BÜNDNIS 90
DIE GRÜNEN
Bundestagsfraktion

lang & schlüssig

14[36]

JUNI 2001

Eine Information der Bundestagsfraktion Bündnis 90/ Die Grünen

Datenschutz und Grundrechtsschutz in der Informationsgesellschaft

Impressum

Herausgeberin	Bündnis 90/Die Grünen Bundestagsfraktion Platz der Republik 1 11011 Berlin http: // www.gruene-fraktion.de
Verantwortlich	Grietje Bettin MdB medienpolitische Sprecherin Bündnis 90/Die Grünen Bundestagsfraktion Platz der Republik 1 11011 Berlin Fon: 030 / 227 75051 Fax: 030 / 227 76051 eMail: grietje.bettin@bundestag.de http: // www.grietje-bettin.de
Redaktion	Thilo Weichert, Deutsche Vereinigung für Datenschutz e.V.
Bezug	Bündnis 90/Die Grünen Bundestagsfraktion Info-Dienst Platz der Republik 1 11011 Berlin Fax: 030 / 227 56566 eMail: public@gruene-fraktion.de
Schutzgebühr	DM 3,---
Redaktionsschluss	Juni 2001

Inhalt

Datenschutz und Grundrechtsschutz in der Informationsgesellschaft

Datenschutz und Grundrechtsschutz in der Informationsgesellschaft

Eine Information der Bundestagsfraktion von Bündnis 90/Die Grünen

Haben Sie sich schon einmal **gefragt**,

- was ein Versandhandelsunternehmen über Sie weiß, das Ihnen adressierte Werbung, genau passend zu Ihren Interessen, zusendet,
- woher eine Versicherung Kenntnis davon hat, dass Ihnen von einer ganz anderen Versicherung vor einiger Zeit der Versicherungsschutz gekündigt worden ist,
- wie es kommt, dass Ihre Bank über Ihre finanziellen Verhältnisse auch bei anderen Finanzdienstleistern Auskünfte hat,
- welche am Arbeitsplatz geführten Telefongespräche von Ihren Vorgesetzten mitgehört werden,
- ob es in Ordnung ist, dass es für ein paar Mark im Handel CD-ROM gibt, auf denen nicht nur Ihr Name, Ihre Adresse und Ihre Telefonnummer verzeichnet sind, sondern auch ein Bild Ihres Hauses,
- was mit den Videobildern passiert, die von Ihnen auf jedem größeren Bahnhof "im Vorbeigehen" angefertigt werden,
- wer welche Daten über Ihre bargeldlosen Einkäufe mit der Kreditkarte bzw. mit der EC-Karte speichert?

Die **Antworten** auf diese und ähnliche Fragen versucht Ihnen das Datenschutzrecht zu geben. In unserer Gesellschaft spielen persönliche Angaben eine immer wichtigere Rolle. Das Datenschutzrecht regelt den Umgang mit - wie es juristisch heißt – personen-bezogenen Daten, also mit den Daten auch von Ihnen als Bürger, als Konsument, als Arbeitnehmer, als Vereinsmitglied, als Mieter oder als Nutzer von elektronischen Medien. Die Begehrlichkeiten nach diesen Daten nehmen in unserer Gesellschaft, in der Informationen eine immer wichtigere Rolle spielen, immer mehr zu. Zugleich gibt es gute Gründe, das die Verwaltung oder Wirtschaftsunternehmen nicht alles über Sie weiß.

Die Politik ist gefordert, den Umgang mit diesen personenbezogenen Daten so zu regeln, dass einerseits die Informationsbedürfnisse in der Gesellschaft befriedigt werden und zugleich die Privatsphäre und die Bürgerrechte der Menschen gewahrt bleiben.

Die vorliegende Informationsbroschüre informiert Sie über aktuelle Probleme des Datenschutzes und, welche Vorschläge zur Lösung dieser Probleme Bündnis 90/Die Grünen haben.

Als 1983 und 1987 die Bevölkerung in Deutschland gegen die damals geplanten **Volkszählungen** protestierte, ging es darum, die eigene Privatsphäre vor staatlicher Ausforschung zu bewahren. Inzwischen scheinen nicht nur Behörden, sondern viele Unternehmen aus der Wirtschaft viel Sensibleres über die Menschen zu wissen, als damals gefragt wurde. Die Grünen hatten sich damals gemeinsam mit den Bürgerinnen und

DER DATENSCHÜTZER - DEIN FREUND UND HELFER !

Bürgern für den Schutz Ihres Persönlichkeitsrechts eingesetzt. Klagen gegen die Volkszählung führten dann dazu, dass das Bundesverfassungsgericht mit dem "**Recht auf informationelle Selbstbestimmung**" dem Datenschutz Grundrechtsrang verlieh. Bündnis 90/Die Grünen haben seitdem nicht locker gelassen bei ihrem Einsatz für den Datenschutz - auch wenn es in den letzten Jahren nicht mehr so spektakuläre Aktionen gab wie zu Volkszählungszeiten.

Die informationelle Einkreisung des Menschen

Die Gefahren für den Datenschutz haben sich gegenüber den 80er Jahren durch die informationstechnische Entwicklung vervielfacht. In der **modernen Informationsgesellschaft** ist der Schutz des Rechts auf informationelle Selbstbestimmung dringender denn je.

Das Rückgrat der Informationsgesellschaft ist das Internet. Wer das Internet nutzt für Informationsangebote, E-Commerce, Tele-Shopping, Online-Banking oder nur zum Versenden von Emails, der kann bei seinen Aktivitäten leicht von Providern, Vertragspartnern, aber auch von Hackern und der Polizei beobachtet werden (siehe dazu die Information der Bundestagsfraktion "Datenschutz im Internet"). Aber nicht nur dort droht die Aushöhlung unserer Privatsphäre. Technisch ist es heute kein Problem mehr, die gesamte Bevölkerung auf Schritt und Tritt zu verfolgen und zu beobachten:

- Bei der Nutzung von personifizierten Chipkarten (von der Kreditkarte bis zum Betriebsausweis) entstehen detaillierte Nutzungsprofile.
- Bei den Telekommunikationsgesellschaften kann minutiös nachvollzogen werden, wer sich wann mit wem ausgetauscht hat.
- Mit Hilfe des aktiv geschalteten Handys kann nachvollzogen werden, wo genau sich wer gerade aufhält.
- Versandhandelsunternehmen, Firmen mit Kunden- und Rabattkarten und Adressenhändler erstellen mit Hilfe von Adressangaben Sozialprofile und an Hand des Einkaufsverhaltens präzise Konsumprofile.
- Firmen führen ihre Kundendaten in gemeinsamen Datenwarenlagern (Data-Warehouse) zusammen und werten diese nach allen nur denkbaren Fragestellungen aus (Data-Mining).
- Auskunfteien sammeln von ihren Vertragspartnern in der Privatwirtschaft sowie aus öffentlichen Quellen alle nur denkbaren Angaben über die Finanzverhältnisse von Bürgerinnen und Bürgern und bieten Sie jedem zahlungsbereiten Menschen zum Kauf an.

