Rechtsprechung dieser Institutionen: »Das menschenverachtende nationalsozialistische Regime wurde durch willfährige Richter und Staatsanwälte gestützt, die das Recht pervertierten. Die Grausamkeit, die das Bild der Justiz in der NS-Zeit prägt, gipfelte in seinem beispiellosen Mißbrauch der Todesstrafe.« (BGH 5 StR 747/94).

Winfried Hassemer
Über die absehbare Zukunft des Datenschutzes*

1. Vorbemerkung

Vor einem Vierteljahrhundert hat im Hessischen Landtag der institutionalisierte Datenschutz angefangen. Das hessische Datenschutzgesetz ist 1970 in Kraft getreten; es war das erste seiner Art in Deutschland und in der Welt, und es hat den Datenschutz theoretisch wie praktisch gefördert.

Die damalige Landesregierung war entschlossen, die Verwaltung zu modernisieren, insbesondere mit Hilfe der automatisierten Datenverarbeitung. Die Idee war, diese Modernisierung – mit der ja ein erheblicher Machtzuwachs verbunden war – nicht ins Werk zu setzen ohne eine ausgleichende Stärkung der Bürger, welche einer effektiver gewordenen Staatsverwaltung ausgesetzt waren. Automatisierte Datenverarbeitung sollte nicht ohne einen wirksamen Datenschutz realisiert werden; die Intensivierung der Herrschaftsmacht sollte durch eine Stärkung der Bürgerrechte normativ ins Lot gebracht werden. Deshalb war das Recht auf informationelle Selbstbestimmung keine Erfindung der 60er und 70er Jahre; es war vielmehr eine Neuformulierung des alten Grundrechts auf Freiheit und auf Privatheit, welche durch die informationelle Aufrüstung des Staates notwendig geworden war. Das Recht auf Datenschutz war in diesem Verständnis – gemäß einer alten und mächtigen Tradition – ein Abwehrrecht gegen einen allzu informationshungrigen Staat, der plötzlich imstande war, ungeahnte Mengen an Daten zur Kenntnis zu nehmen, sie zu sortieren und sie wohlgeordnet vorzuhalten.

An diesem Konzept des Datenschutzes hat sich bis heute nicht viel verändert. Die Datenschutzgesetze innerhalb und außerhalb Deutschlands realisieren mehr oder weniger die Idee eines informationellen Abwehrrechts der Bürger gegenüber einem mächtigen Staat. Diese Idee ist theoretisch weiterhin vernünftig und praktisch notwendig. Der Staat hat seine Rolle seither nicht gewechselt; wachsende Kontrollbedürfnisse der »Risikogesellschaft« werden – etwa vom Verfassungsschutz, der Polizei oder den Sozialbehörden – gerne befriedigt und gestärkt.

Der Staat hat aber als Informationssammler und Informationsverarbeiter mittlerweile Gesellschaft bekommen. Die Datenverarbeitung in privater Hand ist für die Privatheit der Bürger nicht weniger gefährlich als die in öffentlicher, und schon das fordert dringend Neuorientierungen im Konzept des Datenschutzes.

Zwei andere Entwicklungslinien sind bedeutsam. Die Technologien von Information und Kommunikation haben sich rasant entwickelt, und darauf muß sich der Datenschutz natürlich einstellen – nicht nur auf neue Bedrohungen informationeller Selbstbestimmung, sondern hie und da auch auf mögliche Verbündete aus dem Bereich der Technologie. Auch hat mittlerweile die Europäische Richtlinie zum Daten-

* Der Text entstammt einem Vortrag zum Thema »25 Jahre Datenschutz in Hessen« bei einer Veranstaltung des Landes Hessen 1995.

schutz nicht nur die internationale Diskussion wieder angefacht; sie bietet uns auch vielerlei Anregungen und Anlässe, unsere Praxis zu überdenken und zu erneuern. Es gibt also dringende faktische und normative Gründe, ein neues Konzept des Datenschutzes zu entwickeln. Aus diesem Konzept muß dann auch praktisches Handeln folgen.

