken für die Rechte und Freiheiten einer Person beinhalten können und sie tragen dafür Sorge, daß diese Verarbeitungen vor ihrem Beginn überprüft werden. Die Vorabprü-

fungen sind zwar zunächst durch die Kontrollstellen, also den Bundes- und die Landesbeauftragten bzw. die Aufsichtsbehörden durchzuführen. Anstelle der Kontrollstellen kann die Vorabkontrolle aber auch "durch den Datenschutzbeauftragten" erfolgen, wobei nach der Diktion der Richtlinie die (internen) betrieblichen und behördlichen Datenschutzbeauftragten gemeint sind. Es besteht zwar nach der Richtlinie keine Verpflichtung, daß nach dem nationalen Recht derartige interne Datenschutzbeauftragte zu benennen sind. Da diese Institutionen jedoch von Deutschland in die Richtlinie eingebracht wurden, wird es sie nach dem neuen deutschen Datenschutzrecht geben, wie immer dieses aussehen wird. Die Kontrollstellen bleiben ebenfalls nicht unbeteiligt: Die Datenschutzbeauftragten haben diese "im Zweifelsfall zu konsultieren", und sie werden dies - auch zur eigenen Absicherung - häufig tun.

Die Vorgabe der Richtlinie ist in den Entwürfen des Bundesinnenministeriums für das Bundesdatenschutzgesetz in der vergangenen Legislaturperiode nur auf minimalistische Weise umgesetzt worden: Die §§ 4 d Abs. 6 und 7 BDSG sahen vor, daß nur automatisierte Dateien nach Abs. 4 und 5 dieser Vorschrift (betrifft nur die Fremdverarbeiter) und sensible Daten nach Art 8 der Richtlinie (medizinische Daten, Daten über weltanschauliche Gesinnung bis hin zu Daten über Sexualverhalten), soweit sie besondere Risiken aufweisen, der Vorabkontrolle unterliegen sollten.

Der Gesetzentwurf des Abgeordneten Such und der Fraktion Bündnis 90/Die Grünen (Bundestagsdrucksache 13/9082) ging erheblich weiter und lehnte sich zum Teil an das niedersächsische Datenschutzgesetz an, welches als einziges Datenschutzgesetz bereits vor Inkrafttreten der Richtlinie eine Vorabkontrolle kannte. Dieser Entwurf sieht die Vorabkontrolle in allen Fällen vor, in denen spezifische Risiken für die in § 1 Abs. 1 genannten Grundrechte wie die Privatsphäre und das Recht auf informationelle Selbstbestimmung oder - eine wichtige Ergänzung ohne Vorgabe durch die Richtlinie - "für die Wirkungsmöglichkeiten demokratischer Organe" bestehen (§ 20 Abs. 1). Danach hat also die Vorabkontrolle über den Schutz des Einzelnen hinaus auch den gesellschaftspolitischen Kontext zu berücksichtigen, in dem das Verfahren stattfindet.

Die Vorabkontrolle soll in der Form einer Technikfolgenabschätzung stattfinden. Die Kontrollinstanz ist in jedem Fall zu beteiligen. Darüber hinaus sind auch hierfür zugelassene Verbände zur Verwirklichung der Grundrechte zu beteiligen, wobei die Einbindung dieser Verbände auch im privaten Bereich erfolgen soll. Des weiteren wird die Veröffentlichung des Ergebnisses und der Begründung durch die verantwortliche Stelle vorgeschrieben.

Die neuen Landesgesetze, das kürzlich in Kraft getretene hessische sowie die Entwürfe in Schleswig-Holstein und Brandenburg (Stand November 1998), enthalten bereits Regelungen zur Vorabkontrolle. Allerdings ist danach (im öffentlichen Bereich, auf den sich die Landesgesetze beschränken) die Vorabprüfung durch die speichernde bzw. verantwortliche Stelle selbst durchzuführen. Dies verstößt gegen die europäische Richtlinie, nach der die Kontrollstelle bzw. der unabhängige (behördliche) Datenschutzbeauftragte (Art. 18 Abs. 2, dritter Anstrich) zuständig ist. In Hessen ist erst das Ergebnis und dessen Begründung dem behördlichen Datenschutzbeauftragten zuzuleiten (der seinerseits "im Zweifelsfall" den Hessischen Datenschutzbeauftragten zu hören hat), in den Entwürfen von Schleswig-Holstein und Brandenburg ist er "zu beteiligen", was immer das zu bedeuten hat.

Bezugspunkt der Vorabkontrolle

Der BDSG-Entwurf 1998 bezieht sich entsprechend der Tradition des deutschen Datenschutzrechts auf Dateien. Diese sind der Vorabkontrolle zu unterziehen. Das ist allerdings gar nicht durchführbar, da nicht nur größere Verfahren stets eine Vielzahl von Dateien umfassen werden. Die Richtlinie spricht dagegen ausdrücklich von "Verarbeitungen". Damit sind Verfahren gemeint, die in Regel komplex und in sich abgeschlossen sind und die häufig im Rahmen eines Projektmanagements entwickelt und eingeführt werden. Allerdings kann sich die Vorabkontrolle auch nicht wie das Audit auf die Gesamtheit von Verfahren einer bestimmten Organisationseinheit, wie etwa ein Krankenhausinformationssystem beziehen. Die Notwendigkeit, die Vorabkontrolle jeweils durch einen Bericht abzuschließen, zeigt, daß Gegenstand der Prüfung nicht ein kontinuierlicher Prozeß sein kann. Vielmehr ist eine Vorabkontrolle bei jeder Systemkompo-

nente durchzuführen, die in den Betrieb gehen soll. Beim Audit gibt es diese Schwierigkeit nicht, da dieses gerade auf die kontinuierliche Beobachtung des gesamten Verfahrensablaufs angelegt ist.

Darüber hinaus gibt es eine weitere Abgrenzungsschwierigkeit: Ein IuK-Verfahren ist kein monostrukturales Gebilde, es umfaßt vielmehr immer verschiedene, auf einander aufbauende und ineinander verwobene Komponenten: Es umfaßt zum einen technische Geräte wie Großrechner, Netzwerke, PC's, Bildschirme, Tastaturen oder Drucker, zum anderen aber die verschiedenen Ebenen der eingesetzten Software. Häufig wird Standardsoftware genutzt, bei der die einzelnen Funktionen vom Anwender nicht wirklich durchschaut werden (ein Beispiel ist die Software von SAP, deren Funktionsweise kaum einem Anwender bekannt sein dürfte, obwohl sie gerade bei sensibelsten Anwendungen wie Krankenhaus- und Personalinformationssystemen zum Einsatz kommt). Hinzu kommen die einzelnen, vom Benutzer gestalteten Anwendungen; erst hier hat dieser die Möglichkeit, auf die einzelnen Funktionen Einfluß zu nehmen.

Für die Vorabkontrolle bedeutet dies, daß sie für die einzelnen Komponenten getrennt zu erfolgen hat. Da die verantwortliche Stelle jedenfalls bei der eingesetzten Hardware und der Standardsoftware allenfalls in beschränktem Umfang eine eigene Prüfung durchführen kann, wird sie sich bei einem Teil der Komponenten auf anderweit durchgeführte Prüfungen verlassen oder fremden Sachverstand beiziehen müssen. Daraus folgt, daß die Vorabkontrolle jedenfalls bei der Masse von Behörden und Unternehmen nicht isoliert vorgenommen werden kann, sondern Zertifizierungsmechanismen bei Hard- und Software voraussetzt.

Einbezogene Verfahren

Die Richtlinie beschränkt die Verpflichtung zur Vorabkontrolle nicht auf automatisierte Verfahren. Automatisierte und teilautomatisierte Verfahren werden zwar ausdrücklich angesprochen, doch aus der Bezugnahme auf Art. 18 (Meldepflichten) ergibt sich, daß auch komplexe andere Verfahren gemeint sind. Zu denken wäre etwa an herkömmliche Meldeverfahren, die noch auf dem Papierweg stattfinden. Sie werden zwar seltener, existieren aber durchaus noch, wenn

wir etwa an das Personal-, Gesundheits- oder Sozialwesen denken. Daß hier erhebliche Risiken bestehen können, zeigt die oft völlig ungesicherte Nutzung von Telefax.

Zentrale Bedeutung hat natürlich, welche Verfahren "besondere Risiken" aufweisen und deshalb einer Vorabkontrolle unterzogen werden müssen. Als erstes kommt es sicherlich auf die Art der Daten an. Erwägungsgrund 53 der Richtlinie und auch der BDSG-Entwurf 1998 erwähnen ausdrücklich die sensitiven Daten nach Art. 8 der Richtlinie. Ein Beispiel sind medizinische Daten. Jede Arztpraxis, jeder Optiker, jedes Krankenhaus ohnehin, jede Sozialstation, die hilfsbedürftige Menschen betreut, all diese Einrichtungen müssen hinsichtlich jeder Form der Datenverarbeitung, auch wenn es sich nur um einen einfachen PC-Einsatz handelt, eine Vorabprüfung durchführen. Bezieht man auch die anderen sensitiven Daten ein, zeigt sich, daß die Verpflichtung zu Vorabkontrollen durchaus nicht nur ein Randproblem darstellt, sondern eine Vielzahl von verantwortlichen Stellen betroffen sein wird.

Nach den Erwägungsgründen kommt es auch auf die Tragweite der Anwendungen an. Beispielsweise wird der Fall angeführt, daß sich die (öffentliche) Datenverarbeitung auf die gesamte Bevölkerung bezieht. Auf Unternehmensebene wird man konsequenterweise z.B. alle Fälle einbeziehen müssen, in denen die Anwendung die gesamte Belegschaft oder alle Kunden umfaßt.

Hinsichtlich der Zweckbestimmung werden die Erwägungsgründe konkreter und es ist möglich, sich ein deutlicheres Bild zu verschaffen. Daraus ergibt sich z.B., daß Verfahren, die eine Person von der Inanspruchnahme eines Rechts, einer Leistung oder einem Vertrag ausschließen - sämtliche "schwarze Listen", die irgendwo geführt werden, oder die Wagnisdateien der Versicherungsunternehmen - vorab kontrolliert werden müssen.

Auch neue Technologien begründen spezifische Risiken. Hier erwähnt die Richtlinie selbst in den Erwägungsgründen keine besonderen Voraussetzungen. Zu denken wäre hier an biotechnische Verfahren, Videoüberwachung, schwer durchschaubare Verarbeitungsmethoden wie Scoring-Verfahren, Testverfahren, moderne IT-Techniken, die ein besonderes Fehler- oder Mißbrauchsrisiko aufweisen,

oder Verfahren, die die Verknüpfung von Datenbeständen aus verschiedenen Quellen ermöglichen (vgl. z.B. Dammann/Simitis: EG-Datenschutzrichtlinie, Erläuterungen 2.2 zu Art. 20). Damit wird die gesamte Internetnutzung zu einem Risiko, denn die Suchmaschinen sind ja nichts anderes als eine Umsetzung des Data-Mining-Gedankens im gesamten Internet.

Methoden

Große Probleme wird die Frage aufwerfen, mit welchen Methoden die Vorabkontrollen durchzuführen sind.

Ein einfacher Weg wäre, davon auszugehen, daß die Vorabkontrolle nichts anderes als die Risikoanalyse ist, die ohnehin vor der Implementierung eines automatisierten Verfahrens erfolgen muß, um ein Sicherheitskonzept zu entwerfen.

Hierfür spräche, daß es bereits handhabbare Vorgaben gibt: So ist im Grundschutzhandbuch (für einfache Verfahren) und dem Sicherheitshandbuch (für komplexere Verfahren) des Bundesamtes für die Sicherheit in der Informationstechnik gut ausgearbeitet, was bei einer solchen IT-Sicherheitsanalyse alles niederzulegen und zu ermitteln ist. Zu berücksichtigen wären dabei z.B. die Risiken höherer Gewalt, organisatorischer Mängel, menschlichen Fehlverhaltens und technischen Versagens, vorsätzlichen Handelns. Maßnahmen zur Infrastruktur, organisatorische Gestaltung personeller Art, Hard- und Software bis hin zur Notfallvorsorge müssen in die Analyse einbezogen und bewertet werden, um Verfügbarkeit, Integrität und Vertraulichkeit sicherzustellen.

Allerdings ist die Risikoanalyse der erste Schritt einer jeden Festlegung von technisch-organisatorischen Maßnahmen bei einem IuK-System, sie muß also in jedem Fall und nicht nur beim Vorliegen spezifischer Risiken durchgeführt werden. Vorabkontrolle im Sinne des Art. 20 der Richtlinie muß also mehr bedeuten.

Hierfür spricht auch eine Vorschrift aus dem Berliner Landesrecht: Nach § 4 des Informationsverarbeitungsgesetzes ist eine Risikoanalyse bei allen Verfahren durchzuführen, die die allgemeine Verwal-

tung betreffen und bei denen die Registermeldung wegen geringer Sensibilität entfällt. Demnach muß in Berlin eine Vorabkontrolle gerade nicht bei besonders sensitiven Verfahren, sondern bei Alltagsanwendungen (Telefonbücher und dgl.) durchgeführt werden. Trotz der fehlenden Transparenz soll sichergestellt werden, daß die Vorbedingungen für technisch-organisatorische Maßnahmen auf jeden Fall erfüllt werden.

Denkbar wäre, die Vorabkontrolle im Sinne einer Technik- oder gar einer Technologiefolgenabschätzung zu verstehen, wie dies im bisherigen niedersächsischen und künftigen schleswig-holsteinischen Recht vorgesehen ist. Hierfür sind seit vielen Jahren anspruchsvolle Methoden entwickelt worden. Dies zeigt folgendes Zitat: "Das Idealkonzept der Technikfolgenabschätzung erhebt den Anspruch, neben der Früherkennung technologieinduzierter Risiken eine umfassende Analyse des Spektrums möglicher sozialer, wirtschaftlicher, rechtlicher, politischer, kultureller, ökologischer Auswirkungen zu leisten, in der problemorientierten Aufbereitung der Untersuchungsergebnisse alternative Handlungsoptionen entscheidungsorientiert aufzuzeigen und zugleich unterschiedliche gesellschaftliche Interessen und Werturteile, die sich an die Entwicklung und Nutzung neuer Technologien knüpfen, offen zu legen." (Schuchardt/Wolf: Technikfolgenabschätzung und Technikbewertung. In: Ropohl/Schuchardt/ Wolf: Schlüsseltexte zur Technikbewertung. Dortmund 1990. S. 19).

Dieser Anspruch zeigt allerdings, daß angesichts der Breite der einzubeziehenden Verfahren eine methodisch fundierte Technikfolgenabschätzung im Normalfall nicht durchgeführt werden kann. Eine derartige Verpflichtung würde zu einer völligen Überforderung aller Beteiligten oder zur Nichtbeachtung der Technikfolgenabschätzung führen: Man stelle sich vor, in jeder Arztpraxis müßte hinsichtlich aller eingesetzten Verfahren eine Technikfolgenabschätzung der einzusetzenden Hard- und Software sowie aller Verfahren, die ins Ärztenetz der Krankenkassen oder anderer Versorgungsträger eingebunden werden sollen, durchgeführt werden.

Diese einfache Überlegung zeigt, daß auch jedenfalls eine Technikfolgenabschätzung, die den bisher entwickelten Kriterien genügt, allenfalls bei Großverfahren mit gesellschaftlicher Reichweite verlangt werden kann. Für den Normalfall wird ein Mittelweg gefunden

werden müssen, der über die technischen Sicherheitsanforderungen hinaus den sozialen Kontext berücksichtigt, ohne die Beteiligten vor unlösbare Aufgaben zu stellen. Zweifellos bietet sich dabei allerdings an, gewisse methodische Schritte aus dem Repertoire der Technikfolgenabschätzung einzubeziehen.

Verfahren

Die Richtlinie enthält klare Vorgaben, wer für die Vorabkontrolle zuständig ist, nämlich die Kontrollstelle oder der (interne) Datenschutzbeauftragte. Die BDSG-Entwürfe von 1998 setzten dies konsequent um, indem der letztere für zuständig erklärt wurde. Wie bereits erwähnt, verstoßen allerdings die neuen Landesgesetze, die die datenverarbeitenden Stellen selbst für verantwortlich erklären, gegen den klaren Wortlaut der Richtlinie.

Zu klären ist der Zeitpunkt der Kontrolle bzw. Beteiligung. Wie bei der Kontrollstelle ist die Vorabkontrolle wohl "nach der Meldung" (hier zum internen Register) durchzuführen, nicht festgelegt ist jedoch, wann die Meldung zu erfolgen hat. Eine solche Festlegung wäre allerdings sinnvoll. Die Erfahrung der Datenschutzbeauftragten zeigt, daß der Zeitpunkt der Meldung für die Beurteilung von großer Bedeutung ist: Werden die Verfahren zu einem so frühen Zeitpunkt gemeldet, daß außer Bekenntnissen zur Notwendigkeit des Datenschutzes im allgemeinen nichts Konkretes erkennbar ist, ist dies ebenso wenig sinnvoll wie wenn bereits in allen Details festgelegte Verfahren gemeldet werden. Im ersten Fall ist eine Vorabkontrolle noch nicht möglich, im zweiten Fall kann nur noch beanstandet werden. Die Reaktion ist dann notwendigerweise, daß es für Änderungen leider zu spät sei, bestenfalls daß erst bei der nächsten Version Änderungen vorgenommen werden könnten. Hier muß der richtige Zeitpunkt gefunden werden, der eine Einschätzung des Verfahrens ermöglicht, die noch zu Revisionen führen kann.