Dabei ist die technische **Entwicklung erst am Anfang**. Die Automation in den Privatwohnungen, am Arbeitsplatz, bei den Konsum- und Freizeitaktivitäten und die elektronische Überwachung im öffentlichen Raum haben erst begonnen. Schon heute kann vom Weltraum aus über Satellitenüberwachung jedes Stückchen Erde zentimeter-genau kontrolliert werden. In einem vollautomatisierten Haushalt kann aus der Ferne per Handy der Inhalt des eigenen Kühlschranks festgestellt werden. Noch ungeahnte Möglichkeiten eröffnet die Biotechnologie und deren Verbindung mit der Informationstechnik.


EFFIZIENZOPTIMIERER ?

Die Ergebnisse von Genomanalysen geben Auskunft über unsere Erbanlagen, was nicht nur für Mediziner im Rahmen von Gesundheitschecks von Interesse ist, sondern auch für Arbeitgeber, Versicherungen oder gar für die Polizei.

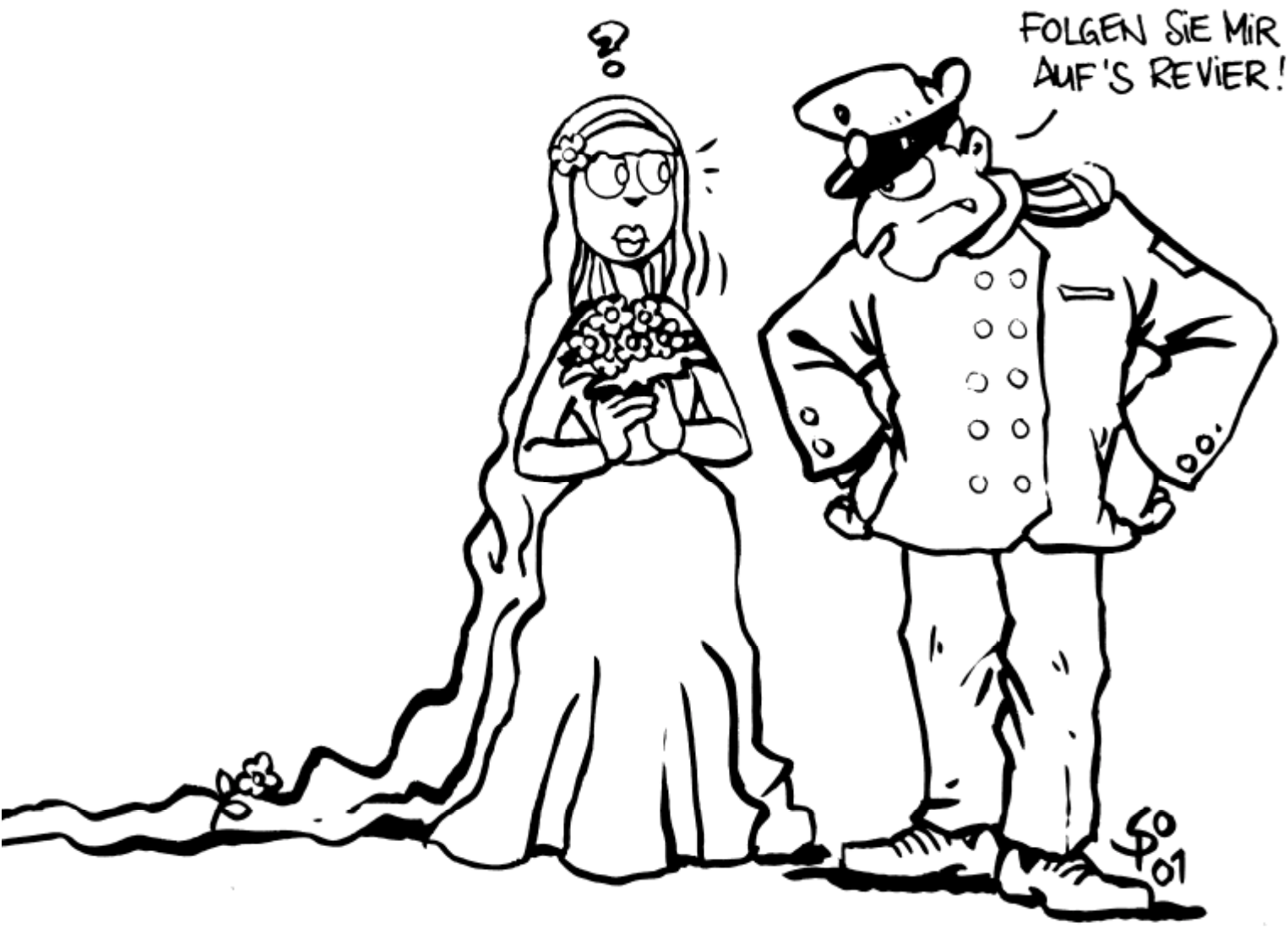
Für Bündnis 90/Die Grünen steht der Datenschutz heute wieder ganz oben auf der Tagesordnung. Aber nicht nur das Recht auf informationelle Selbstbestimmung ist durch die informationelle Einkreisung der Menschen in Gefahr. Es gibt heute praktisch keine **Grundrechte** mehr, die von der informationstechnischen Entwicklung nicht betroffen wären. Ein paar Beispiele:

- Das Recht auf Freizügigkeit wird beeinträchtigt, wenn per Mobilfunk jeweils der aktuelle Aufenthaltsort festgestellt werden kann oder wenn Videokameras im öffentlichen Raum jeden Schritt und Tritt verfolgen.
- Das Abhören von Wohnungen mit Hilfe von Wanzen oder Richtmikrofonen (großer Lauschangriff) ist eine Beeinträchtigung der Unverletzlichkeit der Wohnung.
- Das Grundrecht auf Asyl verliert seinen Wert, wenn die Angaben aus einem Asylantrag an den Staat weitergegeben werden, der den Flüchtling politisch verfolgt.
- Das Recht auf Demonstration oder auf politisches Engagement in einer Bürgerinitiative wird eingeschränkt, wenn der Staat solche demokratischen Aktivitäten erfasst, auswertet und z.B. bei der Einstellung in den öffentlichen Dienst verwertet.
- Mit dem Anzapfen von Telefonen oder dem Mitlesen von Emails wird in das Telekommunikationsgeheimnis eingegriffen.

Es kommt also nicht von ungefähr, wenn das Bundesverfassungsgericht 1983 festgestellt hat, dass das ungehinderte Sammeln von personenbezogenen Daten nicht nur einen Eingriff in das allgemeine Persönlichkeitsrecht der Betroffenen, sondern auch eine **Beeinträchtigung des Gemeinwohls** darstellt, "weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist".

Es ist zu kurz gegriffen, wenn - insbesondere von konservativer Seite - immer wieder behauptet wird, Datenschutz würde eine **effektive Verwaltung** behindern. Ein wirksamer Datenschutz ist Voraussetzung für eine technisierte und zugleich demokratische und freiheitliche Gesellschaft. Er ist Voraussetzung für die Weiterentwicklung der Informationsgesellschaft und die Akzeptanz der Menschen für elektronische Dienstleistungen und Warenangebote. Datenschutz ist aber auch noch aus einem weiteren Grund eine wichtige Voraussetzung für das Funktionieren von Behörden und Wirtschaft. Durch datenschutzrechtliche Regelungen werden die Verwaltungen dazu angehalten, ihren Datenbestand aktuell und verfügbar zu halten, überflüssige Informationen zu vernichten und die Bürgerinnen und Bürger zu beteiligen. Datenschutz hält die Verwaltung zur Ordnung im Umgang mit ihren Informationen an und sichert Verantwortlichkeiten. Datenschutz liegt daher auch im wohlverstandenen eigenen Interesse von Wirtschaft und Verwaltung.