Insgesamt sind fünf Empfehlungen zu geben, die auf die Modernisierung des Datenschutzes zielen. Es ist notwendig, sich auf neue Wirklichkeiten einzustellen (dazu 2), alte Zöpfe abzuschneiden (dazu 3), neue Technologien für den Datenschutz zu nutzen (dazu 4), den Datenschutz näher an die Bürgerinnen und Bürger heranzubringen (dazu 5) und bewährte Traditionen zeitgerecht zu formulieren (dazu 6).

2. Neue Wirklichkeiten

Die Prognose des Gesetzgebers der 70er Jahre hat sich als falsch erwiesen. Die Datenschutzgesetze waren eingestellt auf eine zentrale Datenverarbeitung in staatlicher Hand. Diese gefährliche Quelle wurde markiert und eingezäunt. Die zentralen gesetzlichen Vorschriften und auch die Existenz der Datenschutzbeauftragten sind Konsequenzen dieser Konzeption.

Die heutige Wirklichkeit und die von morgen sehen anders aus. Nicht (nur) zentrale staatliche Rechner interessieren sich für die persönlichen Daten der Leute; es sind viele kleine Bearbeitungsstationen, die immer potenter und billiger werden und sich deshalb schnell ausbreiten. Viele sind untereinander vernetzt, können Informationen austauschen und auf intelligente Weise zusammensetzen. Die meisten von ihnen befinden sich in privater Hand.

All dies wird von einem Trend verstärkt, das Wissen zu dezentralisieren und die Verarbeitung von Daten aus den Zentren wirtschaftlichen Handelns auszulagern. Auf diese Weise verschwimmt der Prozeß der Informationsverarbeitung weithin. Außerdem kommt hinzu, daß dieser Typ fremden Wissens über Menschen seine Gefährlichkeit für diese Menschen leicht kaschieren kann: War die Neugier des Volkszählers noch aufdringlich oder bedrohlich, so sammeln sich Informationen heute mit leichter Hand und gleichsam nebenbei. Die Leute werden zur Preisgabe ihrer Daten nicht mehr verpflichtet, sondern verlockt.

Beispiele dieser neuen Wirklichkeiten begleiten uns mittlerweile in großer Zahl, und morgen werden sie für fast alle von uns alltäglich sein. Ich hebe nur vier davon hervor:

Die SmartCards werden in rasantem Tempo leistungsfähiger, und folglich erobern sie sehr schnell einen Lebensbereich nach dem andern: Kredit, Gesundheit, Reisen, Einkaufen. Sie werden getragen von einem nachdrücklichen wirtschaftlichen Interesse der Anbieter, sie treffen auf eine lebhafte Zustimmung bei den meisten Verbrauchern, und: Sie machen das Leben einfacher, leichter und bunter. Biometrische Verfahren versprechen – jedenfalls auf die Dauer – dasselbe oder mehr. Sie sind absolut individuell und zuverlässige Kennzeichen einer Person, und sie können deshalb – auch in Verbindung mit anderen Technologien – Prozesse der Wiedererkennung so schnell und verläßlich gestalten, daß sie uns von vielen kostspieligen und zeitraubenden Alternativen befreien werden, wenn wir wollen. »Surfen im Internet« ist so verführerisch, wie es klingt, es sieht aus nach einem Palaver, einem spontan regulierten Markt von Informationen, und es verspricht ungeahnt weite informationelle Räume. Multimedia endlich erhebt sich langsam aus dem faszinierenden Dunkel einer revolutionär globalen Kommunikation, die am Ende wirklich sämtliche Informationen verarbeiten kann, welche ein Mensch im Leben braucht.