Auch die Konsequenzen der Vorabkontrolle sind noch unklar. Die Erwägungsgründe der Richtlinie lassen offen, ob die Kontrollstellen bzw. die (behördlichen, betrieblichen) Datenschutzbeauftragten nur eine - letztlich unverbindliche - Stellungnahme abgeben können oder

ob der Gesetzgeber im Sinne der "wirksamen Einwirkungsbefugnisse" (Art. 20 Abs. 3 der Richtlinie) eine Genehmigungspflicht vorsehen muß.

Nach Abschluß der Prüfung stellt sich die Frage der Publikation des Ergebnisses; der BDSG-Entwurf von Bündnis 90/Die Grünen sieht die Veröffentlichung vor. Im Sinne der Transparenz der Datenverarbeitung wäre dies sicherlich zu begrüßen. Ungeachtet der Problematik von Geschäftsgeheimnissen, die sich hier zwangsläufig stellt, ist es allerdings fraglich, ob es Sinn macht, daß jede verantwortliche Stelle das Ergebnis ihrer Vorabkontrolle (wo eigentlich?) veröffentlichen muß. Auch hier ist eine Differenzierung sinnvoll: So bietet sich die Publikation in den Fällen an, in denen eine Vorabkontrolle bei Hardware oder Standardverfahren stattgefunden hat, und deren Ergebnisse von anderen Stellen übernommen werden könnten. Für andere, für die Öffentlichkeit besonders wichtige Verfahren ist die Veröffentlichung ein Mittel der politischen Auseinandersetzung, wie dies ja auch im Entwurf von Bündnis 90/Die Grünen zum Ausdruck kommt. Eine Kannklausel, die diese Zielrichtung vorgibt, wäre hier sicherlich sinnvoll.

Für große (in der Regel staatliche, u.U. aber sogar private) Verfahren kann nach Art. 20 Abs. 3 der Richtlinie die Vorabkontrolle durch den Gesetzgeber selbst vorgenommen werden. Dies setzt voraus, daß die parlamentarische Zustimmung vom positiven Ergebnis einer solchen Kontrolle abhängig gemacht wird. Diese könnte bereits von der Regierung im Rahmen einer Gesetzesvorlage vorgenommen oder vom Parlament selbst in Auftrag gegeben werden: In beiden Fällen bedarf es entsprechender Geschäftsordnungsregeln. Die Richtlinie läßt auch Vorabkontrollen im Zuge einer auf eine "gesetzgeberische Maßnahme gestützten Maßnahme" (sic) zu, mithin beim Entwurf einer entsprechenden Rechtsverordnung oder gar nur einer Verwaltungsvorschrift (z.B. Errichtungsanordnung?). Zwar ist hier die Einschaltung interner Datenschutzinstanzen nicht vorgeschrieben, es liegt aber nahe, in diesen Fällen den bzw. bei mehreren beteiligten Stellen die behördlichen Datenschutzbeauftragten der Ministerien bzw. nachgeordneten Behörden einzubeziehen.

Konsequenzen

Mit dem Instrument der verbindlichen Vorabkontrolle werden die behördlichen und betrieblichen Datenschutzbeauftragten eine Stellung erhalten, die weit über die bisherigen Aufgaben hinausgeht, zumal wenn die Genehmigung durch diese Instanzen Rechtmäßigkeitsvoraussetzung der Datenverarbeitung ist. Sie erhalten die Chance, jedenfalls bei den unter die Regelung des Art 20 fallenden Verfahren sich prospektiv an der Entwicklung zu beteiligen. Dies würde sie stärken und klarmachen, daß sie nicht, wie dies mitunter gesehen wird, auf eine schlichtende Rolle im Einzelfall beschränkt sind. Vielmehr unterstützt dies diejenigen, die richtigerweise den Datenschutz als Qualitätsmerkmal ihrer Produkte entdeckt haben.

Damit verbunden werden muß sowohl bei Behörden und Unternehmen als verantwortlichen Stellen als auch bei den Datenschutzbeauftragten und Aufsichtsbehörden - bei letzteren im besonderen Maße - eine Verbesserung der Ausstattung in jeder Hinsicht. Mit den bisher zur Verfügung gestellten Mitteln werden sich die Aufgaben nicht bewerkstelligen lassen.

Nutzende und Datenschutz im Electronic Commerce

- Empirische Befunde und exemplarische Lösungsansätze der IuK-Industrie[1] -

Georg Schyguda

1. Subjektive Sicherheitsaspekte

Die Entwicklung des Internet hin zu einem globalen virtuellen Marktplatz mit neuen Chancen für Anbieter, Händler und Verbraucher beherrscht gegenwärtig die öffentliche Debatte. Eine der wesentlichen Herausforderungen und zugleich grundlegende Voraussetzung auf dem Weg zur erfolgreichen Realisierung dieses Szenarios ist die Schaffung eines Sicherheitsklimas in bezug auf das Internet. Dazu zählen objektive Aspekte wie die Klärung technischer, ökonomischer und rechtlicher Voraussetzungen sowie deren Implementierung ebenso wie die Erlangung eines subjektiven Sicherheitsempfindens bei allen beteiligten Akteuren. Letzteres bildete ein Schwerpunktthema der hier vorgestellten Umfrage und steht im Mittelpunkt meiner Ausführungen.[2]

---

[1] Teilaspekte der hier vorgestellten Ergebnisse wurden im Rahmen eines durch das Technologiezentrum Darmstadt der Deutschen Telekom AG beauftragten Forschungsprojektes durch das Fraunhofer Institut Systemtechnik und Innovationsforschung, Abteilung Informations- und Kommunikationssysteme sowie dem Südwestfunk, Abteilung Medienforschung im Jahre 1997 erhoben.
Mein Dank gilt hier besonders den Herren Sven Kornetzky und Peter Zoche.

[2] Die WWW-basierte Umfrage erfolgte im Oktober/November 1997 und wurde von 691 Teilnehmern beantwortet, zeitgleich wurde eine Telefoninterviewaktion mit 1000 repräsentativen Online-Nutzerinnen und -Nutzern (Quotierung:

In einer Eingangsfrage wurden die Teilnehmer gebeten, **die Sicherheit** bei der Übermittlung vertraulicher Daten durch verschiedene Medien zu beurteilen. Die Ergebnisse dieser Frage unterstreichen, daß *gegenwärtig sehr wenig Vertrauen in die neuen Mediennutzungen E-Mail und WWW* gesetzt wird, *Abbildung 1.1*. Im Vergleich zu den etablierten Kommunikationsformen wird im Hinblick auf die sichere und unverfälschte Übertragung bzw. Weiterleitung von vertraulichen, für einen Kaufvorgang relevanten Informationen ein deutlich geringeres Sicherheitsempfinden zum Ausdruck gebracht. So empfinden lediglich 22% der repräsentativ Befragten das WWW als sehr bzw. ziemlich sicheres Übertragungsmedium im Vergleich zu 57% bei brieflicher Übermittlung.

Unter den Teilnehmern der netzbasierten Umfrage ist diese Sicherheitsbewertung noch erheblich stärker zu ungunsten der neuen Medien ausgeprägt bei gleichzeitig positiverer Bewertung traditioneller Verfahren (Brief, Telefon, Fax).

Generell gilt, daß mit zunehmender Online-Erfahrung auch die subjektive Bewertung der Sicherheit kritischer gesehen wird. Sind es beispielsweise unter den Teilnehmern mit vergleichsweise geringer Online-Erfahrung (weniger als 1 Jahr) noch 44%, die eine Übermittlung per E-Mail als sehr bzw. ziemlich sicher einstufen, so nimmt diese Zustimmungsquote auf 29% bei den Teilnehmern ab, die 4 und mehr Jahre Online-Erfahrung aufweisen. Mit der Dauer der Online-Erfahrung wird zudem der Abstand zu konventionellen Übermittlungsverfahren größer, *Tabelle 1.1*.

ABL/NBL = 87.5%/12.5% (VUMA 97/1)) geführt, um statistisch valide Daten zu generieren. Die Erhebung erfolgte im Auftrag der Deutschen Telekom AG, Technologiezentrum Darmstadt und wurde vom Fraunhofer Institut Systemtechnik und Innovationsforschung, Abteilung Informations- und Kommunikationssysteme sowie dem Südwestfunk, Abteilung Medienforschung maßgeblich durchgeführt.

Abbildung 1.1: Sicherheitsempfinden bei der Übermittlung vertraulicher Informationen

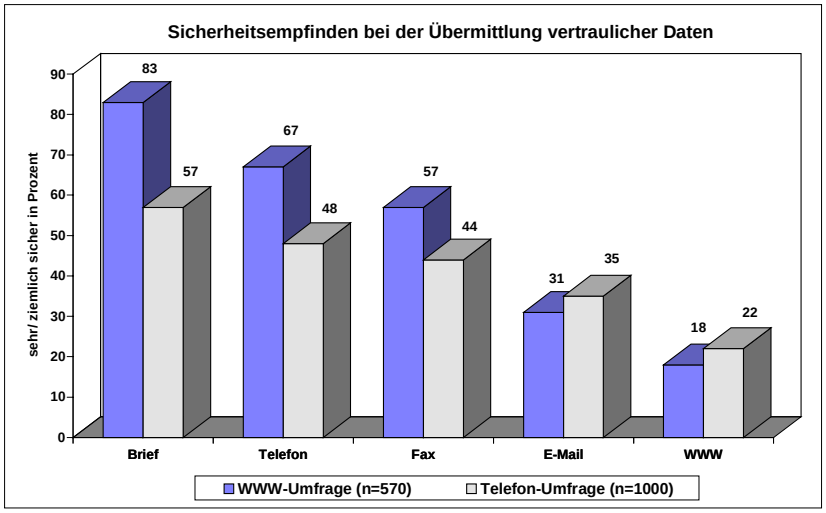


Tabelle 1.1: Sicherheitsempfinden bei der Übermittlung vertraulicher Daten in Abhängigkeit der Online-Erfahrung (Telefon-Umfrage)

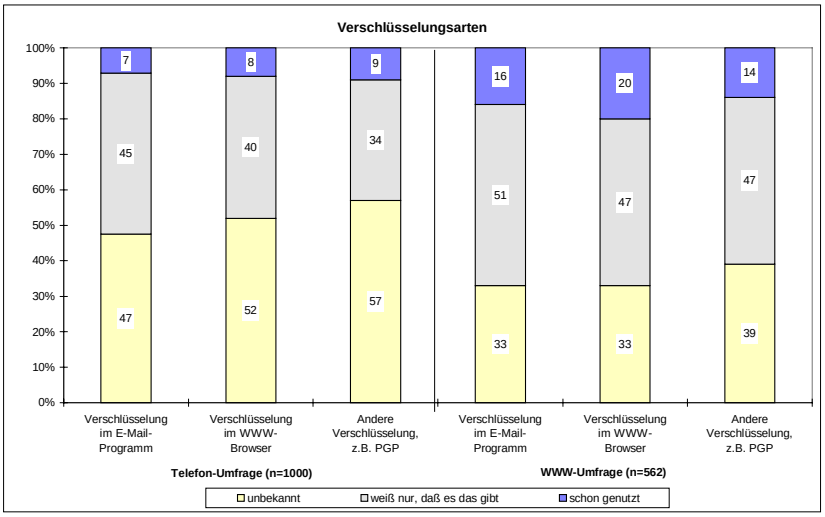
	sehr/ziemlich sicher [%]			
	Beginn der Online-Nutzung			
Medium	**vor bis 1 Jahr**	**vor 1 bis unter 2 Jahren**	**vor 2 bis unter 4 Jahren**	**vor 4 Jahren und mehr**
Brief	48	50	63	60
Telefon	48	49	47	48
Fax	43	42	47	43
E-Mail	44	34	34	29
WWW	27	23	22	15

Vor dem Hintergrund einer negativen Sicherheitsbewertung kommt der Möglichkeit der **Verschlüsselung** von Daten eine hohe Bedeutung zu. Es gibt eine Vielzahl entsprechender Softwareprogramme,

die durch Anwendung kryptographischer Verfahren Daten während der Übertragung in offenen Netzen vor Mißbrauch oder Verfälschung schützen können. Solche Tools sind teilweise bereits Bestandteil von E-Mail-Programmen und WWW-Browsern. Daneben gibt es mehrere, zum Teil frei erhältliche Programme zur Verschlüsselung, z. B. PGP[3].

Abbildung 1.2 zeigt, daß solche *Verschlüsselungsverfahren bei einem großen Teil der Online-Nutzer noch unbekannt* sind *und nur von wenigen Befragten bereits genutzt* wurden. Bekanntheits- und Nutzungsgrad steigen allerdings mit zunehmender Online-Erfahrung.

Abbildung 1.2: Bekanntheitsgrad und Nutzung von Verschlüsselungsarten



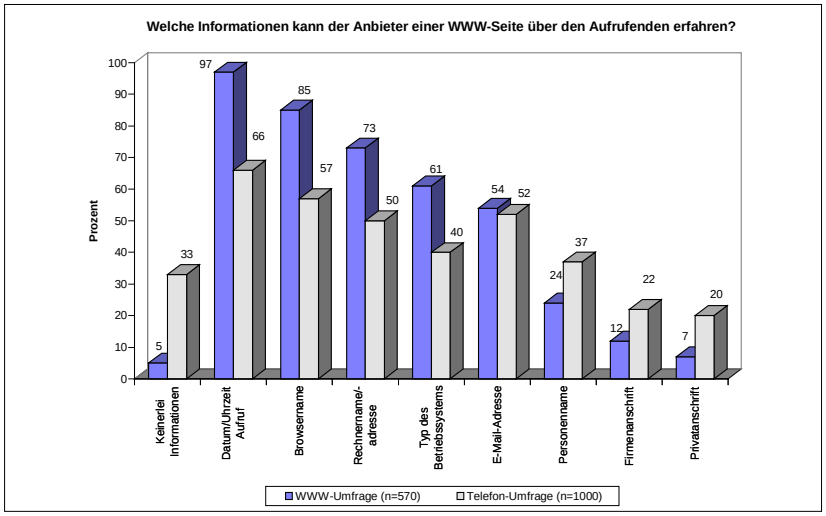
[3] **P**retty **G**ood **P**rivacy ist ein Verschlüsselungsprogramm zur sicheren Übertragung elektronischer Post. "Es verwendet IDEA zur Datenverschlüsselung, RSA (mit Schlüsseln bis zu 2047 Bit) zur Schlüsselverwaltung und für digitale Signaturen sowie MD5 als Einweghashfunktion." Quelle: Bruce Schneier: Angewandte Kryptographie. Addison-Wesley, Bonn 1996, S. 664-667. PGP ist als Freeware (ausschließlich für den privaten Gebrauch) oder als kostenpflichtige Software für verschiedene Plattformen beispielsweise zu beziehen von <http://www.pgp.com/products/personal/products.cgi>.

Insgesamt ist festzuhalten, daß das Sicherheitsniveau im Internet als niedrig eingeschätzt wird. Gleichzeitig kann ein Informationsdefizit im Hinblick auf Maßnahmen, die der Erhöhung dieser Sicherheit dienen, festgestellt werden. Andererseits zeigen die Umfragedaten, daß die diesbezügliche Informiertheit per se keinen Einfluß auf die Nutzung solcher Maßnahmen hat; dies könnte daran liegen, daß die Installation und die Anwendung dieser Programme als zu komplex und wenig nutzerfreundlich angesehen wird. Diese Einschätzung könnte auch erklären, daß unter den (wenigen) Nutzern kryptographischer Verfahren die generelle Sicherheitsbewertung von WWW und E-Mail nicht positiver ausfällt.

Beim Aufruf einer beliebigen WWW-Seite werden grundsätzlich verschiedene personengebundene, zum Teil **vertrauliche Informationen über den Internet-Nutzer** an den Inhalteanbieter weitergeleitet. Dieser Umstand ist ein Aspekt, weshalb die Sicherheit des WWW als gering bewertet wird. Gleichwohl sind ein Drittel der repräsentativ Befragten der - irrtümlichen - Auffassung, daß keine Angaben gespeichert werden können.

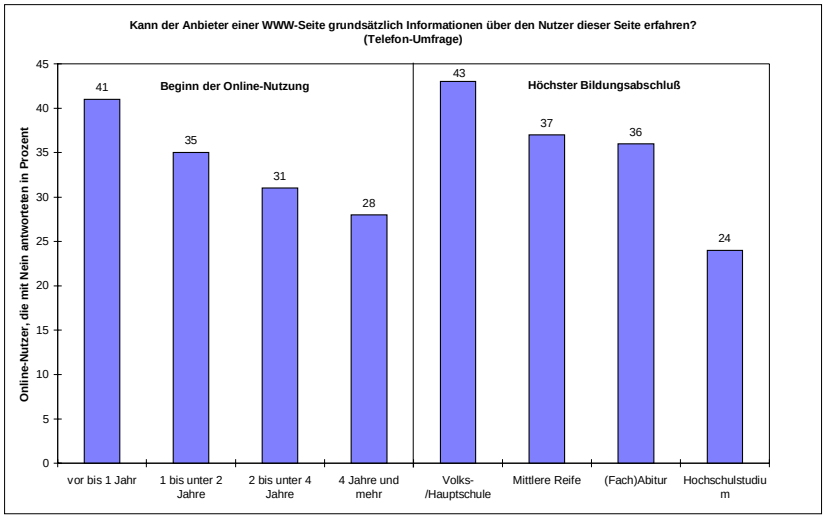
Die in der netzbasierten Umfrage Befragten sind hier realistischer: nur 5 % fühlen sich bei der Netznutzung unbeobachtet, *Abbildung 1.3*. Generell läßt ihr Antwortverhalten erkennen, daß sie über die grundsätzlichen Möglichkeiten, sich durch bestimmte Browser-Einstellungen vor einer Kontrolle des Anbieters zu schützen, besser informiert sind.