Ebenso unsinnig ist die Behauptung, Datenschutz sei nichts anderes als **Täterschutz**. Sicherlich können die grundgesetzlichen Freiheiten zum Schaden anderer missbraucht werden. Das dies nicht geschieht, ist durch eine abwägende Gesetzgebung und durch effektiven Gesetzesvollzug sicherzustellen. Doch ohne Privatsphäre, ohne informationelle Selbstbestimmung würde dem Menschen die notwendige persönliche Sicherheit und damit eine zentrale Lebensgrundlage in einer technisierten Welt genommen.



DIE SOG. "SCHLEIERFAHNDUNG" OFFENBART IMMER WIEDER DEFIZITE IN DER POLIZEI - STRUKTUR.

Das Grundgesetz basiert auf einem positiven Menschenbild. Vor dem Wechsel 1998 waren 16 unionsgeführten Regierungsjahre geprägt von einer **Kontrollkultur von institutionalisiertem Misstrauen**. Überwachung wurde immer damit begründet, Menschen missbräuchten ihre Freiheiten und Rechte. Dieses Denken rechtfertigte die fast uferlose Überwachung von Demonstranten, Asylsuchenden, Versicherten und Sozialhilfeempfängern. Überwachung verhindert jedoch nicht zwangsläufig Missbrauch; oft wird das Gegenteil erreicht. Überzogene Kontrolle ermuntert zur Umgehung der Überwachung; Vertrauen motiviert zur Ehrlichkeit. Sicherlich bedarf es in einer hochtechnisierten Risikogesellschaft an vielen Stellen der Kontrolle. Doch diese muss verhältnismäßig sein. Und regelmäßig genügt eine anonyme Kontrolle; personenbezogene Überwachung ist nur selten unabweisbar.

Insbesondere: Datenschutz und Sicherheit

Moderne Technik eröffnet völlig **neue Perspektiven** bei der polizeilichen Gefahrenabwehr und bei der Strafverfolgung. Das Abhören und Auswerten von Telefongesprächen kann heute weitgehend automatisiert erfolgen. Der genaue Standort eines Mobilfunkgerätes lässt sich genau durch Ortung in der jeweiligen Funkzelle feststellen. Die sog. elektronische Fußfessel ermöglicht die präzise Feststellung des Aufenthaltsortes eines Straftäters. Mit Hilfe des sog. genetischen Fingerabdrucks können mit fast 100% Sicherheit Tatortspuren eindeutig einer Person zugeordnet werden. Mit Hilfe des Internet können weltweite Öffentlichkeitsfahndungen durchgeführt werden. Mit Hilfe von sog. Rasterfahndungen können Daten aus unterschiedlichsten Quellen zusammengeführt und mit dem Profil eines Verdächtigen abgeglichen werden. Mit Abhörgerät kann in die intimsten Bereiche der Wohnung eingedrungen werden. Per Videoüberwachung lassen sich gefährdete Orte rund um die Uhr lückenlos beobachten ... Die Aufzählung könnte fast beliebig fortgesetzt werden. All das soeben Dargestellte ist nach deutschem Datenschutzrecht zulässig. Das Gerede vom “Tatenschutz” hat offensichtlich keine tatsächliche Grundlage.

Die deutschen Sicherheitsbehörden haben sich in den letzten 20 Jahren eine Vielzahl von Befugnissen einräumen lassen, bei denen eine Abwägung mit dem Datenschutz **einseitig zugunsten der Sicherheitsinteressen** ausgefallen ist: So ist nach Ansicht von Bündnis 90/Die Grünen die Zulassung des Großen Lauschangriffs und der damit verbundene Eingriff in die private Wohnsphäre mit erwarteten Ermittlungserkenntnissen nicht zu rechtfertigen. Die verdachtslose Polizeikontrolle (sog. Schleierfahndung) führt nachweisbar zu einer Diskriminierung von fremdartig aussehenden Menschen. Sicherheitsbehörden haben ungehinderten Zugriff auf das zentrale Ausländerregister und können dort Suchvermerke und Gruppenfahndungen durchführen, gegenüber Deutschen haben sie diese Mittel nicht. Die halbjährige Speicherung der Telekommunikations-Verbindungsdaten ausschließlich, weil diese vielleicht von der Polizei benötigt werden könnten, ist eine völlig überzogene Vorratsdatenspeicherung. Der Verpflichtung von Psychologen, Sozialarbeitern und weitgehend auch Anstaltsärzten, den Leiter einer Justizvollzugsanstalt über sämtliche sicherheitsrelevanten Erkenntnisse zu unterrichten, zerstört das für eine Behandlung notwendige Vertrauensverhältnis zum Gefangenen. Die Pflicht von Sozialbehörden, Hilfeempfänger gegenüber der Polizei auf Ersuchen zu melden, untergräbt das Sozialgeheimnis und treibt die gesuchten Personen noch weiter in die Kriminalität. ... Leider lässt sich diese Aufzählung von Beispielen, wo im deutschen Recht im Namen der Sicherheit der Datenschutz übergangen und oft nur noch größere Unsicherheit geschaffen wird, lange fortführen.

Dessen ungeachtet sind die **deutschen Verhältnisse** noch "human", verglichen etwa mit denen in Großbritannien oder auch in den USA, wo selbst bei Bagatelldelikten von den Verdächtigen sog. genetische Fingerabdrücke gesammelt und zentral über Jahre hinweg gespeichert werden, wo die Namen und Adressen von Straftätern veröffentlicht werden und diese auch nach ihrer Entlassung aus dem Gefängnis einem dauernden sozialen Spießrutenlauf ausgesetzt werden, oder wo in ganzen Stadtteilen kein Fleck mehr existiert, wo man sich von einer Videokamera unbeobachtet küssen könnte.

Bei dem Ausgleich von Strafverfolgungs- und Datenschutzinteressen sind nach Vorstellung von Bündnis 90/Die Grünen folgende rechtsstaatlichen **Grundsätze** zu beachten:

- Sicherheitsbehörden dürfen grds. erst dann tätig werden, wenn eine konkrete Gefahr oder ein Straftatverdacht vorliegt.
- Aus dem Resozialisierungsgedanken ergibt sich die Pflicht, nach einer gewissen Zeit, Daten über Straftaten zu löschen, wenn sie für die künftige Aufgabenerfüllung nicht mehr benötigt werden.
- Die Unschuldsvermutung verbietet es, Menschen zu bestrafen oder als Straftäter zu behandeln, solange deren Schuld nicht nachgewiesen wurde.
- Eingriffe in den Kernbereich des Persönlichkeitsrechts dürfen nicht erfolgen.
- Grundsätzlich haben auch Sicherheitsbehörden ihre Daten offen bei den Betroffenen zu erheben.
- Die verdeckte Datenerhebung muss die Ausnahme bleiben.
- Besonderes intensive Eingriffe sind regelmäßig bzgl. ihrer Notwendigkeit und ihrer Wirkungen einer wissenschaftlichen Evaluation und einer parlamentarischen Kontrolle zu unterwerfen.