Die Probleme, welche diese neuen Technologien mit sich bringen, sind bei weitem

weniger gut sichtbar als die Vorzüge und Versprechungen. Und gerade darin besteht schon das erste Problem: Die Leute registrieren die Bedrohlichkeit nicht; die Gefährlichkeit dieser Informationsverarbeitung verschwindet als Phänomen hinter den Bereicherungen und Erleichterungen, welche die neuen Technologien versprechen. Und dabei ist doch klar, daß es allemal um Datenspuren, Datensammlungen und Datenabgleich geht, um Verfahren und Ergebnisse, an denen viele ein lebhaftes Interesse haben, nicht nur Anbieter, sondern unter bestimmten Voraussetzungen möglicherweise auch die Arbeitgeber, die Versicherungen oder die Polizei. Diese Technologien versprechen das Erstellen von Profilen und ungeahnte Einsichten in die Persönlichkeit von Menschen.

Es ist absehbar, daß eine autonome Entscheidung, sich solcher Technologien – aus welchen Gründen auch immer – nicht bedienen zu wollen, erheblichen Mut voraussetzen wird. Wenn beispielsweise fast alle anderen im Besitz einer Gesundheitskarte sind, so wird man sich, wenn man das für sich anders halten will, alsbald wie Robinson auf seiner Insel sehen, und man wird (etwa im Verhältnis zum Arzt oder Apotheker) manifeste Schwierigkeiten gewärtigen müssen. Diese neuen Technologien werden wie ein Strom sein, gegen den einzelne kaum anschwimmen können.

Endlich ist zu erwarten, daß sich unsere Rezeptions- und Interaktionsgewohnheiten ändern werden. Wer über den Bildschirm einkauft oder unter 500 Fernsehprogrammen zu wählen hat, wird – nicht nur wenn er ein Jugendlicher ist – andere Augen, Ohren oder Beine bekommen (wobei natürlich noch nicht ausgemacht ist, daß darauf kein Segen liegt).

Ausgemacht ist freilich, daß diesen Entwicklungen die bisherigen Vorstellungen von Privatheit und Datenschutz nicht gerecht werden. Die beschauliche Konfrontation von Bürgerfreiheit und Staatskontrolle wird durch ein Szenario ergänzt werden, welches ungleich komplexer und mobiler ist. Daraus ergeben sich drei Konsequenzen.

Erstens macht es keinen Sinn mehr, das Konzept des Datenschutzes auf den Staat als Informationsverarbeiter zu konzentrieren und die private Datenverarbeitung nur am Rande wahrzunehmen, sie für das kleinere informationelle Übel zu halten und sie folglich im Zweifel gewähren zu lassen. Gewiß ist klar, daß unsere Grundrechtstradition die private Datenverarbeitung anders gewichtet als die des Staates. Klar ist aber auch, daß das Grundrecht auf informationelle Selbstbestimmung von der privaten Datenverarbeitung jedenfalls nicht weniger intensiv bedroht ist als von staatlicher Kontrolltätigkeit. Deshalb sollte man jedenfalls die öffentliche und die private Datenschutzkontrolle zusammenführen, man sollte versuchen, den Schutzstandard zu vereinheitlichen. Tut man das, so darf man auf Synergie-Effekte hoffen und darf von einer einheitlichen Beurteilung und Strategie erwarten, daß ein Schutz persönlicher Daten auch im privaten Bereich merklich besser greifen wird. Die Differenz von Staat und Gesellschaft hat sich jedenfalls auf dem Feld der Datenverarbeitung eingeebnet; im Bereich des Datenschutzes darf der fortbestehende Glaube an eine solche Differenz nicht dazu führen, die Bürger gegenüber privater Datenverarbeitung vergleichsweise schutzlos zu stellen.