Abbildung 1.3: Verfügbare Informationen des WWW-Seiten-Anbieters über den Aufrufenden



Die Repräsentativumfrage zeigt, daß die Informiertheit über eine mögliche Datenspeicherung während eines Seitenaufrufs mit größerer Online-Erfahrung und höherer Schulbildung tendenziell zunimmt, *Abbildung 1.4*.

Abbildung 1.4: Informationsspeicherung bei WWW-Seitenaufruf versus Online-Erfahrung und höchstem Bildungsabschluß (Telefon-Umfrage)



Im Zusammenhang mit der derzeit geführten **Kryptographiedebatte** und den dabei diskutierten Ansätzen zur Gewährleistung von Anonymität bei der Kommunikation in offenen Netzen wurde nach der Bekanntheit dieser Ansätze (nur WWW-Umfrage[4]) und den Präferenzen der Nutzer gefragt. *Abbildung 1.5* zeigt die Ergebnisse auf diese Frage in beiden Befragungsarten.

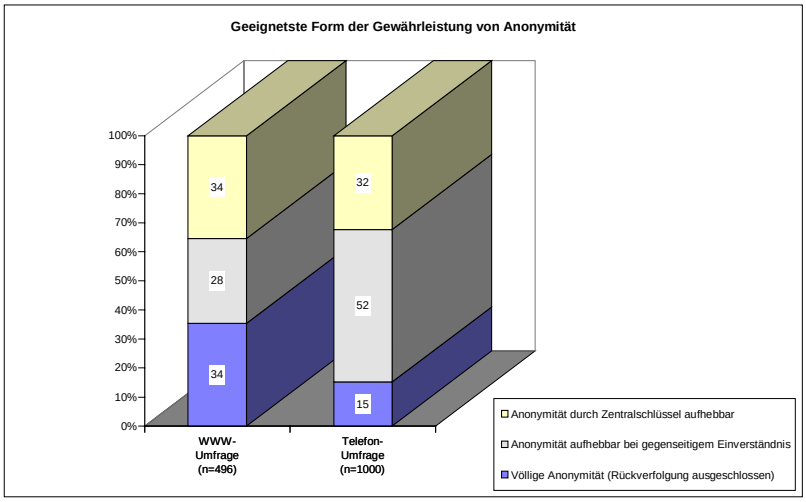
Unter den repräsentativ Befragten tendieren mehr als die Hälfte zu einer bedingt aufhebbaren Anonymität. In diesem Falle erfolgt die Kommunikation beispielsweise über Pseudonyme. Dabei kann die Identität der Kommunikationsteilnehmer nur mit dem Einverständnis aller Akteure offengelegt werden. Immerhin rund ein Drittel spricht sich für das stark umstrittene Konzept des bei einer staatli-

[4] Aus methodischen Gründen konnte eine entsprechende Frage nur bei der schriftlichen, netzbasierten Umfrage gestellt werden; 90% aller Befragten gaben an, die verschiedenen Anonymitätsansätze zu kennen.

chen Stelle (z. B. Staatsanwaltschaft, Polizei) hinterlegten Zentralschlüssels aus. Dabei sinkt dieser Anteil mit zunehmender Online-Erfahrung und höherer Schulbildung der Befragten zugunsten der bedingt aufhebbaren Anonymität. Eine Minderheit von 15% spricht sich für eine völlige Anonymität ohne jedwede Rückverfolgungsmöglichkeit durch Kommunikationspartner oder durch Dritte aus.

Demgegenüber zeichnet sich bei den Teilnehmern der WWW-Umfrage keine klare Präferenz für einen bestimmten Ansatz ab. Interessant ist jedoch, daß die beiden im Hinblick auf Privacy gegensätzlichsten Positionen - völlige Anonymität versus Zentralschlüssel - die größte Zustimmung erhalten.

Abbildung 1.5: Geeignetheit diverser Anonymitätsformen



Zusammenfassend läßt sich sagen, daß die Mehrheit der Online-Nutzer gut über Sicherheitsprobleme im Internet informiert ist. Die Gewährleistung von Sicherheit wird als sehr gering eingestuft. Eine Erhöhung des subjektiven Sicherheitsempfindens kann durch einen Abbau vorhandener Informationsdefizite über den Einsatz kryp-

tographischer Verfahren gefördert werden. Die Anwendung dieser Techniken erfolgt zur Zeit nur marginal, ihr verstärkter Einsatz sollte die künftige Inanspruchnahme von Online-Diensten - insbesondere in sicherheitssensitiven Bereichen - positiv stimulieren.

2. Elektronischer Handel und elektronischer Zahlungsverkehr

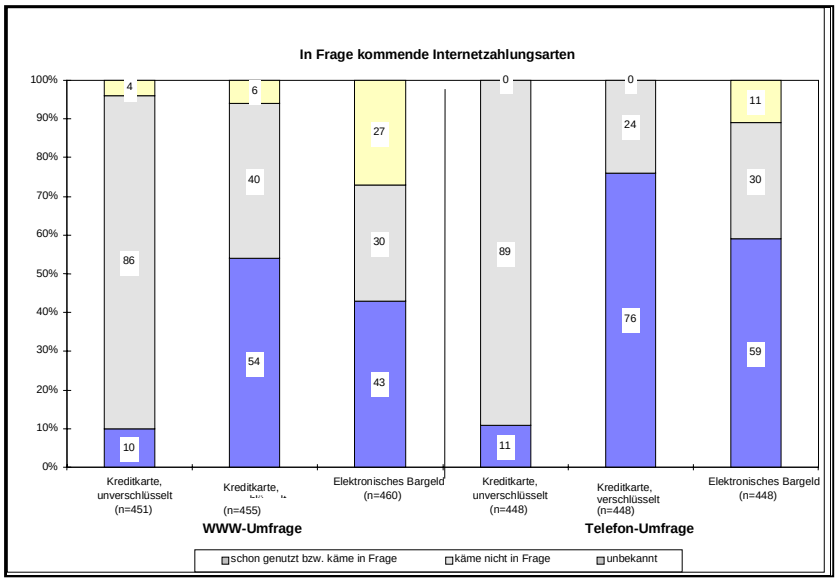
Eine zunehmende Verbreitung des **elektronischen Handels** wird neben der individuell empfundenen Sicherheit während des Kaufvorgangs wesentlich von der Bereitstellung attraktiver Angebote und sicherer **elektronischer Zahlungssysteme** abhängen. In den beiden vorliegenden Umfragen wurden die Ansichten der Online-Nutzerinnen und -Nutzer zur Bekanntheit und Akzeptanz verschiedener Internet-Zahlungssysteme und der bisherigen Verbreitung des Interneteinkaufs erfragt. Die entsprechenden Antworten stehen im Blickpunkt dieses Abschnittes.

Internet und Online-Dienste können ein zusätzlicher, für Hersteller, Händler und Anbieter attraktiver Vertriebsweg herkömmlicher Produkte sein. In diesem Fall erfolgen Auswahl und Bestellung eines Artikels sowie gegebenenfalls die Bezahlung über das Internet, während die Auslieferung der Ware auf traditionellem, d. h. postalischem Wege vonstatten geht. Eine völlig neue Qualität erreicht das Netzgeschäft darüber hinaus durch die wachsende Möglichkeit, einzelne Produkte bzw. Produktgruppen zu immaterialisieren und somit physische Distributionswege durch elektronische zu ersetzen. In diesem Fall können Produkte durch das Internet nicht nur bestellt, sondern auch ausgeliefert werden.

Zum gegenwärtigen Zeitpunkt werden Handelstransaktionen über das Internet vorrangig noch mittels traditioneller Bezahlungsformen (z. B. per Rechnung, Scheck oder Nachnahme) abgewickelt. Daneben wurde die Zahlung per Kreditkarte für das Internet adaptiert. Die Kreditkartendaten wurden dabei zunächst unverschlüsselt, in zunehmendem Maße aber auch verschlüsselt an den Zahlungsempfänger übermittelt. Der **Bekanntheitsgrad** sowie die **Akzeptanz** dieser beiden Ansätze sowie von sogenanntem elektronischem Bargeld sind in *Abbildung 2.1* dargestellt. *Sehr deutlich kommt die ablehnende Haltung der Online-Nutzerinnen und -Nutzer gegenüber*

der unverschlüsselten Übermittlung der Kreditkartendaten als Resultat fehlender Sicherheit zum Ausdruck (89% - Repräsentativerhebung, 86% - Netzumfrage). *Auf die größte Akzeptanz stößt demgegenüber die Kreditkartenzahlung für den Fall, daß die Datenübertragung in verschlüsselter Form erfolgt* (76% - Repräsentativerhebung, 54% - Netzumfrage). Hier kann davon ausgegangen werden, daß die Vertrautheit der Verbraucher mit dem System Kreditkarte eine nicht unwesentliche Rolle spielt. Interessant ist ferner der hohe Bekanntheitsgrad sowie die hohe Akzeptanz des noch recht neuen Konzepts des elektronischen Bargelds bei solchen Befragten, die entweder bereits eine Internetzahlung getätigt haben oder hierzu grundsätzlich bereit wären.

Abbildung 2.1: Bekanntheitsgrad und Akzeptanz ausgewählter gegenwärtiger Internetzahlungssysteme



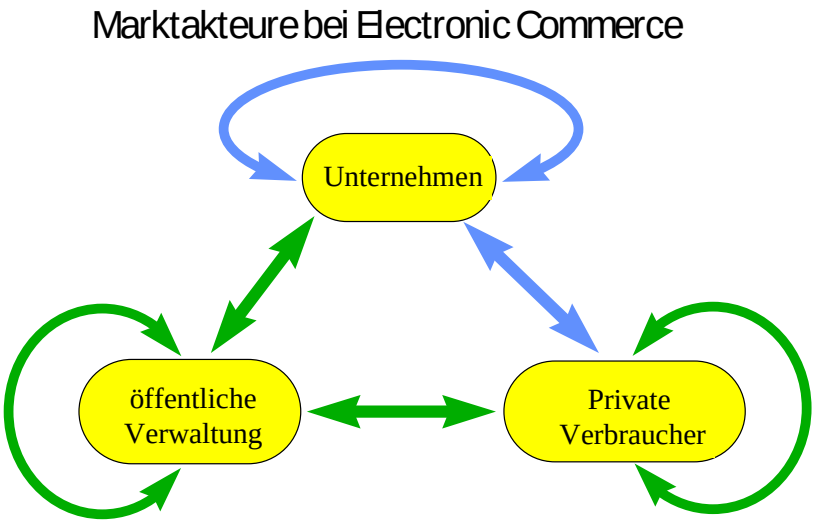
3. Lösungsansätze der Iuk-Industrie

Die im Kontext von "e-commerce"[5] auf dem "Cyber-Marktplatz" anzutreffenden Akteure sind hinsichtlich der verschiedenen Regulierungsinitiativen, technischen und ökonomischen Unwägbarkeiten in der klassischen Situation entweder

1. einen neu entstehenden Dienstleistungsbereich unter dem Aspekt des laissez-faire entstehen zu lassen oder

2. im öffentlichen Recht befindliche Regulatorien teilweise zu internationalisieren und hinsichtlich ihrer Anwendbarkeit auf das Internet zu überprüfen.

Abbildung 3.1: Akteure auf elektronischen Marktplätzen



Quelle: Sacher-Report, OECD

[5] Hinsichtlich der im WWW getätigten Umsätze im Vergleich zu herkömmlichen Handelsdaten steckt der "e-commerce" im Augenblick sicherlich noch in den Kinderschuhen.

Der erste Lösungsansatz birgt die Problematik in sich, daß durch bekannt werdende einzelne Fälle von Datenmißbrauch (etwa E-Mail-Adressenhandel) durch Anbieter vom kommerziellen Diensten im Internet der gesamte Internet-Handel bei den Verbraucherinnen und Verbrauchern in Mißkredit gerät (siehe hierzu auch Boston Consulting Group, in : Red Herring 2/98) und sich vielversprechende Wachstumsprognosen aus Sicht der IuK-Industrie und des Einzelhandels nicht kurz- bis mittelfristig realisieren lassen.

Der zweite Aspekt beinhaltet die Option, den Bereich e-commerce zusätzlich durch freiwillige Selbstverpflichtungen zu regulieren und somit zusätzlich zu den weitergehenden staatlichen Regulierungen aus unternehmens- und anwendungsspezifischer Sicht kurzfristig umsetzbare Konzepte hinzuzufügen, die in der Lage sind, den heutigen nationalstaatlichen Datenschutzgesetzen Rechnung zu tragen.

Eine auch von der Deutschen Telekom AG favorisierte Möglichkeit, zur Beförderung des e-commerce im Sinne aller Beteiligten aus datenschutzrechtlicher und ökonomischer Sicht konstruktiv beizutragen, besteht im Eingehen freiwilliger Verpflichtungen - "codes of conduct". Abschließende, quasi "monolithische" staatliche Regelungen sind nach Ansicht unseres Unternehmens durch die Innovationsgeschwindigkeit und -fülle (technologische Innovationen und neue Geschäftsmodelle) im Bereich des Internet-basierten e-commerce nicht zielführend. Vielmehr wird sich unter den Nutzerinnen und Nutzern sehr bald ein auch subjektiv meßbares, aber auch objektiv begründbares Gefühl der Sicherheit bei der Nutzung von e-commerce Dienstleistungen einstellen, wenn sie vermehrt durch ernstzunehmende Initiativen - wie sie auch die freiwillige Selbstverpflichtung von Unternehmen zur "Datensparsamkeit" darstellt - auf ihre Belange und Rechte zugeschnittene Online-Dienstleistungen kennen- und nutzen lernen.

Um eine Betrachtung internationaler Initiativen anzuschließen werden im folgenden exemplarisch die "codes of conduct" der US-

amerikanischen Initiative "e-trust" dargestellt, die von namhaften Unternehmen bei den jeweiligen unternehmensspezifischen WEB-Auftritten berücksichtigt werden.[6]

Gründe für die Etablierung der non-profit-organisation e-trust sind vor allem folgende, hier exemplarisch durch die Untersuchung der Boston Consulting Group dargestellten Einstellungen von WWW-Nutzerinnen und -Nutzern zu "privacy-policies":

Abbildung 3.2: Boston Consulting Group in: The Red Herring, 3/98

BARRIERS TO REGISTRATION

Why Web users refuse to supply *personal information* online (%)

How the collected information will be used is not specified clearly **69.3**
Gaining access to the site is not worth revealing the information **64.5**
The sites collecting information are thought to be untrustworthy **62.0**
Don't want to reveal postal address **44.5**
Takes too long to complete the form **42.4**
Don't want to reveal name **31.3**
Don't want to reveal e-mail address **25.5**

[6] Sicherlich ist diese freiwillige Selbstverpflichtungsinitiative auch ein Resultat der sich stark von der bundesrepublikanischen Datenschutzgesetzgebung abhebenden Gegebenheiten des US-amerikanischen Rechtssystems.

Abbildung 3.3: Freiwillige Selbstbeschränkung bei "e-trust"

Wie entsteht Vertrauen im Cyberspace?

z.B. durch freiwillige Selbstbeschränkung 

TRUSTe is an independent, non-profit, privacy initiative dedicated to building *users' trust* and confidence on the Internet, and in so doing, accelerating growth of the Internet industry.
We've developed a *privacy program* that bridges the gap between users' concerns over privacy and Web sites' desire for flexible disclosure standards. Our program is backed by a multi-faceted assurance process that establishes Web site credibility, which allows users to be more comfortable offering accurate personal information and making purchases online (http://www.etrust.org/).

Die Aufklärung von Nutzerinnen und Nutzer über die Datenspeicherung und -weiterverarbeitung durch spezifische Anbieter von e-commerce-Lösungen ist sicherlich nur ein Baustein zur Erlangung von subjektiv empfundener, objektiv meßbarer und ökonomisch vertretbarer Sicherheit im WWW. Die Genese dieses soziotechnischen Systems und der darin - national wie international getätigten rechtsverbindlichen Transaktionen - wird sicherlich zusätzlich stark durch folgende Faktoren beeinflußt werden:

1. Sich selbst organisierende Nutzerinnen und Nutzer-Initiativen mit Verbraucherschutz-Charakter (newsgroups zu "best practices" wie dem o.g. privacy-Programm oder der Brandmarkung von "schwarzen Schafen" hinsichtlich Bedienbarkeit und Datensparsamkeit).

2. Die Entscheidung der Teilnehmerinnen und Teilnehmer über die Teilnahme am e-commerce ist nur partiell technikorientiert, vielmehr werden auch in Zukunft die Attraktivität der zur Verfügung stehenden Produkte und Dienstleistungen und

3. bestehende Bankbeziehungen (bezüglich elektronischer Zahlungssysteme) eine große Rolle spielen.

Informationszugang und Datenschutz

Herbert Burkert

1. Elemente des Informationszugangs

Die Zeichen mehren sich. Großbritannien als bisher stärkste Bastion in der Verteidigung des Amtsgeheimnisses hat seit dem Amtsantritt von Premierminister Blair einen Gesetzesentwurf über den Informationszugang in Arbeit. Damit wird die Bundesrepublik zusammen mit Luxemburg bald zu den einzigen Mitgliedsstaaten der Union gehören, die auf nationaler Ebene noch über kein allgemeines Informationszugangsgesetz verfügen.