Big Brother - Du bist nicht allein

Nicht nur durch polizeiliche Datensammelwut oder durch extensive Erstellung von Kundenprofilen durch Wirtschaftsunternehmen ist die Privatsphäre gefährdet. Eine nicht zu unterschätzende Gefahr besteht in dem Voyeurismus und dem Exhibitionismus, den man zunehmend in unseren **Medien** antrifft. Selbstverständlich ist es jedes Menschen eigene Entscheidung, ob er sich Tag und Nacht von Kameras beobachten lässt, um über Fernsehen und Internet von Millionen begafft werden zu können. Es hat aber nichts mehr mit Menschenwürde zu tun, wenn das - völlig unpolitische - Sexualleben eines Politikers an die Öffentlichkeit gezerrt wird, auch wenn es sich um einen Staatspräsidenten oder um eine berühmte Person handelt. Es hat auch nichts mit Menschenwürde zu tun, wenn - wie im Fall Bäcker - die Gerichtsverhandlungen über das Zerbrechen einer Ehe, live im Fernsehen übertragen und dadurch zum öffentlichen Spektakel gemacht werden. Derartige amerikanische Verhältnisse tragen nicht zur demokratischen Meinungsbildung bei, sondern zur Missachtung der Privatsphäre Dritter. Bündnis 90/Die Grünen sehen es als eine zentrale Aufgabe der Presse und der elektronischen Medien an, das Werte wie Menschenwürde und Privatsphäre auch im Informationszeitalter respektiert werden und das für diese Werte geworben wird.

Bündnis 90/Die Grünen - engagiert für den Datenschutz

Für **Bündnis 90/Die Grünen** gehört zur Verteidigung der Menschen- und Bürgerrechte auch das Eintreten für den Datenschutz. Nur wenn überwiegende Gründe des Allgemeinwohls dies nötig machen, darf und soll das Recht auf informationelle Selbstbestimmung zurücktreten.

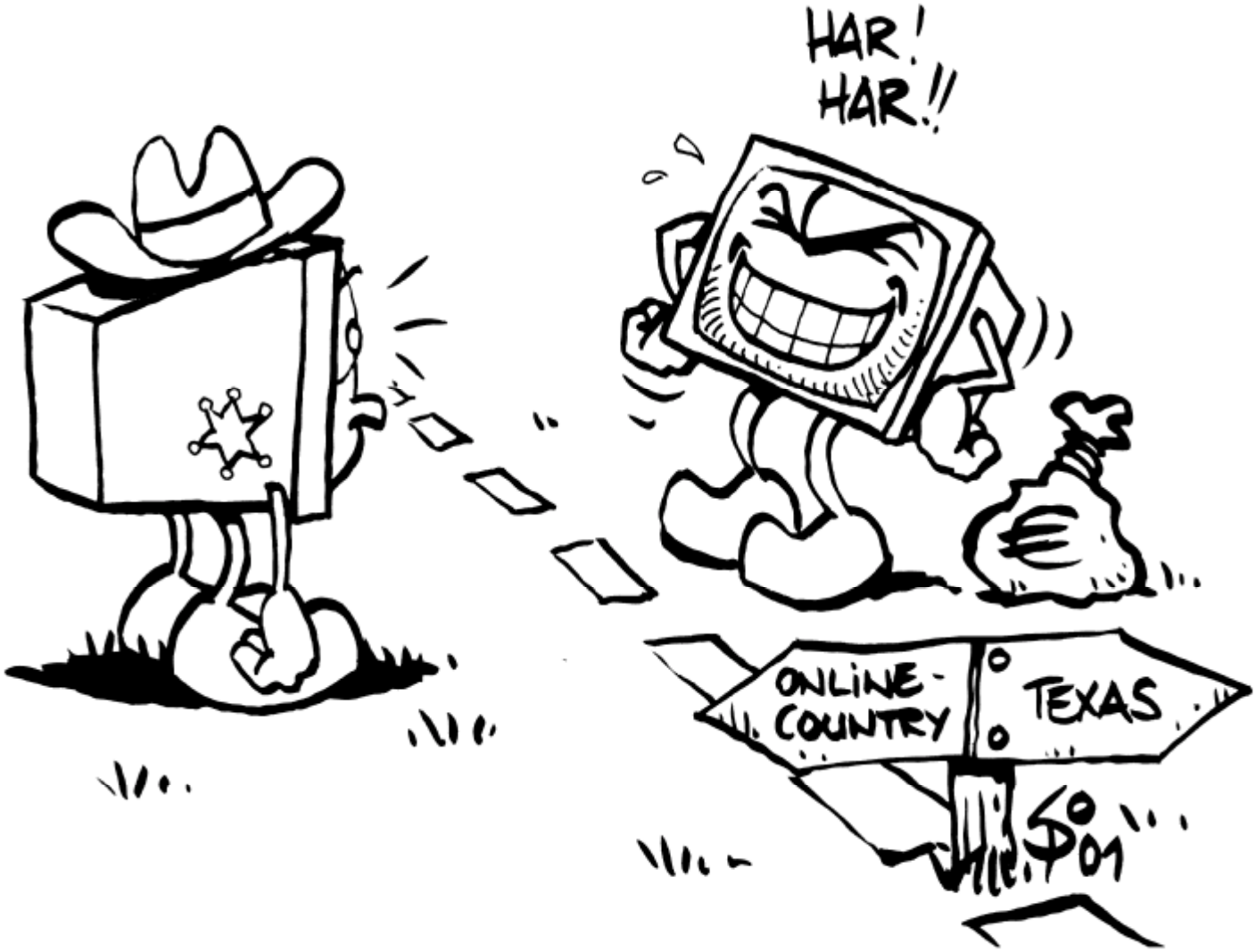
- So waren Bündnis 90/Die Grünen die vehementesten Verfechter der Aktenöffentlichkeit beim Ministerium für Staatssicherheit der ehemaligen DDR. Wer jahrelang dazu beitrug, ein ganzes Volk zu unterdrücken, kann sich nicht auf Datenschutz berufen, wenn diese Unterdrückung öffentlich gemacht wird.
- Genauso konsequent haben sich Bündnis 90/Die Grünen für den Rückbau der westdeutschen Geheimdienste engagiert, die mit ihrer verdeckten Datensammelei den offenen demokratischen Prozess beeinträchtigten.
- Bei der Frage, welche Befugnisse Sicherheitsbehörden, insbesondere die Polizei haben sollen, haben sich Bündnis 90/Die Grünen immer dafür eingesetzt, das die Bürgerrechte beachtet werden und Ermittlungen und staatliche Überwachung nicht zur Diskriminierung von Minderheiten und politisch Andersdenkenden missbraucht werden.
- Die gesetzliche Zulassung von Eingriffen in besonders geschützte private Räume wurden von Bündnis 90/Die Grünen - oft gegen das Votum sämtlicher anderen Parteien - immer abgelehnt, so als es um die Aushöhlung des Sozialgeheimnisses oder des Patientengeheimnisses ging oder um die Zulassung des großen Lauschangriffs.