Zweitens muß sich unsere Vorstellung von »Datenschutz« konzeptionell erweitern und vertiefen. Die Zeiten, da es nur oder vor allem um den Schutz einzelner Daten ging, sind – auch in Hinsicht auf die Europäische Richtlinie – vorbei. Es geht vielmehr um das Freihalten von Räumen privater Autonomie und um die Erhaltung der Voraussetzungen, unter welchen die Menschen furchtlos und geschützt an öffentlicher Auseinandersetzung und Meinungsbildung teilnehmen können. Dazu ist notwendig, aber nicht hinreichend, daß ich weiß, was der Staat über mich weiß (wie das das Bundesverfassungsgericht einst formuliert hat). Es geht auch darum, in Struktu-

ren und Verfahren der Datenverarbeitung Einblick zu bekommen, um die Fähigkeit, die Bedeutung der Informationsverarbeitung zu beurteilen und sich möglichst souverän auf diesem Feld zu bewegen. Nur soweit solche Prozesse der Beteiligung gelingen, wird man davon sprechen können, daß aus »Datenschutz« ein Konzept von »Privatheit« geworden ist, welches nicht nur blind Verbote für bestimmte Typen von Datenverarbeitung aufrichtet, sondern die Menschen darüber hinaus instandsetzt, mit ihren persönlichen Daten selbstbestimmt umzugehen.

Drittens sollte man den Datenschutz noch näher an die Entwicklung der Datenverarbeitung heranführen. Es geht darum, für die betroffenen Menschen Beherrschbarkeit und Durchsichtigkeit der Informationsverarbeitung zu gewährleisten. Wer nicht versteht, was technisch passiert (wobei es natürlich auf Einzelheiten nicht ankommt), wird seine Rechte nicht autonom sichern können, weil er deren Bedrohtheit nicht sieht. Das bedeutet etwa für die Datenschutzbeauftragten konkret, daß sie ihre Beratungsaufgaben in bezug auf die menschlichen, die rechtlichen und die politischen Folgen der Datenverarbeitung ernst nehmen und daß eine funktionierende Technikfolgenabschätzung auch für die Bereiche von Information und Kommunikation organisiert wird.

3. Alte Zöpfe

Mehr und schneller als auf anderen Gebieten bilden sich im Bereich des Datenschutzes in Theorie und Praxis, in Rechtslage und Institution alte Zöpfe deshalb, weil hier die Angemessenheit des Schutzkonzepts besonders intensiv vom schnellen technischen Wandel abhängt. Die Sache wird dadurch noch kompliziert, daß es nicht immer einfach ist, Gewohnheiten als »alte Zöpfe« verläßlich zu diagnostizieren: Es könnte ja sein, daß gerade diese Gewohnheit einen versteckten Sinn hatte, der sich erst dann schmerzlich offenbart, wenn man die Gewohnheit aufgegeben hat. Endlich muß man in Rechnung stellen, daß Gewohnheiten sehr konkrete Phänomene sind. Das bedeutet u. a., daß sie von der jeweiligen Praxis des Berufs oder privaten Lebens abhängen, nicht allgemein verbreitet sind und folglich auch nicht allgemein beurteilt werden können. Unter diesen Kautelen sollte – jedenfalls in Hessen – auf einige Einrichtungen verzichtet werden.

In der richtigen und weiterhin vernünftigen Erkenntnis, daß ein Bürger jedenfalls dann informationell nicht verantwortlich handeln kann, wenn er nicht darüber informiert ist, wie der Staat die Daten automatisiert verarbeitet, hat der hessische Gesetzgeber zur Pflicht gemacht, ein zentrales Register zu führen und dieses auch regelmäßig zu veröffentlichen. Dieser vernünftige Sinn ist mit der Entwicklung der Informationstechnologie und ihrer Wahrnehmung durch die Bevölkerung nach und nach entfallen. Für dieses Register interessiert sich praktisch niemand mehr – wahrscheinlich vor allem deshalb, weil niemand seine Existenz kennt. Folglich macht es keinen praktischen Sinn, es in dieser Form weiterzuführen. Seinen vernünftigen Anspruch, Bürger über die Datenverarbeitung zu informieren, sollte man vielmehr dadurch einlösen, daß man Register dort führt, wo die Datenverarbeitung wirklich stattfindet: in der einzelnen Behörde (s. auch unter 5.).