Der Europäische Gerichtshof legt in - man darf nun sagen - ständiger Rechtsprechung die Beschlüsse des Rates und der Kommission sowie den dazu gehörenden Verhaltenskodex zum Zugang zu Informationen der Union extensiv aus und verlangt gleichzeitig von diesen Stellen eine detaillierte Subsumtion, wenn Ausnahmen gemacht werden sollen. Ein Grünbuch der Union zu diesem und damit verwandten Themen steht unmittelbar bevor. Im Amsterdamer Vertrag haben Transparenzelemente ihren festen Platz.

Als erstes Bundesland hat Brandenburg nach einem nicht immer einfachen Weg dem Gebot der eigenen Verfassung Folge geleistet und ein allgemeines Akteneinsichts- und Informationszugangsgesetz erlassen. Auch die Koalitionsvereinbarung der neuen Bundesregierung scheint deutlich: Ein Informationszugangsgesetz in Deutschland, auch auf Bundesebene, ist keine Frage mehr des Ob, sondern allenfalls des Wie und Wann.

Die notwendigen Bausteine eines solchen Gesetzes will ich ganz kurz in Erinnerung rufen - seit zwanzig Jahren sind sie bekannt, als sich Deutschland der entsprechenden Empfehlung des Ministerrates des Europarates angeschlossen hatte:

- Informationszugangsgesetze schaffen ein voraussetzungsloses, effektiv umzusetzendes Recht auf Zugang;
- auf der Basis der Gleichheit;
- mit Ausnahmen, soweit sie in einer demokratischen Gesellschaft für den Schutz der legitimen öffentlichen und privaten Interessen notwendig sind;
- ein Recht, über das in angemessener Zeit zu entscheiden ist,
- dessen jeweilige Ablehnung angemessen begründet und gerichtlich überprüfbar sein muß.

In meinem heutigen Beitrag zu diesem Thema möchte ich darlegen,

- daß sich ein solcher Schritt zwangsläufig aus der auf Komplementarität angelegten Datenschutzordnung ergibt,
- daß dabei auftretende Gestaltungsaufgaben im Sinne dieser funktionalen Komplementarität lösbar sind.

Ich werde exemplarisch auf einige dieser Lösungen verweisen. Dies sind für mich *Bauprobleme* der sich entwickelnden Informationsordnung. Ich werde weiter darlegen, daß gegenwärtig diskutierte Lösungskonzepte - wie der internationale Vergleich zeigt - einige Folgeprobleme mit sich bringen werden, die nach Möglichkeit bereits jetzt in einer bundesdeutschen Regelung mitbedacht werden sollten. Das sind für mich *Probleme der Bewohnbarkeit* der Informationsordnung. Und abschließend werde ich darauf hinweisen, daß Datenschutz und Informationszugang mit ihrem Aktionensystem und ihrer institutionellen Einbettung nur Teil eines umfassenderen Aufgabenspektrums sind, Aufgaben, die sich vor allem an den Gesetzgeber richten. Diese Probleme nenne ich die *Siedlungsprobleme* unserer Informationsordnung.

2. Informationszugang als notwendige Ergänzung der Datenschutzordnung

Der wesentliche Beitrag, den die deutsche Diskussion zur Entwicklung des Datenschutzkonzeptes geleistet hat, lag in der Betonung des Selbstbestimmungselementes. Dieses Selbstbestimmungselement ergänzt das "right to be left alone" angelsächsischer Prägung, den skandinavischen Versuch administrativer Bewältigung technologischer Veränderung durch Administration, und das französische Konzept: Wenn die Privatsphäre angerührt wird, werden alle bürgerlichen Freiheiten angerührt: Informatique et Libertés. Informationelle Selbstbestimmung verweist dabei unmittelbar auf seine Ergänzung durch Informationszugang: Als Selbstbestimmungsrecht kann es nur durch Einwilligung eingeschränkt werden. Diese Einwilligung aber setzt Wissen voraus. Dabei kann diese Einwilligung individuell in einer Art Informationsvertrag ausgehandelt werden. Hier tritt Wissen zu den üblichen Sicherungen hinzu, die bei solchen Informationsverträgen verhindern, daß die Kluft zwischen dem rechtlichen Konstrukt der Gleichheit und der sozialen Realität der Ungleichheit nicht zu groß wird.

Diese Einwilligung kann aber auch durch den demokratischen Prozeß der Gesetzgebung gewissermaßen kollektiv ausgehandelt werden. Auch dieser Prozeß hat Transparenz als eine seiner Legitimationsvoraussetzungen. Dort wo Bürgerinnen und Bürger individuell oder kollektiv einwilligen, wird daher die subjektive Möglichkeit des Sich Informieren Könnens vorausgesetzt. Auskunftsrecht und Benachrichtigungspflicht flankieren dieses Wissen. Datenschutz ist somit, wie vom Bundesverfassungsgericht ausdrücklich bestätigt, als Schutz durch Wissen konzipiert.

Zum individuellen Wissen tritt das Institutionen-Wissen durch Datenschutzbeauftragte, Registrierungspflichten und öffentlich einsehbare Register. In meinem Beitrag sehe ich nicht den Ort, dem nachzugehen, was die Anwendungswirklichkeit aus den Anwendungsprinzipien gemacht hat. Ich behalte mir das für den prognostizierenden Teil meiner Ausführungen zum Informationszugang vor. Eine kurze Bemerkung sei mir gestattet. Die Vielzahl der Datenschutzbehörden erlaubt uns zu vergleichen und zu lernen; sie schafft "peer groups", denen gegenüber man sich zumindest gelegentlich zur

Rechtfertigung verpflichtet fühlt. Beides hat - dank föderativer Struktur - zum Regulierungswettbewerb "Datenschutz" beigetragen, der ihn europaweit wie international so konkurrenzfähig gemacht hat.

Einwilligung, demokratisch-transparente Regeln für die Fälle, in denen von Einwilligung abgesehen wird, individuelle Rechte auf Wissen und Wissensvermittlung, institutionelle Absicherung des Wissens um allgemeine Systemzusammenhänge im Verhältnis zwischen Bürgerinnen und Bürgern und dem Staat sind zusammengefaßt die Elemente des Datenschutzes, die - in konsequenter Fortschreibung - nach abschließender Ergänzung durch ein umfassendes Informationszugangsgesetz verlangen.

Die informationellen Elemente des Datenschutzes sind gelegentlich in Vergessenheit geraten. Mir scheint, nicht ohne Grund. Die Karriere, die der Datenschutz in der deutschen Verwaltung gemacht hat, verdankt er auch der Betonung seiner retentiven Elemente, mit denen sich die Verwaltung in eigenen Traditionen bestätigt sah. Die Nichtweitergabe an Dritte (wobei als Dritte allerdings nur die Stellen gesehen wurden, die außerhalb der öffentlichen Verwaltung lagen) ist erst jetzt und aus anderen Gründen bei uns zu einem Problem geworden; tiefgreifende Konflikte mit der Verwaltung gab es bisher in erster Linie dort, wo es um Einsichtsrechte ging.

Da wir uns dem Thema vom Datenschutz her nähern und sich, wie ich meine, die Darlegungslast ohnehin gewendet hat, verweise ich nur stichwortartig auf weitere Begründungszusammenhänge für ein Informationszugangsrecht:

- eine Auslegung des Art. 5 Abs. 1 Satz 1 GG etwa, die vermeidet, daß die Allgemeinzugänglichkeit von Quellen durch deren Inhaber allein bestimmt wird, wenn diese Quellen Akten sind;
- das Gleichheitsgebot, das allzu krassen Verfahren ungleicher Informationsverteilung entgegenwirkt;
- das Demokratie- und Rechtsstaatsgebot.

Nicht heranziehen möchte ich hier spezielle, auch durchaus verfassungsrechtlich relevante Informationsprivilegien: für die Massenme-

dien etwa, für Parlamentarier oder Untersuchungsausschüsse, für Rechnungshöfe. Diese bestehenden und zugleich auch einschränkenden Informationszugangsregeln haben sich zumindest rechtspolitisch eher als Hemmnisse auf dem Weg zu einem allgemeinen Informationszugangsrechts erwiesen - entweder unter der Devise "Wenn uns gegeben wird, wird auch den anderen gegeben" oder "Wenn schon uns nicht gegeben wird, warum dann den anderen?"

3. Lösungsaufgaben des Informationszugangsrechts

Gerade auch die jüngsten Erfahrungen in Brandenburg, aber auch eine lange Beobachtung des kanadischen Systems, das unserer Mentalität vielleicht näher liegt als das amerikanische, haben mir deutlich gemacht, daß es hilfreich sein kann, drei Arten von Problemen zu unterscheiden:

- Konstruktionsprobleme, d.h. Gestaltungsprobleme des rechtlichen Rahmens,

- Bewohnungsprobleme, d.h. Probleme in der täglichen Praxis, die sich nicht allein und nicht immer primär aus den Konstruktionen ergeben, und

- Siedlungsprobleme, d.h. politische Probleme, die Konstruktion und Bewohnbarkeit etwas grundsätzlicher in Frage stellen können als den Rechtsarchitekten lieb sein mag.

3.1 Konstruktionsfragen

3.1.1 Ausnahmen im Interesse der Privatsphäre

Was wird aus dem Schutz der Privatsphäre, was wird aus den Interessen privater Dritter? Das erscheint - vor dem Hintergrund des Datenschutzes - als die zentrale Konstruktionsfrage. Es ist eine Selbstverständlichkeit, die aber, wenn sie schon als solche bezeichnet wird, immer wieder wiederholt werden muß: Es gibt keine Informations-

zugangsregelungen ohne Regelung der Ausnahmen derselben. Das führt zu den Problemen:

- Wer formuliert wie die Ausnahmen?
- Verändert sich das Gewicht von Ausnahmen, bei denen aus Gründen des Datenschutzes eine Weitergabe nicht zulässig war, wenn diese Ausnahmen nunmehr im Kontext eines Informationszugangsprinzips auftauchen?
- Wie ist das Verfahren zu gestalten?

3.1.1.1 Materielle Probleme

Datenschutzrelevante Entscheidungen unter Informationszugangsregeln unterscheiden sich strukturell nicht von Entscheidungssituationen, in denen etwa die Verwaltung über eine Weitergabe an Dritte zu entscheiden hatte. Die brandenburgische Regelung zur Akteneinsicht, soweit sie sich auf personenbezogene Daten bezieht, setzt daher konsequenterweise an den Standardausnahmen der Datenschutzgesetze an:

- Zustimmung,
- gesetzliche Regelung, die Offenbarung zuläßt,
- allgemein zugängliche Quellen, sofern diesen nicht schutzwürdige Belange entgegenstehen.

Die brandenburgische Regelung trägt dem expliziten Verfassungsgebot zusätzlich dadurch Rechnung, daß sie zusätzlich eine Ausnahme der Ausnahme gewährt soweit "aufgrund besonderer Umstände des Einzelfalls im Hinblick auf den Zweck der politischen Mitgestaltung [das ist der verfassungsrechtliche Bezug] das Offenbarungsinteresse des Antragstellers das Interesse der betroffenen Person an der vertraulichen Behandlung der Information überwiegt" (AIG § 5 Abs. 2 Ziff. 3).

Der Gesetzentwurf der Fraktion BÜNDNIS 90/DIE GRÜNEN (BT Drucksache 13/8432 vom 27.08.1997) verfolgt zunächst das gleiche Prinzip, in dem er auf Zustimmung und rechtliche Regelung ver-

weist. Dann hebt er aber einen Personenkreis hervor, der unter besonderen Umständen "öffentlich" ist oder geworden ist: den Amtsträger oder die Amtsträgerin in Ausübung seiner oder ihrer Ämter, allerdings nur mit eben diesen öffentlichkeitszugewandten Daten; weiterhin diejenigen, die sich in den Prozeß der Meinungsbildung öffentlicher Organe öffentlich einbezogen haben oder einbezogen wurden, wie etwa Gutachter, und schließlich solche personenbezogenen Daten, die für den Nachvollzug behördlichen Handelns erforderlich sind. Ein Vortrag ist nicht der Rahmen, diese Regelungen einer detaillierten Prüfung zu unterziehen. Vor dem Hintergrund der Erfahrungen in Ländern mit langer Transparenztradition sollen zwei grundlegende Bemerkungen genügen:

- Der Abgleich der Formulierungen zwischen Datenschutzgesetz und Informationszugangsgesetz ist wichtig, um Auslegungs- und/oder Umgehungsprobleme zu minimieren oder gar nicht erst entstehen zu lassen. Um ein Beispiel zu nennen: Der Zugang zu personenbezogenen Daten ist logisch ein Unterfall des allgemeinen Zugangs; die Verweigerung des Zugangs nach Datenschutzregeln ein Spezialfall der Verweigerung des allgemeinen Zugangs, mit der Ausnahme, daß diese Verweigerung gegenüber dem Betroffenen anders zu gewichten ist als gegenüber einem Dritten. Fallen nur Daten eines bestimmten Formats unter das Datenschutzgesetz, wird der Betroffene auf das Informationszugangsgesetz verweisen, wenn er wegen des Formats vom Datenschutzgesetz ausgeschlossen bleibt; die Ausnahmen des Informationszugangsgesetzes nehmen aber in der Regel nicht darauf Rücksicht, daß der Betroffene in ihn betreffende Unterlagen Einsicht nehmen will. Das Gewicht dieser Probleme sollte man nicht überschätzen; ihre Häufigkeit aber auch nicht unterschätzen.
- Die zweite Bemerkung gilt mittelfristigen Folgen: Dem Datenschutzgesetz sind bereichsspezifische Regelungen gefolgt. Dem Informationszugangsgesetz werden bereichsspezifische Regelungen folgen. So wie die ersteren zur Hauptsache Weitergaberegeln präzisiert haben, werden letztere zur Hauptsache Geheimhaltungs- und Zurückbehaltungsrechte formulieren. Es wird notwendig werden, einen Weg zu finden, der es vor allem auch der Legislative erlaubt, die Kon-

trolle über diese spezifischen Abweichungen zu behalten und insbesondere dieses Geflecht transparent zu machen. Dies ist hier auch ein schon vorweggenommenes Argument für eine spezifische institutionelle Ausgestaltung.

3.1.1.2 Verfassungsfragen

Es bleibt natürlich eine tiefer gehende unausgesprochene Grundsatzfrage: Entkleiden wir für einen Augenblick unser Tun der Rhetorik der praktischen Konkordanz, der wir selbstverständlich alle verpflichtet sind, so bleibt die Kernfrage, ob sich der "Geist der Gesetze" in den bisherigen Informationsgesetzen und ihre Auslegung spürbar wandeln wird; weiter, wie ist denn mit dem Umstand umzugehen, daß Datenschutz seine verfassungsrechtlichen Weihen (schon) - zumindest interpretativ - empfangen hat, der Informationszugang jedenfalls auf Bundesebene noch nicht?

Hier, so meine ich, ist an die Komplementarität zu erinnern. Selbst wenn nur der Datenschutz explizit in die Verfassung aufgenommen würde, wäre eine Formulierung erforderlich, die seinem Transparenzgehalt genügen würde. Beachtet man aber zugleich die symbolische Wirkung einer Verfassungsänderung, so liegt auf der Hand, daß das nachzuvollziehen wäre, was in der letzten Revisionsanstrengung versäumt wurde, nämlich Datenschutz und Informationszugang in ihrer Komplementarität explizit auszuweisen.

3.1.1.3 Verfahren

Zu klären bleibt die Verfahrensfrage. Hat man es im Datenschutz weitgehend hingenommen, daß Weitergabeentscheide von der Verwaltung eigenverantwortlich getroffen werden, so sehen eine Vielzahl ausländischer Regelungen, das brandenburgische Gesetz im § 6 Abs. 3 und der Entwurf der Fraktion BÜNDNIS 90 / DIE GRÜNEN ein abgesetztes - im deutschen Verwaltungsrecht aber keinesfalls unübliches - Anhörungsrecht des Dritten vor. Die brandenburgische Regelung setzt darüber hinaus in bestimmten Fällen die Zustimmung des Dritten voraus (§ 6 Abs. 5).

Zusätzlich werden dem Dritten dann - ohne daß dies im Gegensatz zu anderen Ländern besonders im Informationszugangsgesetz geregelt ist - die üblichen verwaltungsrechtlichen Mittel - wie bei Verwaltungsakten mit Doppelwirkung - an die Hand gegeben. Den Gerichten wird Gelegenheit geboten werden, ihre Erfahrungen aus Baugenehmigungsverfahren im Terrain des Informationsrechts zu erproben.

Die verfahrensrechtlichen Konsequenzen scheinen mir - obwohl doch schon einschlägige Erfahrungen mit dem Umweltinformationsgesetz vorliegen - im übrigen noch nicht voll durchdacht, wenn auch zumindest im Entwurf des Informationsfreiheitsgesetzes angedacht: So ist zu beachten, daß dem betroffenen Dritten Gelegenheit zu geben ist, wirksam Widerspruch einzulegen, so daß zwar der Offenlegungsbescheid an Antragsteller und Dritten gleichzeitig ergehen kann, die Offenlegung in diesen Fällen aber erst nach Ablauf der Widerspruchsfrist, so daß diese Frist den Verzögerungen durch die Aufforderung zur ersten Stellungnahme hinzugerechnet werden muß. Die Erfahrung zeigt jedenfalls, daß es zur Einbindung Dritter keine Alternativen gibt, die von Befürwortern eines besseren Umgangs mit Informationen durch die Verwaltung guten Gewissens vertreten werden könnten, daß andererseits aber diese Art der Einbeziehung die Verfahren erheblich verlängern wird.