Defizite aus der Vergangenheit

Die Idee des Datenschutzes hat sich in den letzten dreißig Jahren in Deutschland etabliert. Die Grundsätze des deutschen Datenschutzes wurden zum Exportschlager in vielen Ländern der Welt. Die seit 1995 geltende **Europäische Datenschutzrichtlinie** hat sich in großem Maße am deutschen Datenschutzrecht orientiert. Inzwischen hat diese Europäische Datenschutzrichtlinie in vielen Ländern Osteuropas und selbst in vielen Ländern, z.B. in Asien und in Amerika, Vorbildfunktion und spielt eine wichtige Rolle beim Modernisierungs- und Demokratisierungsprozess in diesen Ländern.

Doch zugleich hat sich der deutsche Datenschutz nicht viel weiterentwickelt. Er hat sich den Herausforderungen der modernen Informations- und Kommunikationstechnik nur ungenügend gestellt. Die Vorstellung, Datenschutz sei technikfeindlich, ist antiquiert. Sie hat sich aber bis zum Ende der schwarz-gelben Regierung Ende der 90er Jahre hartnäckig am Leben gehalten. Ebenso überholt ist die Vorstellung, allein mit Gesetzen und behördlicher Kontrolle ließen sich die Persönlichkeitsrechte verteidigen. In Deutschland gab es bis vor Kurzem einen Reformstau hinsichtlich des Gestaltung der Informationstechnik, der den Datenschutz zu diskreditieren drohte:

- Der bisherige Datenschutz funktioniert mit **Geboten und Verboten**, obwohl deren Beachtung wegen des Umfangs, der Komplexität und der Qualität der heutigen Datenverarbeitung oft nicht mehr erzwungen werden kann. Ergänzende Mechanismen, die z.B. die Beachtung des Datenschutzes wirtschaftlich belohnen, wurden nicht eingeführt.



DIE INTERNATIONALISIERUNG DER DATENVERARBEITUNG FÜHRT RECHTLICH ZU ALTBEKANNTEN PROBLEMEN.

- Die Gesetze wurden immer **komplizierter**, so dass sie heute oft weder von den Anwendern noch von den Bürgerinnen und Bürgern verstanden werden können. Die Konsequenz ist, das viele Regelungen einfach ignoriert und nicht mehr ernst genommen werden.
- Die meisten der heutigen Gesetze stammen noch aus den 70er und 80er Jahren, **der Zeit zentraler Großrechner**, in der sich das Internet noch in Kinderschuhen befand, in der es kaum vernetzte, geschweige denn mobile Kleincomputer gab. Diese Techniken gehören aber heute, ebenso wie z.B. der Einsatz der CD-ROM- und der Chipkartentechnologie, zum informationstechnischen Alltag. Auf diese neuen Techniken sind die alten Gesetze oft überhaupt nicht mehr oder nicht mehr vernünftig anwendbar.
- Die Datenschutzbehörden wurden mit **Verwaltungsbeamten** besetzt, die sich darauf beschränken, kontrollierend einzelnen Beschwerden nachzugehen. Präventive und vor allem technische Beratung für die Anwender wie für die Betroffenen der Informationstechnologie kann wegen unzureichender technischer und personellen Ausstattung und mangels rechtlicher Kompetenzen nur in unzureichendem Umfang geleistet werden.
- Die **Aufspaltung des Datenschutzes** zwischen einem öffentlichen und einem privaten Bereich ist angesichts der immer fließender werdenden Übergänge (Privatisierung öffentlicher Aufgaben, sog. Outsourcing) künstlich und hinderlich. Die gemeinsame Nutzung des Internet oder auch anderer Medien (z.B. Chipkarten) erlaubt keine Geltung zweierlei Rechts. Diese Trennung ist besonders eklatant bei der Datenschutzkontrolle, wo zudem durch Sonderregelungen für viele Bereiche (Kirchen, Medien, Telekommunikation) ein Zuständigkeitswirrwar besteht, den selbst Experten nicht mehr durchschauen.
- Die **Internationalisierung der Datenverarbeitung** macht den auf nationaler Gesetzgebung basierenden Datenschutz zum zahnlosen Tiger; durch eine Verlagerung ins Ausland können sich Firmen ihrer Verantwortung und einer staatlichen Kontrolle entziehen. Dies macht zum einen internationale Bemühungen erforderlich. Durch die Förderung des Selbstschutzes durch die Nutzerinnen und Nutzer kann dem Datenmissbrauch vorgebeugt werden.
- Datenschutz war bisher die Aufgabe von wenigen rechtlichen und technischen **Experten**. Angesichts der Allgegenwart der elektronischen Datenverarbeitung muss Datenschutzkompetenz allgemein in der Bevölkerung etabliert werden.

Engagement für eine neue Informationsordnung

Datenschutz ist ein wichtiger Faktor für die **Akzeptanz des Technikeinsatzes** durch die Menschen. Solange diese kein Vertrauen in die Beherrschbarkeit der Technik, in die Ungefährlichkeit und in die Sicherheit vor Missbrauch haben, werden sie elektronischen Handel und eine automatisierte Verwaltung nicht annehmen. Wirksamer Datenschutz ist Voraussetzung für die Verwirklichung der Visionen beim E-Commerce und für einen modernen technisch ausgerüsteten Staat. Wer die Informationstechnik fördern will, muss den Datenschutz fördern.

MANGELS TRANSPARENTER TECHNIKEN BLEIBT DEM USER MANCH LIEBEVOLLES DETAIL DER SOFTWARE VERBORGEN.

Es war die Fraktion von Bündnis 90/Die Grünen, die 1997 mit einem neuen Datenschutzkonzept und dem **ersten modernen Entwurf eines Bundesdatenschutzgesetzes** (BT-Drs. 13/9082) an die Öffentlichkeit trat. Es kann nicht mehr darum gehen, die überkommenen bürokratischen Strukturen fortzuschreiben. Es geht auch nicht mehr um die Begrenzung der Informationstechnik, sondern um deren demokratische Gestaltung. Diese Vorschläge der grünen Fraktion waren richtungsweisend für die weitere Entwicklung und Vorbild für fortschrittliche Regelungen in einzelnen Bundesländern.

Informationstechnik ist eine Herausforderung, keine Bedrohung; sie eröffnet auch völlig neue Chancen für den Datenschutz. Neue Techniken zur Anonymisierung und Pseudonymisierung, Prepaid-Verfahren, bei denen keine persönlichen Datenspuren zurückbleiben, Verschlüsselungstechniken, mit denen der Zugriff nicht berechtigter Personen auf elektronisch gespeicherte Daten ausgeschlossen werden kann, und digitale Signaturen, mit denen die Verlässlichkeit (Integrität und Authentizität) von elektronischen Dokumenten gesichert wird, sind neue Verfahren, die zu mehr Datenschutz führen. Für Bündnis 90/die Grünen ist es eine zentrale staatliche Aufgabe, die Entwicklung von **datenschutzfreundlichen Techniken** (privacy enhancing technologies) zu unterstützen und deren Einführung zu fördern.