Ganz ähnlich liegt es bei der Pflicht der Behörde, die Bürger unter bestimmten Voraussetzungen darüber zu informieren, daß Daten über sie automatisiert verarbeitet werden. In dieser Hinsicht fühlen sich in wachsender Zahl Leute für dumm verkauft, weil ihnen Mitteilungen gemacht werden, welche sie entweder nicht interessieren oder welche ihnen schon bekannt waren. Statt dessen sollte man die Benachrichtigungspflichten auf diejenigen Informationen konzentrieren, welche für die Bürgerinnen und Bürger wirklich informativ sind.

Es ist ferner wenig sinnvoll, dem Datenschutzbeauftragten eine Pflicht zur Beanstandung in allen Fällen aufzuerlegen, in welchen er Verstöße gegen das Recht des Datenschutzes feststellt. Die Datenschutzbeauftragten haben bekanntlich kaum einen formellen Einfluß; ihre Chancen der Veränderung liegen im Argument und in der öffentlichen Auseinandersetzung. Ihre Möglichkeit, einen Fehler zu beanstanden, ist funktional äquivalent der »Roten Karte« im Fußball: Man sollte sie äußerst sparsam benutzen und sie jedenfalls dann nicht einsetzen (müssen), wenn der Fehler marginal war oder alsbald behoben wird.
Auch die Pflicht, jedes Jahr einen Tätigkeitsbericht vorzulegen, läßt sich möglicherweise datenschutzfreundlich dahin verändern, daß dieser Bericht jährlich alterniert mit schriftlichen Stellungnahmen, Äußerungen oder Informationen zu wechselnden spezifischen Problemen des Datenschutzes.

4. Moderne Technologien

Das Verhältnis von Datenschutz und Datenverarbeitung ist herkömmlich kein freundliches: Neue Entwicklungen im Bereich der Datenverarbeitung bedeuteten regelmäßig eine weitere Aufrüstung des kontrollierenden Staates und damit eine erhöhte kritische Wachsamkeit auf dem Gebiet des Datenschutzes. Mir scheint, daß sich hier Veränderungen abzeichnen. Es gibt Entwicklungen moderner Kommunikationstechnologie, welche dem Datenschutz hilfreich sein können; er sollte sie deshalb nutzen.
So könnte man beispielsweise dem oben (unter 2.) dargestellten Problem, daß der Mensch im Einzelfall real keine Möglichkeit hat, die Technologie für sich abzulehnen, dadurch begegnen, daß man die Entscheidungsfreiheit mit Hilfe der Technologie auf vernünftige Einzelheiten konzentriert. Nach meiner Erwartung kann kein Datenschützer etwas daran ändern, daß die SmartCards sich durchsetzen werden und daß die Benutzer nur theoretisch die Wahlfreiheit behalten, ob sie eine solche Karte für sich akzeptieren oder nicht. Mit Hilfe der kryptographischen Verfahren könnte man aber sicherstellen, daß – beispielsweise auf einer Gesundheitskarte – die Betroffenen darüber entscheiden können, welche Informationen ihre Karte enthält oder wer die auf der Karte enthaltenen Informationen lesen darf. So könnten unterschiedliche »Lesetiefen« dazu führen, daß bestimmte Informationen an bestimmte Leser gelangen, an andere hingegen nicht.
So hängt im Bereich von Multimedia für die Privatheit der Betroffenen sehr viel davon ab, wie »benutzerfreundlich« und informativ die Oberfläche dieser Programme sein wird. Eine Entscheidung über die Weitergabe von Daten ist umso eher selbstbestimmt, je genauer der Betroffene darüber informiert ist, was er im Einzelfall tut. Folglich muß es darauf ankommen, die Autonomie der Menschen auch mit Hilfe technischer Möglichkeiten zu verstärken. Insoweit könnte die Technologie zu ihrer eigenen Beherrschbarkeit beitragen.
Auch in einer letzten Hinsicht kann die Informationstechnologie dem Datenschutz hilfreich sein – freilich auf eine verzwickte Weise. Traditionell steht den Datenschützern nur ein schwaches Instrument zur Verfügung, wenn sie auf Verletzungen des Grundrechts der informationellen Selbstbestimmung aufmerksam machen wollen: die Warnung vor einem Grundrechtseingriff. Mit dieser Warnung wird gemeinhin wenig erreicht. Neuerdings tritt – in Gestalt der »Akzeptanz« – ein neuer Helfer auf den Plan. Damit ist die Erwartung gemeint, daß die Bürger, sofern sie die Technik nicht verstehen oder sie ihnen unheimlich bleibt, diese Technik nicht akzeptieren werden. Bei der Autobahnmaut oder bei der Bahn-Card scheint es den Datenschützern gelungen zu sein, mit Hinweisen auf die mangelnde »Akzeptanz« bei den