Schließlich - so zeigt die ausländische Erfahrung - gibt es auch noch Fälle, in denen es zwar betroffene Dritte gibt, ihre Einbeziehung aber aus verfahrenstechnischen Gründen nicht oder nur sehr schwer möglich sein wird. Auch hierfür muß Vorsorge getroffen werden.

3.1.2 Weitere Ausnahmen

Der Vollständigkeit halber sei noch auf die anderen geregelten und zu regelnden Ausnahmen verwiesen:

- den Schutz von Geschäfts- und Betriebsgeheimnissen,
- den Schutz der Strafverfolgung und Rechtsdurchsetzung,
- den Schutz staatlicher Interessen im Bereich der Verteidigung, Wirtschaft und Außenpolitik.

Über den Geltungsgrund derartiger Ausnahmen bestehen kaum Meinungsverschiedenheiten, eher hinsichtlich ihrer rechtstechnischen Ausgestaltung: Wieviel Spielraum bleibt den Gerichten, wie eng hat der Gesetzgeber diesen Spielraum zu ziehen? Wo sind widerlegbare Vermutungen, wo unumstößliche Geheimhaltungspflichten? Wo sind materielle Abwägungen vorzunehmen? Wo genügen Typenmuster?

Grundsätzlich wichtig scheint mir eine Erkenntnis zu sein, die sich schon längst durch die Entscheidungen in Datenschutzfragen zieht - durch die ausländischer Gerichte zum Informationsrecht einschließlich des inländisch-ausländischen EuGH: Es werden präzise Abwägungen verlangt werden, die sich nicht pauschal auf ein Dokument oder Dokumentenensemble beziehen können, sondern die einzeln den verschiedenen Informationskomplexen nachzugehen haben und darüber hinaus noch verschiedene Teil- und Unterformen der Informationsvermittlung (teilweise Schwärzung, Auskunft statt Einsicht etc.) zu berücksichtigen haben werden. Diese von der Verwaltung eingeforderte größere informationsbezogene Präzision ist durch die Auslegung der Datenschutzgesetze - und der bestehenden bereichsspezifischen Informationszugangsgesetze (Umweltinformationsgesetz) bereits vorbereitet worden. Auch hier jedoch werden weitere gegenstandsbezogene Informationszugangsregelungen notwendig werden. Im Interesse der Transparenz der Transparenzregeln werden wir dann - wie angedeutet - nicht an einer systematischen Zusammenfassung und Fortführung von Geheimhaltungsregeln vorbeikommen, wie dies etwa im schwedischen Sekretesslag oder im entsprechenden Schedule des kanadischen Bundesgesetzes zum Informationszugang fortlaufend geschieht.

3.1.3 Institutionelle Einbindung

Das zweite Lieblingsthema in der Diskussion über Informationszugang und Datenschutz in Deutschland ist die institutionelle Einbindung. Damit hat die Diskussion bereits einen wesentlichen Fortschritt gemacht: Das Ob der institutionellen Einbindung steht nicht mehr in Frage. In der Tat zeigen die ausländischen Beispiele auch jenseits einer gewissen Vorliebe deutscher Rechtskultur für die Versinnlichung von Recht durch den oder die Beauftragte, daß Rechts-

veränderungen einer institutionellen Begleitung bedürfen und zwar gleichermaßen für Berechtigte wie für Verpflichtete.

Zum Wie gibt es im wesentlichen zwei Modelle, das integrative oder das antagonistische, wobei letzteres zumeist Kooperationsmodell genannt wird. Seltsamerweise hat sich in dem Land, das als erstes die vollen Auswirkungen des Zusammenwirkens von Informationszugang und Datenschutz national erkannt hatte, in Kanada, auf Bundesebene aufgrund historischer und politischer Zufälligkeiten trotz einer anderen gesetzlichen Möglichkeit das antagonistische Element durchgesetzt, während in einem Land wie Frankreich, wo man sich zu Anfang gar nicht des Zusammenhangs zweier kurz hintereinander verabschiedeter Gesetze bewußt war, sich zwischen beiden Institutionen trotz anfänglicher Schwierigkeiten, aber dank gemeinsamer sekundärer und tertiärer Sozialisation, eine gute Zusammenarbeit entwickelt.

Das verweist auf ein anderes in der Diskussion immer wieder anklingendes Motiv, das Vergleichen zwischen Rechtsordnungen vor allem im öffentlichen Recht eine Dissonanz mitgibt: Unterschiede in Verwaltungskulturen, in Verwaltungsstilen, wenn man schon nicht von Kultur sprechen möchte. Neben all den haushaltsrechtlichen und verwaltungspraktischen Argumenten, den Hinweisen auf erworbene Anerkennung und erworbenes Wissen um Informationszugänge scheint mir dies ein zusätzliches Argument für die Zusammenlegung von Informationszugangs- und Datenschutzbeauftragten zu sein: Die Datenschutzbeauftragten sind die Einrichtungen, die der Verwaltungskommunikation bisher am nächsten standen, die so auch wahrgenommen werden und die ihre Stile mit den Verwaltungen gefunden haben. Sie sind daher auch mit der Aufgabe des Informationszugangsbeauftragten zu betrauen. Das wird sie nicht - wie die ausländische Erfahrung zeigt - vor gelegentlich schwierigen Abwägungen bewahren und es wird an ihnen liegen, jenes Organisationsmuster zu finden, daß diesen Entscheidungsprozeß intern optimiert. Wobei ohnehin zu beachten sein wird, daß in unserem System diesen Beauftragten zwar eine möglicherweise verfügende, aber keine streitentscheidende Funktion zukommen wird.

3.2 Probleme der Bewohnbarkeit

3.2.1 Aktive Information und Informationsroutinen

Mein kurzer Exkurs in den verwaltungsrechtlichen und verwaltungsgerichtlichen Alltag hat es schon angedeutet: Die gesetzliche Regelung des Informationszugangs wird zu einer Verförmlichung der Informationsbeziehungen zwischen Bürgerinnen und Bürgern führen. Das ist zwangsläufig so: Durch Informationszugangsgesetze werden Privilegierungen zwar nicht völlig beseitigt - informelle Informationskanäle, gezielte Indiskretionen wird es weiterhin genau so geben wie Mauern oder Verschleiern oder Beschönigen. Der Gewinn an Gleichheit, die Möglichkeit der Erzwingung, der Druck, der auf Verhalten ausgeübt wird, wird mit Formalisierung erkauft werden müssen.

Freilich - ähnlich wie beim Datenschutz, der doch zunehmend von den Verwaltungen auch als "learning teaching system", als lernendes Lehrsystem wahrgenommen wird, besteht mit der Regelung des Informationszugangs die Möglichkeit einer mittel- bis langfristigen Verhaltensänderung. Zwar muß dieser Anstoß durch Gesetz erfolgen, da andernfalls Verwaltungen erfahrungsgemäß Ressourcenverlagerungen weder nach innen noch nach außen wirksam rechtfertigen können. Die Anpassung wird jedoch ihre eigenen verwaltungsökonomischen Gesetzmäßigkeiten entfalten. Zum einen erlegen alle Informationszugangsgesetze im internationalen Vergleich aktive Informationspflichten auf, die mir im brandenburgischen Gesetz überhaupt nicht und im zitierten Gesetzentwurf nur sehr unzureichend entwickelt scheinen. Auch hier muß der Anstoß aber durch Gesetz erfolgen; die Verwaltungen werden sehr bald wahrnehmen, daß sich Informationsanfragen erübrigen bzw. leichter bearbeiten lassen, wenn sie derartige Metahilfen zur Verfügung stellen. Auch bei der Bearbeitung einzelner Informationsanfragen wird sich die Praxis entwickeln, zwischen bereits entschiedenen und noch zu entscheidenden Informationsbeständen zu unterscheiden und bei ersteren die Weitergabe zu routinisieren. Hinzu kommen die neuen informationstechnischen Möglichkeiten, die die Verbreitung von Information und ihre gleichzeitige innerorganisatorische Nutzung erheblich erleichtern. Diese Überlegungen haben in den USA zur Verabschiedung des Electronic Freedom of Information Act geführt.

Auch andere Reformgedanken und ihre ja schon lange anhaltende Umsetzung mögen mit zur Wahrnehmung beitragen, daß Verwalten in erster Linie einen angemessenen Umgang mit Informationen erfordert. Auch zu diesem an Informations- und Kommunikationsmanagement orientierten Verhalten hat die Implementationsgeschichte des Datenschutzes in Deutschland zumindest in einigen Teilen der öffentlichen Verwaltung beigetragen.

3.2.2 Kommerzialisierung

Das neuere serviceorientierte Managementdenken hat und wird allerdings auch andere Folgen mit sich bringen: Vielfach zählen die Informationsbestände zu den wenigen Ressourcen von wirtschaftlichem Wert, die Verwaltungen besitzen. Bestimmte Informationsbestände können auch ganz plötzlich ungeahnten wirtschaftlichen Wert erhalten. Aufgrund der Anforderungen kosteneffizienter Verwaltung, der Public-Private-Partnerships und nicht zuletzt aufgrund der Versuchungen vor allem im gemeindlichen Bereich, Vorteile staatlichen Handelns mit den Vorteilen des privatrechtlichen Formenreichtums zu verbinden, liegt es nahe, Bestände zur unmittelbaren oder mittelbaren Vermarktung, Teil- oder Vollprivatisierung vorzubereiten.

Die Konsequenzen für den Informationszugang liegen auf der Hand: Vermarktung und Informationszugangsrecht können hinsichtlich des gleichen Informationsbestandes und gleicher Retrievalmöglichkeiten nicht koexistieren. Selbst wenn noch gelegentlich die Tendenz besteht, das Gebührenrecht als Prohibitionsgesetz gegen den möglichen Rausch des Informationszugangs einsetzen zu wollen, wird sich aus eben diesen gebührenrechtlichen Grundsätzen ein Preis in Nähe der Grenzkosten der Verteilung einpendeln, die bei elektronischer Verteilung gegen Null tendieren. Das mag man bedauern, aber es scheint mir unaufhaltsam. Daneben aber können langfristig Informationen gleicher Art und Güte nicht vermarktet werden, abgesehen von Problemen, die im Bereich personenbezogener Informationen weiterhin bestehen bleiben werden. Dagegen werden sich zwei Strategien entwickeln, die bereits jetzt wahrzunehmen sind, leider vor allem auf der Ebene der europäischen Institutionen, die Transparenz so sehr betont haben. Die eine Strategie besteht darin, zwar nicht die zugängliche oder allgemeinzugänglich zu haltende Information zu

beschränken, statt dessen aber ihre Handhabbarkeit erheblich einzuschränken. Aktuelle Gerichtsurteile stehen zwar im Volltext zur Verfügung, aber nur für einen begrenzten Zeitraum, Gesetzestexte werden zwar elektronisch veröffentlicht, aber nur so, daß ein Lesen des gesamten Textes nur unter physischen und elektronischen Kraftanstrengungen möglich ist; oder Informationen werden, obwohl elektronisch vorhanden, nur in Papierform herausgegeben.

Die andere Strategie besteht darin, Informationsbestände ganz aus der öffentlichen Hand zu geben und die Bürgerinnen und Bürger darauf zu verweisen, sie sich zu Marktpreisen zu beschaffen, während die Verwaltungen selbst auf diese Informationen weiter zu Präferenzpreisen zugreifen können.

Neuere urheberrechtliche Entwicklungen scheinen Vermarktungstrends eher zu unterstützen: Die Datenbankrichtlinie verlangt von den Mitgliedsstaaten explizit zu sagen, daß sie auf ihr sui generis-Recht hinsichtlich ihrer Datenbanken verzichten; im Rahmen des Urheberrechtes ist das gesetzlich selbstverständlich gewesen. Wie leicht sich die öffentliche Verwaltung hier von ihr zugefallenen Rechten trennen wird, bleibt abzuwarten.

Aber auch vor dem anderen Weg ist zu warnen: Gelegentlich wird gefordert, man solle die weitere kommerzielle Nutzung durch private Dritte zumindest gebührenrechtlich schlechter stellen als die Informationsanfragen der Bürgerinnen und Bürger, denn schließlich verfolgten die einen ihr Bürgerrecht, die anderen aber würden die Verwaltung in diesen Fällen als billige Informationsquelle mißbrauchen.

Dem ist entgegenzuhalten:

- Die Möglichkeit, gegenüber der Informationsindustrie höhere Gebühren zu verlangen, ist verführerisch; sie wird über kurz oder lang die Verwaltungen veranlassen, ihre Informationsressourcen eher nach den Bedürfnissen dieser zahlungskräftigen Abnehmer auszurichten, auch wenn sie selbst dem Informationsmarkt fernbleiben wollen.

- Eine solche Regelung wird europarechtlich bedenklich, wenn andere europäische Verwaltungen gegenüber deutschen

Nachfragern aufgrund ihrer Regelungen Informationen kostenlos abgeben.

- Auch die Unternehmen haben mit ihren Steuern zur Produktion dieser Informationen beigetragen; gerade kleinere und mittlere Unternehmen der Informationsindustrie in Deutschland könnten zur Belebung der Informationsversorgung beitragen. Die kostenlose Abgabe der Informationen könnten sie aus den dargestellten Gründen ohnehin nicht dazu mißbrauchen, die Informationen, so wie sie sie erhalten haben, zu verkaufen, denn die Bürgerinnen und Bürger können sie ebenfalls kostenlos direkt von der Verwaltung erhalten.
- Und schließlich: Die Verwaltungen wären gezwungen, das zu tun, was sie im Interesse der Informationsfreiheit nicht tun sollten, nämlich nachzuforschen, was denn mit den angefragten Informationen geschehen soll. Wird die Bürgerinitiative Hochglanzbroschüren verkaufen, um sich notwendige zusätzliche Ressourcen zu verschaffen? Oder gibt sie sie bloß kopiert weiter? Wer soll das kontrollieren? Eine ähnliche Regelung in Frankreich hat sich jedenfalls nicht bewährt und sie ist in Belgien, das die französische Regelung kritiklos kopiert hatte, vor ihrem Scheitern.

Die Zukunft der Informationsgesellschaft in Deutschland wird nicht erleichtert, wenn von vornherein die Interessen der Informationsindustrie gegen die Interessen der Bürgerinnen und Bürger ausgespielt werden sollen. Warum nicht Regelungen finden, die Bürgerinnen und Bürgern *und* diesem sich entwickelnden Wirtschaftszweig zugute kommen. In den USA scheint das gelungen zu sein. Das wird allerdings voraussetzen, in Zukunft politisch deutlicher und genauer zu definieren, was in die Informationsverantwortung des Staates fallen wird und wie er hier Qualität und Nachhaltigkeit sichern wird.

3.2.3 Machtverlust

Ich komme zum dritten Problem - keinem eigentlich juristischen -, aber dafür wichtigen Problem: Information ist nicht nur gelegentlich die einzige wirtschaftliche Ressource, die der Verwaltung geblieben ist, sie ist weithin schlicht die einzige und letzte Machtressource, die

der Verwaltung geblieben ist. Das gilt vor allem dort, wo die Verfügung über Geldmittel eingeschränkt wird oder eingeschränkt worden ist, unmittelbarer Zwang nicht opportun ist und die Wirkungsmöglichkeiten über Status sich wegen der großen Nähe nicht so einfach herstellen. Das ist der Bereich der lokalen Verwaltung.

Wir erinnern: Unter Datenschutzaspekten war und ist hier das Konzept der informationellen Gewaltenteilung besonders hart auf das Verständnis von der Verwaltung als Einheit getroffen. Das Auslagern weiterer Verwaltungsfunktionen auf die Städte und Gemeinden bei sinkenden finanziellen Ressourcen, der Druck bürgerfreundlicher zu werden in einem Klima der Verwaltungsfeindlichkeit, stärkt diesen umfangreichen Teil unserer öffentlichen Verwaltungen in ihren Befürchtungen vor Informationszugangsgesetzen. Hinzu kommt, daß diese Verwaltungen im Pflichtaufgabenbereich nach Weisung zwar als lokale Verwaltung wahrgenommen, in ihren Handlungsmöglichkeiten aber beschränkt, wenn nicht gar fremdgesteuert sind. In der Beziehung zwischen lokalen Parteien und Verwaltung, aber auch zwischen Verwaltung und zu Verwalteten stand und steht - gewissermaßen notgedrungen - Steuerung durch Information synonym für Politik *und* Verwaltung. Zumindest potentiell werden hier dann gesetzlich, im Einzelfall aber unvorhersehbar Informationen dieser Verfügungsmöglichkeit entzogen. Es steht zu erwarten, daß hier die nun wirklich allerletzte Ressource, über die Verwaltung verfügt, verstärkt eingesetzt werden wird, ohne daß dies durch Regelungen ausreichend eingegrenzt werden kann: Zeit. Zeitablauf ermöglicht gegebenenfalls, Einsichtsansprüchen ihre mögliche politische Brisanz zu nehmen. Die Verwaltung wird ihre Möglichkeit, über die Zeit verfügen zu können, voll ausschöpfen. Aus der Sicht der Bürgerinnen und Bürger bedeutet dies: Die Zeitdauer zwischen Antrag und Bescheidung wird zum größten praktischen Problem werden. Dieses Problem wird auch - wie die ausländische Erfahrung zeigt - nur schwer durch Regelungen zu kontrollieren sein. Der Verwaltung wird der Rückgriff auf Ausnahmeregelungen im jeweiligen Einzelfall kaum zu nehmen sein.