Datenschutzfreundliche Techniken müssen **transparente Techniken** sein. Die Funktionsweise von Hard- und Software ist für die wenigsten Anwender noch nachvollzieh-, geschweige denn verstehbar. Gefährliche Nebenwirkungen sind oft nicht durchschaubar, z.B. ob in amerikanischen Produkten Hintertüren eingebaut sind, über die US-Geheimdienste bei an Netzen angeschlossenen Computern Daten mitlesen und manipulieren können.

Zu einer modernen demokratischen Informationsordnung gehört nicht nur der Schutz des Privaten, sondern auch die Veröffentlichung des Öffentlichen. Daher setzen sich Bündnis 90/Die Grünen von Anfang an für **Informationsfreiheitsgesetze** ein. In drei Bundesländern - in Brandenburg, Berlin und Schleswig-Holstein - gibt es inzwischen solche Gesetze. Nach einem Umweltinformationsgesetz, mit dem der Zugang zu Umweltinformationen für jede interessierte Person eröffnet wird, soll nun mit einem allgemeinen Informationsfreiheitsgesetz ein genereller Zugang zu behördlichen Informationen erteilt werden. Nur eine transparente Verwaltung kann wirksam demokratisch kontrolliert werden. Informationsfreiheit und Datenschutz sind zwei Seiten einer Medaille; beide sind Voraussetzung für individuelle und demokratische Selbstbestimmung. Daher ist es auch sinnvoll, die Datenschutzbeauftragten auch zu Beauftragten für die Informationsfreiheit zu machen. Nur wenn überwiegende öffentliche oder private Interessen entgegenstehen, sollen behördliche Informationen nicht öffentlich gemacht werden; dies kann der Fall sein, wenn es sich um Betriebs- und Geschäftsgeheimnisse oder um schutzwürdige personenbezogene Daten handelt.

Kein Export von Überwachungstechnologie in Diktaturen

Der Schutz vor Überwachung darf nicht nur das Privileg der Bürgerinnen und Bürger in modernen freiheitlichen Staaten sein. **Datenschutz ist ein Menschenrecht**. Zwar ist das, was unter Privatsphäre als schützenswert angesehen wird, von Kultur zu Kultur unterschiedlich. Dies ändert aber nichts daran, das in allen Kulturen staatliche oder

AM GESCHÄFT MIT KONTROLL- UND ÜBERWACHUNGSTECHNIKEN HABEN NICHT ALLE GLEICH VIEL FREUDE.

private Kontrolle und Überwachung zu Eingriffen in die unveräußerlichen Menschen- und Freiheitsrechte führen können. Bündnis 90/Die Grünen setzen sich für die Verteidigung der Privatsphäre und des Rechts auf informationelle Selbstbestimmung nicht nur in Deutschland und Europa, sondern in der ganzen Welt ein. Angesichts der globalen informationstechnischen Vernetzung ist ein solches Engagement letztendlich Voraussetzung für die Sicherung des Datenschutzes zu Hause.

Kontroll- und Überwachungstechnologien werden in großem Umfang aus demokratischen Industriestaaten in Diktaturen in Dritte-Welt- und in Schwellenländern exportiert. Mit Hilfe westlicher Videoüberwachung wurden noch Jahre nach den Protesten auf dem Platz des himmlischen Friedens in Peking im Jahr 1989 Dissidenten von der chinesischen Regierung verfolgt. Chipkarten-Sicherheitssysteme sorgen in vielen Staaten dafür, das bestehende Diskriminierungen gegenüber ethnischen Minderheiten, Ausländern oder Flüchtlingen zementiert werden. Kontroll- und Überwachungstechnologien wirken zwar nicht tödlich. Doch sind sie für autoritäre Regierungen in der Welt Voraussetzung zur Aufrechterhaltung ihrer Gewaltherrschaft. Bündnis 90/Die Grünen setzen sich dafür ein, dass der Export von Sicherheitstechnologie in Diktaturen transparent gemacht wird. In einem zweiten Schritt müssen Maßnahmen ergriffen werden, die den **Export von Kontroll- und Überwachungstechniken** zum Zweck der Aufrechterhaltung von Gewalt und Unfreiheit verhindern.

Novellierung des Datenschutzrechts

Die rot-grüne Regierung hat 1998 von der Vorgänger-Regierung ein schweres Erbe übernommen: Bis dahin hätte das deutsche Datenschutzrecht an die Europäische Datenschutzrichtlinie von 1995 angepasst sein müssen. Nichts Vorzeigbares war passiert. Selbst die Vorbereitungen für diese Anpassung waren unausgereift und umstritten. Um wegen der Verletzung von EU-Recht nicht mit Sanktionen oder Schadensersatzforderungen überzogen zu werden, haben sich die Regierungsfraktionen von SPD und Bündnis 90/Die Grünen darauf verständigt, das **Datenschutzrecht in zwei Stufen zu erneuern**. In einer ersten Stufe, die voraussichtlich Mitte 2001 abgeschlossen ist, wird das Bundesdatenschutzgesetz (BDSG) an das europäische Recht angepasst und bzgl. einiger unstreitiger Punkte modernisiert. In einer zweiten Stufe soll dann eine Totalrevision des Datenschutzrechtes erfolgen. Im Rahmen dieser Revision wird das BDSG vollständig überarbeitet werden.

Moderner Datenschutz muss nach den Vorstellungen von Bündnis 90/die Grünen folgende Merkmale aufweisen:

- Er muss wirksam und den Risiken angemessenen Persönlichkeitsschutz gewähren.
- Er muss transparent und verstehbar sein.
- Er muss sich für die Beteiligten lohnen.

Für Bündnis 90/Die Grünen ist das vorrangige Ziel der zweiten Stufe der BDSG-Novelle, das inzwischen unleserlich gewordene, kaum noch anwendbare und technisch überholte Gesetz zu einem **Gesetz für die Bürgerinnen und Bürger** zu machen, das diesen in verständlicher Sprache klare Rechte und effektiv durchsetzbare Ansprüche sichert. Die absehbaren technischen Entwicklungen sind zu berücksichtigen, so dass nicht bei jeder Innovation eine Gesetzesänderung nötig wird, um den Persönlichkeitsschutz zu gewährleisten.

In der zweiten Stufe ist es außerdem erforderlich, sämtliche bisher bestehenden **Datenschutzregelungen auf den Prüfstand** zu stellen. Die Kohlregierung hat während ihrer ganzen 16 Jahre - abgesehen von einer vom Bundesverfassungsgericht erzwungenen kleinen Kurskorrektur im Jahr 1990 - nichts anderes gemacht, als für die Verwaltung neue Datenverarbeitungsbefugnisse zu schaffen. An vorderster Front standen die Sicherheitsbehörden, denen vom Gesetzgeber ein gewaltiges Arsenal von Rechten zugestanden wurde, das teilweise seit Jahren ungenutzt in dicken Gesetzessammlungen verstaubt. Aber auch in anderen Bereichen wurde eine unübersichtliche Masse von Regelungen geschaffen, die vorne und hinten nicht mehr zueinander passt. So sind in der Sozialgesetzgebung derart oft Änderungen vorgenommen geworden, dass selbst ausgewiesene Experten keinen Überblick mehr haben, was erlaubt und was verboten sein soll. Zugleich blieben über Jahre hinweg grundlegende Fragen, insbesondere im Bereich der Wirtschaft, ungeregelt. Die Menschen blieben der Datenmacht kommerziell interessierter Unternehmen, z.B. Adressenhändler oder Auskunfteien, weitgehend schutzlos ausgeliefert. Ziel muss es sein, dass spätestens nach 10 Jahren das gesamte **allgemeine und bereichsspezifische Datenschutzrecht** nach abgestimmten Standards überarbeitet worden ist.