Bürgern datenschutzfreundliche Lösungen durchzusetzen, welche eher durchschaubar und beherrschbar sind. Mir scheint, daß auf diesem Feld noch nicht alle Früchte geerntet sind.

5. Bürgernähe

Eine Chance, Lösungen für die realen Probleme der Zeit anzugehen, bietet das »Forum Datenschutz«, welches bislang viermal vom Präsidenten des Hessischen Landtags und vom Hessischen Datenschutzbeauftragten veranstaltet worden ist. Es hat eine große Resonanz in der Öffentlichkeit gehabt und am Beispiel konkreter Problemlagen (Stasi-Unterlagen, Innere Sicherheit und Organisierte Kriminalität, Situation der Ausländer) die Aspekte des Datenschutzes vor den Betroffenen ausbreiten können.

Von entscheidender Bedeutung für die Bürgernähe des Datenschutzes ist aber das Interesse der Bürger am Datenschutz selber. Wer seine Rechte auf Auskunft oder Information niemals wahrnimmt, hat sie im Grunde nicht. Auch unter diesem Aspekt ist es wichtig, die Konzeption des Datenschutzes als eines Abwehrrechts gegen staatliche Eingriffe zu erweitern und unter »Datenschutz« auch ein Recht auf Zugang zu Informationen zu verstehen.

Das Konzept »Freedom of Information«, welches in anderen Ländern bereits zum selbstverständlichen Bestand der Bürgerrechte gehört, ist bei uns aus mannigfachen Gründen nicht gut entwickelt. In meinen Augen muß man alles daransetzen, daß die Bürgerinnen und Bürger dieses Recht zur Kenntnis nehmen und beginnen auszuüben. So gesehen, ist das Umweltinformationsgesetz ein guter Anfang, indem es einen Zugang zu Informationen der Umweltverwaltung unter Beachtung von Persönlichkeitsrechten und Betriebsgeheimnissen erlaubt. Es steht dem Datenschutzbeauftragten konzeptionell gut an, sich auch in der Rolle des »Informationsbeauftragten« zu bewähren, welche als eine Beratungs- und Clearingstelle funktioniert, um den Bürgern ihre Informationsrechte im Einzelfall auch praktisch zugänglich zu machen.

Endlich gehört zu einem bürgernahen Datenschutz heute ein Konzept von »Datenschutz von unten«. Die dargestellte Entwicklung der Datenverarbeitung hat dazu geführt, daß es nicht mehr um die Kontrolle zentraler Rechner gehen kann. Dezentralisierung und Vernetzung der Datenverarbeitung müssen auch zu einer Veränderung des Konzepts der Datenverarbeitungskontrolle führen. Der zentral in den Ländern und im Bund eingerichtete Datenschutzbeauftragte hat keine Chance, diese Art von Datenverarbeitung wirklich zu überblicken.