Ich habe hier nur drei Probleme des täglichen Lebens mit Informationszugangsgesetzen herausgegriffen, die mir struktur- und entwicklungsbedingt zu sein scheinen. An all die anderen Probleme braucht hier nicht weiter erinnert zu werden; auch hier hat uns der

Datenschutz reichlich Gelegenheit gegeben zu erfahren und zu lernen: Tendenzen rechteminimierender Auslegung, Beschwerlichkeit des Rechtsweges, mangelnde Lernfähigkeit von Verwaltungen, aber auch Kleinlichkeiten und Rechthabereien bei den Verwalteten.

Wir stehen aber - unabhängig von der Existenz oder Nichtexistenz, unabhängig vom guten oder schlechten Funktionieren informationsrechtlicher Regelungen - vor einem größeren, vor einem - um im Bild zu bleiben - Siedlungsproblem.

3.3 Siedlungsprobleme der Informationsordnung

Ich will es hier - wenn ich so sagen darf - im Rahmen unserer Diskussionen um mittlere Reichweiten nur ansprechen:

Es gelingt uns nicht, Austauschbeziehungen zwischen Bürgerinnen und Bürgern einerseits und staatlichen Institutionen anderseits so zu gestalten und weiter auszugestalten, daß sie durchschaubar und nachvollziehbar werden. Dies gilt sowohl für das Steuer- und Abgabensystem wie für die Systeme der sozialen Sicherung. Beides sind Bereiche, in denen technisch gestützte Informationssysteme eine ganz erhebliche, wenn nicht gar schon allein systemerhaltende Bedeutung bekommen haben und die sowohl hinsichtlich ihrer Auswirkungen auf die Privatsphäre als auch in ihrer strukturellen Intransparenz verfassungsrechtlich relevant geworden sind.

Der Prozeß der Ausdifferenzierung, der Professionalisierung - die Begleitmusik der Moderne - hat vielfältige Ursachen und Wirkungen. Ich verweise hier auf einen Beitrag von Frau Verfassungsrichterin Jaeger zum System der sozialen Sicherung in Deutschland und seinem sozialen Kontext in Europa. Sie hat darin deutlich gemacht, wie wenig wir von diesem System und seinen Alternativen wissen, wie viel von diesem System zu wissen wäre und wie es gestaltbar wäre, so daß man es verstehen kann (in Lamnek/Tinnefeld: Globalisierung und Rechtskultur in Europa, Baden-Baden 1998, 65ff.).

Hierzu werden uns Informationszugangsgesetze allein nicht verhelfen, auch wenn sie weitreichende, aktive Informationspflichten enthalten werden. Aber vielleicht werden die komplementären Informa-

tionszugangsregeln und die Erfahrung mit ihnen dazu führen, daß sich auch für den Bereich des Informationszugangs ein Minimalprinzip durchzusetzen beginnt. Wird im Datenschutz immer deutlicher, wie wichtig die Vermeidung von personenbezogenen Daten ist, wie wichtig es ist, zwar eindeutig kennzeichnende, nicht aber identifizierende Systeme zu entwickeln, so wichtig wird es werden, Systeme zu entwickeln, die mit einem tendenziellen Minimum an erläuternden, differenzierenden Informationen auskommen, so daß sie mit einem Minimum an Transparenzregeln versehen werden müssen, weil sie bereits strukturell transparent sind.

Das freilich würde von uns auch ein gewandeltes Verständnis von Verteilungssystemen voraussetzen, aber vielleicht kann die Wahrnehmung der informationsökologischen Probleme auch hier zu einem allmählichen Bewußtseinswandel beitragen.

Und schließlich: Täuschen wir uns nicht, die Forderung nach Transparenz, nach Information ist die Einstiegsdroge für Beteiligung. Systeme, die für unser tägliches Wohlergehen immer wichtiger werden, die Netzsysteme des Verkehrs etwa oder der Telekommunikation, müssen nicht nur transparenter werden, sie werden sich auch Verfahren zu öffnen haben, an denen sich unmittelbar Betroffene stärker und wirksamer beteiligen können als vermittelt über Regulierungs- und Aufsichtsinstanzen. Beispiele finden sich bei Public Utility Verfahren in Nordamerika.

Diese Entwicklung wiederum wird ein Thema wichtig werden lassen, das wir im Datenschutz glücklicherweise hinter uns gelassen haben: die Frage der Drittwirkung von Informationszugangsrechten. Aber wir wollen unseren kleinen Bauplatz für das Eigenheim eines Informationszugangsgesetzes noch nicht mit langfristigen Siedlungsplänen belasten.

4. Schlußbemerkung

Sprach man anläßlich des Volkszählungsurteils noch ernsthaft von verfassungswidrigen Verfassungsgerichtsentscheidungen und Fragen ihrer Gültigkeit - gibt es ein Widerstandsrecht gegen den Datenschutz? - so gehört es mittlerweile zum guten Ton, ist es politically

correct, einem "hypertrophen Datenschutz" nunmehr "Informationszugangsrechte" entgegenzustellen. Nun, man vergißt sehr leicht, daß das allererste Datenschutzgesetz - das Hessische, das übrigens auch das erste in Deutschland bei der Umsetzung der EU-Richtlinie ist, [für Griechenland und Italien gilt eher der Satz, wer zu spät kommt, den belohnt die EU] - starken, wenn auch privilegierenden Informationszugangsaspekten Rechnung trug. Man vergißt, daß seit beinahe zwanzig Jahren die Bundesrepublik Deutschland in der Verpflichtung der erwähnten Ministerratserklärung des Europarats stand, allgemeine Informationszugangsrechte in nationales Gesetz umzusetzen.

Ich führe diesen selbstverständlichen "Wandel in der Verkehrsanschauung" allein aus zwei Gründen an:

Aus Dankbarkeit: Wir haben diese Entwicklung den Folgen des Jahres 1989 zu verdanken; sie ist - verspätet - ein Teil der Verfassungsbeeinflussung durch das Volk, das noch frische Erfahrungen mit Intransparenz hatte. Zum anderen um uns zu wappnen: Wenn wir erst im Alltag des Informationszugangs sind, sollten wir den Argumenten von der Hypertrophie des Informationszugangs mit einem Lächeln begegnen können, mit einem wissenden Lächeln.

Unlauterer Wettbewerb durch Datenschutzverstöße

Thomas Hoeren/Sven Lütkemeier *

I. Einführung

A. Schwächen des Datenschutzes im nicht-öffentlichen Bereich

Der Datenschutz in der Privatwirtschaft ist in letzter Zeit zunehmend in den Blickwinkel gerückt.[1] Nach über 20 Jahren Bundesdatenschutzgesetz (BDSG) werden immer noch erhebliche Vollzugsdefizite gerade im Bereich der Wirtschaft[2] beklagt. Teilweise wird das BDSG in diesem Bereich sogar für allenfalls partiell wirkungsfähig gehalten.[3] Wiederholt stellen Aufsichtsbehörden eine hohe Quote an Mängeln fest.[4] So werden etwa entgegen § 36 BDSG entweder gar keine Datenschutzbeauftragte bestellt oder ihnen keine ausreichenden Mittel zur Erfüllung ihrer Aufgaben zur Verfügung gestellt.[5] Einer der Gründe hierfür liegt in der Orientierung des BDSG an den

---

* Der folgende Text gibt den Vortrag wieder, den der Verfasser (Thomas Hoeren) in Münster gehalten hat. Der Vortragsstil wurde beibehalten; die Fußnoten geben nur zentrale Belege wieder. Sven Lütkemeier hat das Manuskript erstellt und den Inhalt des Vortrages um eigene Ideen bereichert, die auch Gegenstand seiner Dissertation sind.

1 vgl. z.B. Hassemer, DuD 1995, 448 (449); Nitsch, ZRP 1995, 361 (365).

2 Gola, NJW 1997, 3411 (3418) m.w.N.

3 v. Westerholt, Festschrift für Beier (1996), 561 (574).

4 vgl. LReg NRW, 5. TB DS im nicht-öffentlichen Bereich (1995/1996), Gliederungspunkt 1.4.

5 vgl. LReg Hessen, 10. TB DS im nicht-öffentlichen Bereich (1996), LT Drucksache 14/3086 v. 1.8.1997, Gliederungspunkt 16.

Datenverarbeitungssystemen der 70er Jahre. Einige Instrumente sind durch den zwischenzeitigen technischen Fortschritt überholt, neue Instrumente sind erforderlich.[6] Eine weitere Hauptursache liegt in der großen Unbestimmtheit der BDSG-Bestimmungen. Diese Unbestimmtheit mag angesichts der Weite des Regelungsgegenstandes, der sämtliche Verarbeitungssituationen abdeckt, gleich zu welchen Zwecken welche Art personenbezogener Daten verarbeitet werden, unvermeidbar sein.[7] Die Häufung von Generalklauseln, die weitgehend beliebig auslegbar zu sein scheinen,[8] führt aber dazu, daß das Ziel des BDSG, die Datenverarbeiter zu einer kritischen Überprüfung ihrer Verarbeitungswünsche mit Blick auf die Belange der Betroffenen zu veranlassen, nicht erreicht wurde. Unter dem Deckmantel der Generalklauseln lassen sich Verarbeitungswünsche als berechtigte Interessen leicht rechtfertigen.[9] Dem 1978 von Sasse erhobenen Vorwurf, der Gesetzgeber habe mit dem BDSG nur scheinbar die Datenverarbeitung im privaten Bereich geregelt und die Regelung tatsächlich der praktischen Anwendung durch die betroffenen Personen überlassen,[10] wurde auch mit der Novellierung des BDSG im Jahre 1990 nicht der Boden entzogen.

B. Unzureichende Sanktionierung von Datenschutzverstößen

Diese konzeptionelle Schwäche des BDSG wird noch durch das tatsächlich weitgehende Leerlaufen der vorgesehenen Sanktionen bei Datenschutzverstößen verstärkt. Soweit das BDSG nicht der Selbstkontrolle der Datenverarbeiter vertraut, gibt es den Aufsichtsbehörden nur wenige Zwangsmittel in die Hand, mit denen die tatsächliche Beachtung des Datenschutzrechts durchgesetzt werden könnte (vgl. § 38 V BDSG). Hinzu tritt eine oft unzureichende sachliche und personelle Ausstattung der Aufsichtsbehörden.[11] Zwar werden im Rahmen der Anpassung des BDSG an die Vorgaben der EG-

6 Garstka, MMR 1998, 449 (450); Hassemer, DuD 1995, 448 (448); Nitsch, ZRP 1995, 361 (363).
7 vgl. Simitis in Simitis u.a., BDSG, § 1 Rdnr. 16.
8 Nitsch, ZRP 1995, 361 (363).
9 Simitis in Simitis u.a., BDSG, § 1 Rdnr. 16.
10 Sasse, Festschrift für W. Mallmann (1978), 224 ff. (225 f).
11 Wind, Die Kontrolle des Datenschutzes im nicht-öffentlichen Bereich (1994), S. 46 u. 172.

Datenschutzrichtlinie[12] weitergehende Zwangsmittel der Behörden eingeführt werden müssen (vgl. Art. 28 III EG-DSRl), es muß aber bezweifelt werden, ob die mangelhafte Ausstattung der Behörden angesichts knapper Finanzen der öffentlichen Hand in absehbarer Zeit behoben werden wird. Auch die Ansprüche, die das BDSG den Betroffenen selbst einräumt, haben in der Praxis keine Abhilfe gebracht. Die Gründe hierfür liegen auch hier nicht zuletzt in der offenen Formulierung und Unbestimmtheit der einschlägigen Vorschriften, die eine Klage des Betroffenen auf Löschung oder Berichtigung seiner Daten (§ 35 BDSG) mit einem nicht unerheblichen Prozeßrisiko belastet.[13] Hinzu tritt ein oft geringes Interesse der Betroffenen an einer gerichtlichen Durchsetzung ihrer Rechte, da eine Beeinträchtigung durch rechtswidrige Datenverarbeitung außerhalb einiger sensibler Bereiche (Arbeitsplatz, Bankgeschäfte u.ä.) oft nicht wahrgenommen wird.[14] Aber selbst wenn ein Betroffener zum Beispiel seinen Anspruch auf Löschung seiner Daten erfolgreich durchsetzt, bewirkt dies für den Verarbeiter kaum einschneidende Folgen. Erhebliche Schadensersatzforderungen braucht er nicht zu fürchten, da ein Ersatz für nicht-materielle Schäden (also für die rechtswidrige Verarbeitung der Daten selbst) regelmäßig nicht erfolgen wird.[15] Die Straf- und Bußgeldvorschriften, die §§ 43 f. BDSG vorsehen, können ebenfalls keine tatsächliche Beachtung des BDSG sicherstellen. Die Bußgeldvorschrift des § 44 BDSG bezieht sich nur auf Verstöße gegen bestimmte formale Vorschriften des BDSG, meist in Zusammenhang mit dem Zusammenspiel zwischen Aufsichtsbehörde und Datenverarbeiter. Die Strafvorschrift des § 43 BDSG sieht sich erheblichen verfassungsrechtlichen Bedenken ausgesetzt, da in sie alle Unsicherheiten, die bei der Anwendung des BDSG auftreten, einfließen.[16] Die präventive Wirkung ist durch den geringen Bekanntheitsgrad beeinträchtigt.[17] Zudem ist eine Strafverfolgung nur auf Antrag des Betroffenen möglich (§ 43 IV BDSG). Der Betroffene muß also

---

12 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Amtsblatt Nr. L 281 vom 23.11.1995.

13 v. Westerholt, Festschrift für Beier (1996), 561 (574).

14 v. Westerholt, Festschrift für Beier (1996), 561 (574).

15 vgl. Schneider, CR 1993, 35 (39).

16 vgl. Dammann in Simitis u.a., BDSG, § 43 Rn. 8.

17 vgl. Dammann in Simitis u.a., BDSG, § 43 Rn. 8.

erst einmal Kenntnis von der unrechtmäßigen Verarbeitung seiner Daten erlangen. Bei seiner Entscheidung über einen Strafantrag wird dann auch wieder das oft geringe subjektive Interesse an der Nicht-Verarbeitung seiner Daten eine Rolle spielen. Verurteilungen aufgrund dieser Vorschrift sind nicht ersichtlich. Die Sanktionen für BDSG-Verstöße bewirken wegen der beschriebenen Unzulänglichkeiten keinen "gesunden Druck"[18] auf die Datenverarbeiter, von sich aus zur Vermeidung von einschneidenden Sanktionen die Einhaltung des Datenschutzes sicherzustellen.

C. Nutzung von Sanktionen des Wettbewerbsrechts

Angesichts der unzureichenden Instrumente, die das derzeitig geltende Datenschutzrecht selbst zu seiner tatsächlichen Durchsetzung vorsieht, ist zu überlegen, ob die Sanktionen anderer Rechtsgebiete für den Zweck des Datenschutzes nutzbar gemacht werden können, um den erforderlichen "gesunden Druck" zur Einhaltung des Datenschutzrechts auszuüben. In diesem Zusammenhang erscheint ein Blick auf das Wettbewerbsrecht besonders vielversprechend. Dieses Rechtsgebiet ist hauptsächlich im Gesetz gegen den unlauteren Wettbewerb (UWG) normiert. Es stellt insbesondere über die Verbandsklagen des § 13 UWG und das vorgeschaltete Abmahnwesen hoch wirksame Sanktionen bereit. Selbstverständlich ist es aber nicht möglich, diese Sanktion, so hilfreich sie auch dem Datenschützer erscheinen mag, einfach aus dem UWG "auszuleihen". Das UWG darf nicht zum Sheriff des ordnungsgemäßen Vollzuges aller möglichen Gesetze gemacht werden.[19] Eine Verbandsklage nach § 13 UWG ist nur zur Durchsetzung eines wettbewerbsrechtlichen Anspruchs möglich. Es kommt also darauf an, ob ein Verstoß gegen das Datenschutzrecht zugleich auch einen solchen Anspruch auslöst. Dies erscheint angesichts der zunehmenden Bedeutung, die Informationen für den wirtschaftlichen Erfolg eines Unternehmens haben durchaus nicht abwegig. Informationen sind zu einem Wirtschaftsgut geworden.[20] Diese Informationen bestehen oft aus personenbezogenen Daten (z.B. Anschriftenliste, Einsatzprofile einer Kreditkarte…) oder sind aus ihnen gewonnen worden (z.B. Marktforschungsergeb-

18 Schneider, CR 1993, 35 (39).
19 Tilmann, GRUR 1991, 796 (798).
20 Büllesbach, RDV 1997, 239 (239).

nisse, die sich nicht mehr auf individuelle Personen beziehen, sondern nur noch statistische Aussagen enthalten). Der Umgang mit personenbezogenen Daten wird durch das Datenschutzrecht reguliert, um Beeinträchtigungen für das Persönlichkeitsrecht der betroffenen Personen zu vermeiden (§ 1 I BDSG). Sind Informationen einerseits für den Erfolg eines Unternehmens im Wettbewerb entscheidend und ist andererseits der Umgang mit ihnen durch das Datenschutzrecht beschränkt, so sind Wechselbeziehungen zwischen dem Wettbewerbsrecht - der Regulierung des Wettbewerbsverhaltens - und dem Datenschutzrecht naheliegend. Angesichts dieses Zusammenhangs zwischen Datenschutz und Wettbewerb überrascht es nicht, daß sich in der veröffentlichten Rechtsprechung mehrere Entscheidungen finden, die wettbewerbsrechtliche Ansprüche auf die Verletzung von Datenschutzbestimmungen stützen. Soweit ersichtlich fand die Thematik einen ersten Anklang in einer Entscheidung des OLG Köln vom 26.3.1982.[21] Da allerdings in dem zu entscheidenden Fall ein Datenschutzverstoß verneint wurde, mußte sich das OLG nicht näher mit dem Verhältnis von BDSG und UWG befassen. In der Folgezeit schien die Problematik lange Zeit in Vergessenheit geraten zu sein,[22] wenn auch der BGH bestimmte Formen der verdeckten Laienwerbung, bei denen ein Unternehmen seine Kunden bittet, ihm mögliche Neu-Kunden aus dem Freundes- und Bekanntenkreis zu nennen, unter anderem auch in Hinblick auf die datenschutzrechtlich bedenkliche Datenerhebung bei Dritten ohne Kenntnis der Betroffenen als wettbewerbsrechtlich unzulässig angesehen hat.[23] Ins Rampenlicht gerückt ist die Schnittstelle zwischen UWG und BDSG schließlich Mitte der 90er Jahre im Zusammenhang mit den Auseinandersetzungen um Telefonbuch-CD-ROMs. Hier hat das LG Mannheim die wettbewerbsrechtliche Unzulässigkeit des Vertriebes einer solchen CD-ROM unmittelbar auch auf einen Verstoß gegen § 4 I BDSG gestützt.[24] In ähnlich gelagerten Fällen haben sich etliche Gerichte dieser Argumentation angeschlossen.[25] Im Fall einer Lifestyle-

---

21 OLG Köln, WRP 1982, 540 = Simitis u.a., BDSG Dok. § 24 BDSG 1977 E 4.

22 vgl. v. Westerholt, Festschrift für Beier (1996), 561 (561).