Insbesondere: Arbeitnehmerdatenschutz

Der Schutz der Persönlichkeitsrechte ist für die Menschen nicht nur als Konsumenten und als Staatsbürger von Bedeutung. Die längste aktive Zeit ihres Lebens verbringen die meisten Menschen am Arbeitsplatz. Hier ist das Risiko, unangemessen kontrolliert und reglementiert zu werden besonders groß. Daher setzen sich Bündnis 90/Die Grünen für eine **Verabschiedung eines Arbeitsnehmerdatenschutzgesetzes** noch in dieser Legislaturperiode ein. Generell gilt, dass die Menschen auch am Arbeitsplatz einen Anspruch auf Schutz ihrer Privatsphäre und ihrer Persönlichkeitsrechte haben. Kontrollen durch den Arbeitgeber dürfen nur insoweit erfolgen, als dies im Rahmen des Arbeitsverhältnisses unabdingbar ist.

Beispiele:

- Bei der Bewerbung und Einstellung dürfen nur Fragen gestellt werden, die für den Arbeitsplatz relevant sind. Diskriminierende Fragen, z.B. auch nach einer bestehenden Schwangerschaft, sind unzulässig. Alle unzulässigen Fragen müssen nicht und können ohne Folgen falsch beantwortet werden.
- Die Vorlage genetischer Untersuchungsergebnisse kann weder bei der Einstellung noch im Rahmen des Arbeitsverhältnisses gefordert werden.
- Eine verdeckte Arbeitnehmerüberwachung ist grundsätzlich zu verbieten.
- Private Kommunikation am Arbeitsplatz ist für den Arbeitgeber tabu, auch wenn sie leicht überwachbar über die firmeneigene Telefonanlage oder über den firmeneigenen Rechner erfolgt.

Bündnis 90/Die Grünen setzen sich dafür ein, dass in den Betrieben spezifische Betriebsvereinbarungen zur Verhinderung von unangemessenen Verhaltens- und Leistungskontrollen abgeschlossen werden. Neben den allgemeinen Datenschutzinstanzen (betrieblicher Datenschutzbeauftragter, Datenschutzbehörden) kommt zur Wahrung des Arbeitnehmerdatenschutzes dem **Personal- bzw. dem Betriebsrat** eine wichtige Funktion zu. Sämtliche technischen Einrichtungen und Maßnahmen, die sich zu einer Arbeitnehmer-

kontrolle eignen, sind mitbestimmungspflichtig. Diese Mitbestimmungspflicht ist angesichts des Einsatzes neuer Techniken auch im Bereich der Datenschutzorganisation (Datenschutzbeauftragter, Datenschutzmanagement, Privacy Policy) auszuweiten. Die Befugnisse der Personalvertretung, sich angesichts der zumeist technisch und juristisch komplizierten Sachverhalte bei unabhängigen Sachverständigen beraten zu können, müssen gestärkt werden.

(Neue) Instrumente des Datenschutzes

- Forderungen für den Datenschutz des 21. Jahrhunderts -

Die Informationstechnik hat zwar unseren Alltag erobert, hat aber noch keinen Eingang in unser Grundgesetz gefunden. In modernen Verfassungen - z.B. auch in einem Entwurf für eine EU-Grundrechtscharta - ist es eine Selbstverständlichkeit, eine Informationsordnung festzuschreiben, wozu die **grundrechtliche Absicherung** des Rechts auf informationelle Selbstbestimmung gehört.

Das Hauptproblem des Datenschutzes in der Wirtschaft liegt derzeit darin, dass die Verarbeitung der Daten an den Betroffenen vorbei erfolgt. Ihnen wird allenfalls ein Widerspruchsrecht (opt out) zugestanden. Angesichts der vielfältigen Nutzungsformen und Übermittlungen ist dies nicht mehr zeitgemäß. Dem Vorbild des Multimediarechts folgend, sollte die Nutzung von Konsumentendaten für Werbe- und Marktforschungszwecke nur noch zugelassen werden, wenn hierzu eine **ausdrückliche Zustimmung** (opt in) erteilt worden ist. Eine nachträgliche Opt-Out-Möglichkeit muss natürlich beibehalten werden. Der Werbebranche muss klar gemacht werden, dass es kein Beweis von Kundenfreundlichkeit und Serviceorientierung ist, die Menschen ungefragt mit Werbung zu behelligen. Zustimmungserklärungen können in einer elektronischen Welt nicht mehr ausschließlich schriftlich erfolgen. Vielmehr müssen adäquate technische Lösungen (elektronische Einwilligung, Zustimmungsmanagement) gefunden werden, den Willen der betroffenen Menschen zu erkennen und umzusetzen.

Wo Datenverarbeitung im Allgemeininteresse steht, kann und braucht keine Zustimmung verlangt werden. Dies ist im Wirtschaftsbereich z.B. der Fall bei der **Überprüfung der Bonität** und der Seriosität von (künftigen) Vertragspartnern. Um so wichtiger ist aber dann, dass die Daten einer klaren Zweckbindung unterworfen werden. Es ist z.B. ein Skandal, dass Informationen über schlechte finanzielle Verhältnisse dazu genutzt werden, überschuldeten Personen Wucherkredite ("ohne Schufa-Auskunft") anzudienen. Datenschutz soll der notwendigen Transparenz in einem freien Wirtschaftssystem nicht entgegenstehen; diese darf aber nicht zur Diskriminierung und Benachteiligung der ohnehin schon wirtschaftlich Schwächeren führen.