In diesem Kontext hilfreich sind die behördlichen und die betrieblichen Datenschutzbeauftragten, welche Ahnung von der Technik und Einblick in konkrete Vorgänge der Informationsverarbeitung in ihrem Bereich haben. Deren Stellung muß man verbessern – sowohl hinsichtlich ihrer Ausbildung als auch hinsichtlich ihrer Kontrollmöglichkeiten; hier steckt noch vieles in den Anfängen. Auch wäre es sinnvoll, daß dezentrale Register (vgl. oben unter 3.) bei diesen Datenschutzbeauftragten geführt werden; bei ihnen darf jeder diese Register praktisch vermuten, und sie sind imstande, die nötigen Informationen beizutreiben.

Dies ändert nichts daran, daß mit dem Datenschutzbeauftragten des Landes eine zentrale Stelle der Koordination weiterhin sinnvoll bleibt; es geht nur darum, daß diese zentrale Stelle ihre Kontrollaufgaben mit besserem Einblick und größerem Nachdruck wahrnehmen kann.

Nach 25 Jahren kann man im Datenschutz bereits von »guten Traditionen« sprechen. Heute kommt es darauf an, diese Traditionen aus ihren eher zufälligen Einkleidungen herauszupräparieren und sie so zu formulieren, daß sie neu verstanden werden können.

Das Bundesverfassungsgericht hat in seinem grundlegenden Volkszählungsurteil 1983 die beiden klassischen Ziele des Datenschutzes gültig formuliert: Es kommt – in meiner Sprache – darauf an, die Rechte der Menschen in zweierlei Hinsicht informationell zu sichern: Als Individualperson sollen sie geschützt sein gegen fremdes geheimes Wissen, welches zum Instrument von Manipulation und Erniedrigung werden kann. Als Sozialperson sollen sie geschützt sein vor der Gefahr, daß die Möglichkeit fremden geheimen Wissens ihnen den Mut nimmt, auch in der Öffentlichkeit für ihre Meinung einzutreten. Die Verletzung von Privatheit, welche im Recht des Datenschutzes gemeint ist, besteht in einer vagen Angst vor informationeller Überwältigung durch Mächtigere und in einer sozialen Desorientierung, welche sich dem Nichtwissen darüber verdankt, daß andere einem gerade in denjenigen Bereichen informationell überlegen sind, welche zum Kernbereich der Person gehören. Informationelle Selbstbestimmung ist das Gegenteil von Vagheit, Vermutungen, Desorientierung, Undurchsichtigkeit. Sie ist autonome und souveräne Entscheidung eines Menschen darüber, was mit seinen personenbezogenen Informationen geschehen soll – freilich immer innerhalb der Grenzen berechtigter Gemeinschaftsinteressen.

Sieht man es so, dann wird ohne weiteres klar, daß ein modernes Datenschutzkonzept sich nicht auf ein Negativum beschränken darf, nämlich auf die Abwehr informationeller Eingriffe. In einer Informationsgesellschaft, wie wir sie bereits haben bzw. erwarten dürfen, muß der Schutz der informationellen Selbstbestimmung viel früher einsetzen, und er muß umfassender sein. In dieser Welt kann die Abwehr informationeller Eingriffe überhaupt nur dann gelingen, wenn die Betroffenen verläßlich orientiert sind über das, was »Informationsgesellschaft« heißt und was in ihr passiert.

Folglich ist ein Konzept des Datenschutzes heute vor allem anderen die Veranstaltung, den Bürgerinnen und Bürgern die Welt der Informationsverarbeitung und deren Konsequenzen für die Durchsetzung ihrer informationellen Rechte näherzubringen. Sodann ist sie die Beförderung von Typen der Informationsverarbeitung, welche den Menschen so leicht wie möglich kognitiv zugänglich sind und welche ihnen möglichst viele Alternativen der Entscheidung über die Verarbeitung ihrer Daten real zugänglich machen. Erst dann besteht sie in einem Freihalten von Räumen und Sphären, innerhalb deren die Menschen sich selbst gehören und den Mut zur autonomen Selbstdarstellung entwickeln können. Datenschutz ist heute sowohl der Schutz einer informationellen Partizipation am öffentlichen Leben als auch der Versuch, das private Leben von informationeller Überwältigung freizuhalten.