23 BGH, Verdeckte Laienwerbung, NJW 1992, 2419 (2419).

24 LG Mannheim, D-Info 2.0, NJW 1996, 1829 (1831) = CR 1996, 411 m. Anm. Wuermeling.

25 vgl. OLG Koblenz, DuD 1999, 357; LG Hamburg, CR 1997, 21; LG Stuttgart, CR 1997, 83; LG Mannheim, CR 1996, 672; LG München I, CR 1998, 83.

Befragung[26] hat das LG Stuttgart ebenfalls die datenschutzwidrige Datenerhebung und -speicherung als Grundlage eines wettbewerbsrechtlichen Anspruchs herangezogen.[27] Anderer Auffassung war das OLG Frankfurt, das einen wettbewerbsrechtlichen Unterlassungsanspruch aufgrund eines Datenschutzverstoßes ablehnte.[28] Im Schrifttum wurde bis vor kurzem das Thema UWG/BDSG nur sehr knapp behandelt. So hat Knauth in den 80er Jahren im Zusammenhang mit dem von einigen Banken angebotenen Umzugsservice erwogen, daß ein Datenschutzverstoß unter Umständen einen wettbewerbsrechtlichen Anspruch auslösen könne.[29] Auch in der Literatur wurde das Thema dann erst wieder in den 90er Jahren aufgegriffen.[30] Eine umfassende Darstellung der Thematik ist allerdings bisher noch ausgeblieben.

II. Wettbewerbsrechtliche Folgen von Datenschutzverstößen

Das UWG enthält neben zwei Generalklauseln (§§ 1, 3 UWG) eine Reihe von Sondertatbeständen, die sich insbesondere mit bestimmten Werbeformen und Arten von Sonderverkäufen befassen, jedoch keine erkennbare Affinität zum Datenschutzrecht aufweisen. Datenschutzverstöße können also nur im Rahmen der beiden Generalklauseln Bedeutung erlangen.

A. Datenschutzverstöße und § 3 UWG

Die "kleine Generalklausel" des § 3 UWG verbietet es, im geschäftlichen Verkehr zu Zwecken des Wettbewerbs irreführende Angaben zu machen. Ein Rechtsverstoß, der im Zusammenhang mit einem angebotenen Produkt oder einer Dienstleistung steht, wird eine solche Irreführung nur in Ausnahmefällen bewirken.[31] Regelmäßig wird der Anbieter keine Angaben über die datenschutzrechtlichen Fragen machen; es ginge zu weit, anzunehmen, das bloße Angebot einer

---

26 vgl. hierzu Breinlinger, RDV 1997, 247 ff.
27 LG Stuttgart, RDV 1998, 262.
28 OLG Frankfurt/Main, CR 1997, 275 (282).
29 Knauth, in Amann/Lambsdorff, RWW 5.1 Rn. 385.
30 v. Gamm, GRUR 1996, 574 ff., v. Westerholt, Festschrift für Beier (1996), 561 ff., Wuermeling, CR 1996, 414 f.
31 Baumbach/Hefermehl, § 1 UWG Rn. 646.

Ware enthalte die stillschweigende Aussage, daß keine Rechtsverstöße in Zusammenhang mit dieser Ware begangen worden seien.[32] Bedeutung gewinnt § 3 UWG aber zum Beispiel in Hinblick auf das diskutierte Datenschutzaudit: eine unberechtigte Werbung mit einer Auditierung, die tatsächlich gar nicht erfolgt ist, würde gegen § 3 UWG verstoßen und könnte also mit den Mitteln des Wettbewerbsrechts bekämpft werden.

B. Datenschutzverstöße und § 1 UWG

Die "große Generalklausel" des § 1 UWG ist offener formuliert als § 3 UWG. Sie unterwirft jede Handlung im geschäftlichen Verkehr, die zu Zwecken des Wettbewerbs erfolgt ("Wettbewerbshandlung"), dem Maßstab der "guten Sitten". Ein Datenschutzverstoß löst also dann die Sanktionen des § 1 UWG aus, wenn er im Wettbewerb erfolgt und mit dem Rechtsverstoß zugleich auch ein Verstoß gegen die guten Sitten im Sinne des § 1 UWG gegeben ist. Bevor dies für einzelne denkbare Datenschutzverstöße geprüft wird, ist vorab der Tatbestand des § 1 UWG zu skizzieren.

1. Wettbewerbshandlung

Gegenstand des § 1 UWG ist eine Handlung, die im geschäftlichen Verkehr zu Zwecken des Wettbewerbs erfolgt. Als Handlung kommt dabei neben einem Tun auch ein pflichtwidriges Unterlassen in Betracht.[33] Handlung im geschäftlichen Verkehr ist jede nach außen gerichtete Tätigkeit, die irgendwie der Förderung eines beliebigen Geschäftzwecks dient.[34] Kontur erlangt der Begriff vor allem durch Ausgrenzungen. Danach liegt eine Handlung im geschäftlichen Verkehr bei privaten und rein hoheitlichen, aber auch bei nur betriebsinternen Handlungen nicht vor.[35] Insbesondere die Ausgrenzung von Betriebsinterna stellt für BDSG-Verstöße eine erhebliche Hürde

---

32 Franke, Arbeitsschutz und unlauterer Wettbewerb (1992), S. 29 f.

33 Schünemann, Großkommentar, Einl. UWG Rn. D 194.

34 BGH, Fleischbezug, GRUR 1953, 293 (294); BGH, Betonzusatzmittel, GRUR 1962, 45 (47); Baumbach/Hefermehl, Wettbewerbsrecht, Einl. UWG Rn. 208.

35 BGH, Reparaturversicherung, GRUR 1974, 666 (668); Baumbach/Hefermehl, Wettbewerbsrecht, Einl. UWG Rn. 208.

auf, da Datenverarbeitung häufig betriebsintern erfolgt und insoweit unmittelbar dem Anwendungsbereich des § 1 UWG zunächst entzogen erscheint. Ein betriebsinterner Vorgang kann allerdings mit einer nachfolgenden Handlung im geschäftlichen Verkehr in einem so engen Zusammenhang stehen, daß er in die Beurteilung der Lauterkeit dieser Handlung einzubeziehen ist.[36] Somit also können auch zunächst rein betriebsintern erfolgende Verstöße gegen das BDSG wettbewerbsrechtlich Bedeutung erlangen. Das Erfordernis, daß die Handlung zu Zwecken des Wettbewerbs erfolgt, wird von Rechtsprechung und Literatur unterschiedlich gehandhabt. Nach der Rechtsprechung und dem ihr folgenden Teil der Lehre ist in objektiver Hinsicht erforderlich, daß die Handlung geeignet ist, den Wettbewerb einer Person zum Nachteil desjenigen einer anderen zu fördern.[37] Hinzutreten muß eine entsprechende Absicht,[38] die allerdings bei Gewerbetreibenden regelmäßig vermutet wird.[39] Andere Teile der Literatur halten das Merkmal, daß die Förderung des Wettbewerbs einen Nachteil bei einem anderen Mitbewerber bewirken (bzw. bei abstrakter Betrachtung bewirken können muß) für entbehrlich.[40] Auch das Erfordernis der subjektiven Absicht wird häufig abgelehnt.[41] Beide Fragen können in dem hier interessierenden Zusammenhang, ob Datenschutzverstöße die Rechtsfolgen des § 1 UWG auslösen können, auf sich beruhen. Sie betreffen allgemeine Fragen des Wettbewerbsrechts und in Bezug auf das Datenschutzrecht ergeben sich keine Besonderheiten. Wesentlich hingegen ist, worin genau eine relevante Förderung des Wettbewerbs, zu der eine Handlung zu Zwecken des Wettbewerbs geeignet sein muß, besteht. Angesichts der großen Spannbreite möglicher Wettbewerbshand

---

36 Baumbach/Hefermehl, Wettbewerbsrecht, Einl. UWG Rn. 118 u. § 1 UWG, Rn. 609, 663.

37 BGH, Beitragsrechnung, GRUR 1992, 450 (452), Baumbach/Hefermehl, Wettbewerbsrecht, Einl. UWG Rn. 215.

38 BGH, Beitragsrechnung, GRUR 1992, 450 (452), Baumbach/Hefermehl, Wettbewerbsrecht, Einl. UWG Rn. 232.

39 BGH, Torsana, GRUR 1962, 34 (36), Baumbach/Hefermehl, Einl. UWG Rn. 235.

40 Schünemann, Großkommentar, Einl. UWG Rn. D 225 ff.

41 Schünemann, Großkommentar, Einl. UWG Rn. D 243.

lungen wird man sich damit begnügen müssen, daß eine irgendwie geartete Förderung des Wettbewerbs ausreichend ist.[42] Auf eine quantitative Steigerung von Absatz oder Bezug kommt es also nicht an.[43]

2. Verstoß gegen die guten Sitten

Es überrascht kaum, daß sich sehr verschiedene Ansätze entwickelt haben, den Begriff der "guten Sitten" im Sinne des § 1 UWG zu bestimmen. Ausgehend von diesen grundlegenden Konzepten haben sich wiederum Unterschiede in der Behandlung bestimmter Fallgruppen im Rahmen des § 1 UWG ergeben. Die Frage, ob ein Verstoß gegen die guten Sitten aufgrund eines Rechtsverstoßes gegen eine Norm außerhalb des UWG gegeben ist, wird unter dem Stichwort "Rechtsbruch" diskutiert. Im Rahmen dieser Arbeit ist es nicht möglich, auch nur die wichtigsten Konzepte zur Bestimmung der guten Sitten und die hieraus folgenden Regeln für die Fallgruppe Rechtsbruch darzustellen. Eine Beschränkung der Darstellung auf den Ansatz der Rechtsprechung und neueren Entwicklungen in der Literatur ist unerläßlich.

a) Ansatz der Rechtsprechung

Nach Ansicht der Rechtsprechung verstößt ein Verhalten dann gegen die guten Sitten im Sinne des § 1 UWG, wenn es dem Anstandsgefühl der beteiligten Verkehrskreise widerspricht oder von der Allgemeinheit mißbilligt und für untragbar angesehen wird.[44] Maßgeblich hierfür sind insbesondere die Regeln der Sittlichkeit, allerdings nicht als alleiniger Maßstab.[45] So spielt etwa die Unterscheidung zwischen Leistungs- und Nichtleistungswettbewerb eine wichtige Rolle.[46] In

---

42 Baumbach/Hefermehl, Wettbewerbsrecht, Einl. UWG Rn. 215; Schünemann, Großkommentar, Einl. UWG Rn. D 236.

43 BGH, stern, GRUR 1967, 256 (257).

44 BGH, Busengrapscher, BGHZ 130, 5 (7); Baumbach/Hefermehl, Wettbewerbsrecht, Einl. UWG Rn. 66.

45 BGH, Busengrapscher, BGHZ 130, 5 (7 f.).

46 BGH, Stuttgarter Wochenblatt I, BGHZ 51, 236 (242); Piper in Köhler/Piper, UWG, Einf. Rn. 176, 178.

der Fallgruppe Rechtsbruch geht die Rechtsprechung davon aus, daß nur ein Verstoß gegen eine sogenannte wertbezogene Norm bereits per se als sittenwidrig anzusehen ist.[47] Bei sonstigen wertneutralen Normen müssen hingegen weitere Umstände hinzutreten.[48] Als ein solcher Umstand wird vor allem ein ungerechtfertigter Vorteil, den ein Wettbewerber gegenüber seinen gesetzestreuen Mitbewerbern durch den Rechtsverstoß erhält, angesehen. Wertbezogen sind solche Normen, die entweder selbst einem sittlichen Gebot entsprechen oder aber ein wichtiges Gemeinschaftsgut schützen, so daß ihre Einhaltung einem sittlichen Gebot entspricht.[49] Der Kreis dieser wichtigen Gemeinschaftsgüter ist dabei zusehends angewachsen. Als wichtige Gemeinschafsgüter wurden von Rechtsprechung und Literatur zunächst vor allem die Volksgesundheit[50] und die Funktionsfähigkeit der Rechtspflege angesehen.[51] Im Laufe der Zeit wurden weitere "wichtige Gemeinschaftsgüter" entdeckt. So sah der BGH auch im Schutz der Rundfunkfreiheit den Schutz eines wichtigen Gemeinschaftsgutes.[52] Auch der Jugendschutz wurde als wichtiges Gemeinschaftsgut angesehen.[53] In der Literatur finden sich in den letzten Jahren häufig Bestrebungen, auch den Umweltschutz in den Kreis der wichtigen Gemeinschaftsgüter aufzunehmen,[54] ein Gedanke, der vom OLG Köln aufgegriffen worden ist.[55] Vereinzelt werden auch Regelungen des Urheberrechts als wertbezogen angesehen, da sie vor dem sittlich verwerflichen geistigen Diebstahl schützen sollen.[56] Schließlich erklärten in Zusammenhang mit den Telefon-CD-Auseinandersetzungen einige instanzgerichtliche Entscheidungen auch das vom BDSG geschützte Recht auf informationelle Selbstbestimmung zu einem wichtigen Gemeinschaftsgut.[57] Angesichts der

---

47 BGH, Werbung im Programm, BGHZ 110, 278 (289 f).
48 BGH, Flughafen-Zubringerdienst, GRUR 1973, 146 (147).
49 BGH, Werbung im Programm, BGHZ 110, 278 (290); Baumbach/Hefermehl, Wettbewerbsrecht, § 1 UWG, Rn. 614.
50 z.B. BGH, Apothekenpflichtige Arzneimittel, BGHZ 22, 167 (180); Baumbach/ Hefermehl, Wettbewerbsrecht, § 1 UWG, Rn. 615.
51 BGH, Preisbindungsüberwachungs-Treuhand, BGHZ 48, 12 (17), Baumbach/ Hefermehl, Wettbewerbsrecht, § 1 UWG, Rn. 623.
52 BGH, Werbung im Programm, BGHZ 110, 278 (289 f).
53 OLG Hamburg, NJW-RR 1997, 745 (746).
54 Brandner/ Michael, NJW 1992, 278 (279); Friedrich, WRP 1988, 641 (643).
55 OLG Köln, Plastik-Tragetaschen, BB 1993, 1387 (1387).
56 Seifert, ZUM 1985, 81 (84).
57 OLG Koblenz, DuD 1999, 357; LG Hamburg, CR 1997, 21; LG Mannheim,

grundlegenden Bedeutung, welche die informationelle Selbstbestimmung als Voraussetzung einer demokratischen Gesellschaftsordnung[58] hat, erscheint dies durchaus nach den Grundsätzen der Rechtsprechung folgerichtig. Den übrigen wertbezogenen Normen gleichgestellt ist die Gruppe der unmittelbar wettbewerbsregelnden Normen. Das sind Normen, die in ihrer Zielsetzung dem § 1 UWG vergleichbar sind.[59]

b) Neuere Entwicklungen in der Literatur

Sowohl der grundlegende Ansatz der Rechtsprechung als auch die Regeln zur Behandlung der Fallgruppe Rechtsbruch sehen sich scharfer Kritik aus der Literatur ausgesetzt. Das Abstellen der Rechtsprechung auf die Regeln der Sittlichkeit wird als nicht tragbar angesehen, da es ein einheitliches sittliches Fundament in der heutigen durch Pluralismus geprägten Gesellschaft nicht mehr gebe.[60] Die darauf beruhende Unterscheidung zwischen wertbezogenen und wertneutralen Normen sei mit nicht lösbaren Abgrenzungsschwierigkeiten verbunden.[61] Zudem könne sie nicht befriedigen, da sie nicht auf wettbewerblichen Gesichtspunkten beruhe.[62] Statt dessen wird vorgeschlagen, den Schutzzweck des UWG stärker zu berücksichtigen. Nur dann, wenn eine außerwettbewerbliche Norm einen dem UWG entsprechenden Schutzzweck aufweise, sei in dem Normverstoß zugleich ein Verstoß gegen die guten Sitten des § 1 UWG zu sehen.[63] Für die übrigen Normen wird - insoweit in weitgehender Übereinstimmung mit der Rechtsprechung - auf den Vorsprungsgedanken abgestellt.[64] Die guten Sitten verletzt ein Rechtsverstoß dem-

---

D-Info 2.0, NJW 1996, 1829/1831; LG Stuttgart, CR 1997, 83; LG Mannheim, CR 1996, 672; LG München I, CR 1998, 83.

58 vgl. Simitis in Simitis u.a., BDSG § 1 Rn. 167.

59 BGH, Werbung im Programm, BGHZ 110, 278 (291); Baumbach/Hefermehl, Wettbewerbsrecht, § 1 UWG, Rn. 665.

60 Braun, JuS 1994, 727 (731); Schünemann, Großkommentar, Einl. UWG Rn. D 19.

61 Schünemann, Großkommentar, Einl. UWG Rn. D 60.

62 Mees, GRUR 1996, 644 (644).

63 Schricker, Gesetzesverletzung und Sittenverstoß, S. 252; Schünemann, Großkommentar, Einl. UWG Rn. D 62.

64 Schricker, Gesetzesverletzung und Sittenverstoß, S. 260 f.; Schünemann, Großkommentar, Einl. UWG Rn. D 62.

nach dann, wenn er dem Rechtsverletzer einen ungerechtfertigten Vorteil gegenüber seinen Mitbewerbern einbringt. Dieser Ansatz der Literatur überzeugt. Er vermeidet die mit dem Abstellen auf sittliche Wertungen verbundenen Unsicherheiten. Der Schutzzweck des UWG wird angemessen berücksichtigt. Als Schutzzweck des UWG wird dabei der Schutz des lauteren Wettbewerbs angesehen.[65] Zum Teil wird auch der Schutz bestimmter außerwettbewerblicher Rechtsgüter, gemeint sind die oben genannten "wichtigen Gemeinschaftsgüter", als vom Schutzzweck des UWG umfaßt angesehen.[66] Hierfür findet sich aber im Gesetz kein Anhaltspunkt.[67] Es ist deshalb davon auszugehen, daß solche Rechtsgüter nicht vom UWG besonders geschützt werden. Der Schutzzweck des BDSG, das Persönlichkeitsrecht des Einzelnen vor Beeinträchtigungen durch den Umgang mit seinen Daten zu schützen (§ 1 I BDSG), deckt sich also nicht mit dem Schutzzweck des UWG.[68] Verstöße gegen Normen des BDSG vermögen also nur mittels des Vorsprungsgedankens wettbewerbsrechtliche Relevanz zu entfalten.

3. Wettbewerbsvorteile durch Datenschutzverstöße

Im folgenden werden die Instrumente des Datenschutzes daraufhin untersucht, ob und unter welchen Umständen ein Verstoß gegen sie einem Wettbewerber einen ungerechtfertigten Vorteil gegenüber seinen Mitbewerbern vermitteln kann. Aufgrund der Eigenheit des Datenschutzes, als Querschnittsmaterie eine sehr große Zahl unterschiedlicher Lebensbereiche zu erfassen, ist dabei auch der jeweilige Zweck der Datenverarbeitung zu berücksichtigen.

a) Unzulässige Datenerhebung

Kernstück des Datenschutzrechts sind die Zulässigkeitsregeln. Gemäß dem in § 4 I BDSG zum Ausdruck gekommenen Verbotsprinzip ist die Verarbeitung personenbezogener Daten nur dann zulässig, wenn der Betroffene eingewilligt hat oder ein gesetzlicher Erlaub-

65 Schünemann, Großkommentar, Einl. UWG Rn. D 45.
66 Baumbach/Hefermehl, Wettbewerbsrecht, § 1 UWG, Rn. 612.
67 Tilmann, WRP 1987, 293 (297).
68 ebenso v. Westerholt, Festschrift für Beier (1996), 561 (569).

nistatbestand die Verarbeitung erlaubt. Die Erhebung personenbezogener Daten selbst ist bisher noch nicht vom Verbotsprinzip umfaßt. Dies wird sich allerdings im Rahmen der Anpassung des BDSG an die EG-Datenschutzrichtlinie ändern müssen (Art. 7 i.V.m. Art. 2 lit. b)). Jedoch ist auch bisher für das BDSG anerkannt, daß eine Datenerhebung unzulässig ist und gegen § 28 I 2 BDSG verstößt, wenn sie mit der Absicht erfolgt, die gewonnen Daten anschließend auf eine unzulässige Weise weiterzuverarbeiten.[69] Hieraus ergibt sich, daß bei einer geplanten dateimäßigen Weiterverarbeitung bereits bei der Erhebung die Einwilligung des Betroffenen in die beabsichtigte Verarbeitung einzuholen ist, soweit die Verarbeitung nicht auf einen gesetzlichen Erlaubnistatbestand gestützt werden kann. Geschieht dies nicht oder nicht ordnungsgemäß, so ist nicht erst die Speicherung der Daten rechtswidrig, sondern bereits die Erhebung der Daten. Erheben ist das Beschaffen von Daten über den Betroffenen (§ 3 IV BDSG), es findet also nicht betriebsintern statt, sondern regelmäßig im geschäftlichen Verkehr. Anders kann es im Bereich der Arbeitnehmerdaten liegen, wenn Daten betriebsintern bei den eigenen Beschäftigten erhoben werden. Ob nun eine Erhebung auch zu Zwecken des Wettbewerbs erfolgt, ist nach dem Zweck der Erhebung zu unterscheiden. Erfolgt die Erhebung zu Zwecken des Direktmarketings, sollen die gewonnenen Daten also später dazu benutzt werden, geeignete Adressaten für bestimmte Werbemaßnahmen auszuwählen, ist von einem solchen Handeln zu Zwecken des Wettbewerbs auszugehen.[70] Die Erhebung der Daten dient in solchen Fällen bereits der Verbesserung des Absatzes der beworbenen Produkte und Dienstleistungen. In anderen Fällen erscheint dies zweifelhaft. Generell sind personenenbezogene Daten durchaus als Wirtschaftsgut anzusehen. Dies läßt es gerechtfertigt erscheinen, die Erhebung solcher Daten dort als Handeln zu Zwecken des Wettbewerbs anzusehen, wo sie als eigenständiges Wirtschaftsgut genutzt werden und nicht lediglich der Erfüllung anderer Zwecke dienen sollen. Dies wird in den Fällen des § 29 BDSG regelmäßig der Fall sein. Zu denken ist insbesondere an die Tätigkeit von Auskunfteien, die geradezu mit der Ware "personenbezogene Daten" handeln. Kein Handeln zu Zweckes des Wettbewerbs liegt vor, wenn die erhobenen Daten lediglich zur Abwicklung eines Vertrages mit dem Betroffenen etc. verwendet

69 Gola/Schomerus, BDSG, § 28 Anm. 4.1.

70 so auch v. Westerholt, Festschrift für Beier (1996), 561 (568).

werden sollen. In solchen Fällen kommt den Daten keine eigenständige Bedeutung als Wirtschaftsgut im Wettbewerb zu. Dies gilt insbesondere für den Bereich der Arbeitnehmerdaten, deren (rechtswidrige) Verarbeitung allerdings erhebliche Vorteile aus betriebswirtschaftlicher Sicht begründen kann. Diese betriebswirtschaftlichen Vorteile stellen aber eben nicht unmittelbar Vorteile im Wettbewerb dar. Eine Erhebung von Arbeitnehmerdaten erfolgt daher grundsätzlich nicht zu Zwecken des Wettbewerbs. Unterliegt die Datenerhebung dem Anwendungsbereich des § 1 UWG, so ist zu fragen, ob eine unzulässige Datenerhebung zu einem Wettbewerbsvorteil führt. Ein solcher Wettbewerbsvorteil kann darin gesehen werden, daß die erhebende Stelle Daten erhält, die sie auf rechtmäßige Weise so nicht erlangt hätte. Deutlich wird das etwa anhand einer Verbraucherbefragung (insbesondere die in letzter Zeit zu beobachtenden Lifestyle-Umfragen), bei der umfassende Daten über das Konsumverhalten erhoben werden. Wird die Ausfüllung des Bogens zudem mit der Teilnahme an einem Gewinnspiel versüßt, jedoch nicht deutlich gemacht, daß diese Daten personenbezogen weitervermarktet werden sollen, liegt es auf der Hand, daß hier mit mehr Rückläufen zu rechnen ist, als bei der Einhaltung der gesetzlichen Vorgaben anzunehmen wäre, da dann den Betroffenen die Tragweite ihres Handelns deutlich würde.[71] Ähnliches gilt für eine Datenerhebung, die entgegen den Geboten von Treu und Glauben bei Dritten und nicht bei dem Betroffenen selbst erfolgt.[72] Bittet ein Unternehmen seine bereits gewonnenen Kunden, ihm mögliche Interessenten aus dem Bekanntenkreis zu nennen und erhebt hier formularmäßig Daten über das Konsumverhalten dieser Bekannten, wird es qualitativ besser verwertbare Daten erhalten, als wenn es die Gewinnung der Daten potentieller Kunden datenschutzkonform gestaltet hätte. Bei einer solchen Gestaltung müßte etwa auf die Angabe bestimmter sensibler Merkmale der potentiellen Neu-Kunden verzichtet werden. Dann würden deren Belange nicht mehr durch die Datenerhebung bei Dritten erheblich beeinträchtigt. Das Unternehmen jedoch müßte auf diese aus seiner Sicht wertvollen Angaben verzichten. Eine andere datenschutzkonforme Gestaltung könnte in einem indirekten Verfahren liegen: Die bestehenden Kunden werden gebeten, ihre Bekannten über das Angebot des Unternehmens zu informieren, und diese dann

---

71 vgl. LG Stuttgart, RDV 1998, 262 (262).

72 vgl. Simitis in Simitis u.a., BDSG § 28 Rn. 67.

zu bitten, ihrerseits mit dem Unternehmen Kontakt aufzunehmen. In einem solchen Fall wird das Unternehmen mit einem deutlich geringeren Rücklauf der Werbeaktion zu rechnen haben.

b) Unzulässige Weiterverarbeitung

Die eigentliche Verarbeitung im Sinne des § 4 I BDSG wird regelmäßig betriebsintern stattfinden. Auch soweit ein Auftragsdatenverarbeiter eingeschaltet wird (§ 11 BDSG), ist ein Handeln im geschäftlichen Verkehr aufgrund der maßgeblichen wirtschaftlichen Betrachtungsweise[73] nicht gegeben. Ein Handeln im geschäftlichen Verkehr ist dagegen denkbar, wenn Daten übermittelt werden, denn hier verlassen sie wieder den betriebsinternen Bereich. Auch eine Nutzung vorhandener Datenbestände für einen Dritten (z.B. Vermietung eines Adreßbestandes an einen Dritten für eine Werbeaktion) läßt sich wirtschaftlich betrachtet als Handeln im geschäftlichen Verkehr ansehen. Entsprechendes gilt, wenn eigene Datenbestände auch für eigene Werbung genutzt werden. Allerdings erscheinen auch rein intern bleibende Verarbeitungsvorgänge nicht vollkommen irrelevant für den Wettbewerb. Nutzt ein Unternehmen etwa eigene und erworbene Datenbestände dazu, detaillierte Profile über die Betroffenen zu erzeugen, ist dies angesichts der verbesserten Nutzbarkeit solcher aufbereiteten Daten für die spätere Werbung nicht unbedeutsam. Da jedoch ein Einsatz dieser Daten im Wettbewerb eine weitere Verarbeitung erfordert und eine Weiterverarbeitung vorher rechtswidrig verarbeiterer Daten unzulässig ist, besteht kein Bedürfnis, diese betriebsintern bleibenden Vorgänge eigenständig in Bezug auf Folgen für den Wettbewerb zu betrachten. Gegebenenfalls ist an die Möglichkeit einer vorbeugenden Unterlassungsklage zu denken. Ein Handeln zu Zwecken des Wettbewerbs wird wie bei der Datenerhebung auch hier anzunehmen sein, wenn Daten tatsächlich als eigenständiges Wirtschaftsgut übermittelt oder genutzt werden. Zu denken ist wiederum an Maßnahmen des Direktmarketings. Aber auch der Verkauf einer Datensammlung, z.B. einer Telefon-CD, ist als Handeln zu Zwecken des Wettbewerbs anzusehen. Hierbei kann ein Vorteil im Wettbewerb bei einer datenschutzrechtlich unzulässigen Übermittlung oder Nutzung darin gesehen werden, daß die ü-

[73] vgl. BGH, Branchenverzeichnis, GRUR 1971, 119 (120).

bermittelnde Stelle Daten zur Verfügung hat bzw. stellen kann, wie es gesetzestreu handelnden Mitbewerbern nicht möglich ist. Dies ermöglicht zum Beispiel zielgenaueres Direktmarketing, das höhere Chancen der wohlwollenden Beachtung bei den Adressaten hat.[74] Bei einer angebotenen Datenbank mit personenbezogenen Daten kann sich die Unzulässigkeit der Übermittlung auch gerade aus den gebotenen Recherchefunktionen ergeben. Erlaubt eine Telefon-CD etwa die Suche auch nach unvollständigen Telefonnummern oder den Rückschluß von Telefonnummer auf Anschlußinhaber, kann hierin die datenschutzrechtliche Unzulässigkeit der Übermittlung der entsprechenden Daten liegen. Diese Suchfunktionen, die ein gesetzestreuer Wettbewerber nicht bieten kann, bedeuten ebenfalls einen Wettbewerbsvorteil.

c) Sonstige Instrumente des Datenschutzes

Die verbleibenden Instrumente des BDSG befassen sich vorwiegend mit Fragen der innerbetrieblichen Organisation der datenverarbeitenden Unternehmen. Ein unmittelbarer Bezug zwischen einem Verstoß gegen solche Vorschriften - etwa die Pflicht zu technisch-organisatorischen Maßnahmen nach § 9 BDSG oder die Bestellung eines betrieblichen Datenschutzbeauftragten (§§ 36, 37 BDSG) - zu einer Wettbewerbshandlung ist nicht ersichtlich. Allerdings kann ein Zurückbleiben hinter den gesetzlichen Vorgaben in diesen Fällen dem Unternehmen Kostenersparnisse einbringen, die je nach Art und Größe des Unternehmens durchaus erheblich sein können. In diesen - zunächst rein betriebsintern bleibenden - Ersparnissen ist aber noch kein relevanter Wettbewerbsvorteil zu sehen, der eine Anwendung des § 1 UWG auslösen könnte.[75] Nur wenn die Einsparungen nicht bloß die Gewinnspanne vergrößern, sondern tatsächlich im Wettbewerb eingesetzt werden, um etwa das eigene Angebot preislich günstiger zu gestalten, ist ein Vorteil im Wettbewerb gegeben. Dieser muß jedoch spürbar, also nicht bloß unerheblich sein.[76] Diesbezüglich werden sich je nach Branche, Größe des Unternehmens und Bedeutung der Datenverarbeitung für das Unternehmen Unterschiede

---

74 Schweiger/Wilde in Hilke [Hrsg.] "Direkt-Marketing", Wiesbaden 1993, S. 89 (92).

75 Baumbach/Hefermehl, Wettbewerbsrecht, § 1 UWG, Rn. 656.

76 Baumbach/Hefermehl, Wettbewerbsrecht, § 1 UWG, Rn. 656.

ergeben. So wird ein Auftragsdatenverarbeiter, für den eine ordnungsgemäße Durchführung des § 9 BDSG einen erheblichen Kostenaufwand bedeutet, gegebenenfalls eine größere Kostenersparnis aufgrund eines Zurückbleibens hinter den gesetzlichen Anforderungen im Wettbewerb erreichen können, als ein kleines Unternehmen, das ausschließlich für eigene Zwecke Daten verarbeitet. Es ist aber kaum anzunehmen, daß solche Fallgestaltungen in der Praxis Bedeutung erlangen werden. Um den Anspruch aus § 1 UWG gerichtlich durchzusetzen, müßte dem Beklagten nicht nur der Verstoß gegen das BDSG, sondern auch die daraus folgende Kostenersparnis und schließlich auch noch der Einsatz dieser Ersparnis im Wettbewerb nachgewiesen werden.

III. Ergebnis

Nur ein Ausschnitt der denkbaren Verstöße gegen datenschutzrechtliche Bestimmungen vermag - und auch dies nur in bestimmten Fällen - Sanktionen des Wettbewerbsrechts auszulösen. Dies betrifft insbesondere die Datenverarbeitung zu Zwecken des Direktmarketings oder in den Fällen des § 29 BDSG, in denen die verarbeiteten und zur Übermittlung bestimmten Daten tatsächlich als Ware erscheinen. Weite Bereiche des Datenschutzes bleiben hingegen ausgenommen, insbesondere soweit sie bestimmte innerbetriebliche Vorkehrungen verlangen. Dies mag aus der Sicht des Datenschutzes enttäuschen. Dennoch ist das Ergebnis hinzunehmen: Wettbewerbsrecht dient eben dem Schutz des Wettbewerbs, nicht dem Schutz der informationellen Selbstbestimmung. Wo es aber eingreift, ist das UWG eine willkommene Ergänzung der unzureichenden BDSG-Sanktionen.