Angesichts des Umstands, dass die Menschen in der Informationsgesellschaft an vielen Stellen zwangsläufig "Datenschatten" hinterlassen, ist zu fragen, ob diese Datenschatten in jedem Fall personenbezogen sein müssen. Die Antwort ist eindeutig: "Nein". So, wie es bisher möglich ist, beim Bäcker Brötchen zu kaufen, ohne Name, Adresse und Kontoverbindung zu hinterlassen, muss dies auch in der digitalen Welt beim E-Commerce sein. Diese Überlegung soll mit dem **Prinzip der Datensparsamkeit** umgesetzt werden. Das Prinzip besagt, dass dort, wo auf die Erhebung von personenbezogenen Daten verzichtet werden kann, dies auch erfolgen muss. Die Verfahren sind so zu gestalten, dass möglichst wenig personenbezogene Daten erhoben und dass diese frühestmöglich wieder gelöscht bzw. anonymisiert werden. Der Grundsatz der Datenminimierung verlangt

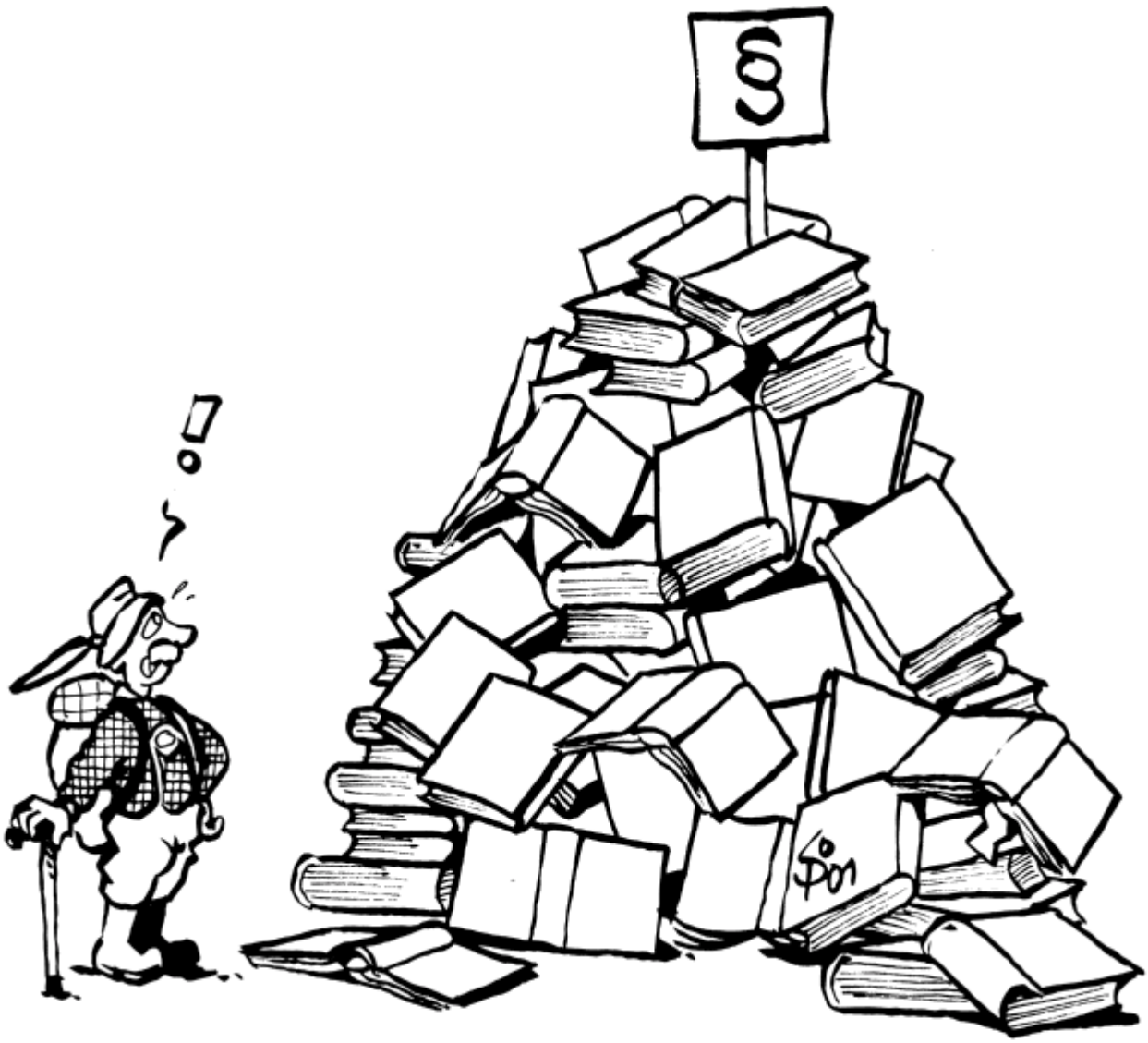
PSEUDONYMITÄT LÄSST SICH AUCH IM ALLTAG MIT EINFACHEN MITTELN AUFRECHT ERHALTEN.

eine entsprechende Gestaltung der technischer Verfahren, z.B. im Bereich des E-Commerce der Zulassung von nicht personalisierten Prepaid-Chipkarten (elektronische Geldbörsen).

Rechtlich hat diese Überlegung zur Konsequenz, dass aus dem Recht auf informationelle Selbstbestimmung ein **Recht auf Anonymität und Pseudonymität** abgeleitet werden muss. Für einen Geschäftspartner ist es regelmäßig nur wichtig, dass er für seine Ware bezahlt wird; es spielt für ihn keine Rolle, dass Peter Panther unter dem richtigen Namen oder als "Theobald Tiger" bezahlt; es kommt nur darauf an, dass unter dem Namen Theobald Tiger ein gedecktes Konto geführt wird. In der digitalen Welt wird es üblich sein, dass eine Person, je nachdem in welcher Rolle sie aktiv ist, unter verschiedenen Namen auftritt. Die Teilnahme an einem Internet-Chat kann mit einer anderen "Identität" erfolgen als die Führung eines Guthabenkontos; die Mitgliedschaft in einem Rabattverein und in einer medizinischen Selbsthilfegruppe erfolgt wieder mit anderen Pseudonymen. Damit dies auch tatsächlich möglich wird, bedarf es einer rechtlichen Absicherung des rechtsgeschäftlichen Verkehrs unter Pseudonym, wobei nach einem geregelten Verfahren nur im Konfliktfall eine Zuordnung zum wirklichen Namen gefordert werden darf. Wer statt einer personenbezogenen eine anonyme oder pseudonyme Kommunikations- oder Handlungsform wählt, darf deshalb nicht benachteiligt werden. Zur technischen Umsetzung dieser Zukunftsvision sind digitale Identitätsmanager zu entwickeln.

Schon in den 70er Jahren hat das Bundesverfassungsgericht festgestellt, dass die Erstellung vollständiger oder teilweiser **Persönlichkeitsprofile** gegen die Menschenwürde verstößt. In Computersprache ausgedrückt: der Mensch ist mehr als eine Ansammlung von Nullen und Einsen. Aus diesem Grund verlangt auch die europäische Datenschutzrichtlinie, dass die Menschen keinen auf Persönlichkeitsprofilen basierenden automatischen Entscheidungen unterworfen werden dürfen. Der Umstand, dass heute die Menschen von Auskunfteien in einem geheim gehaltenen Verfahren automatisch auf Grund ihrer Kredit- und Finanzdaten mit einem sog. Scoring-Wert bedacht werden, der dann darüber entscheidet, ob man als kreditwürdig gilt oder nicht, ist mit dieser Regel nicht vereinbar. Mit Hilfe von sog. intelligenten Systemen (z.B. Data-Mining) werden heute von vielen Stellen digitale Persönlichkeitsprofile erstellt, die oft mehr über einen Menschen aussagen, als dieser über sich selbst weiß, die aber zugleich vom Wesentlichen des Menschseins keine Ahnung haben können. Dort, wo solche Profile erstellt werden, müssen die Betroffenen umfassend informiert sein; die Daten sind einer strengen Zweckbindung zu unterwerfen.

Auch wenn es kein unsensibles Datum gibt - selbst die Adresse, z.B. eines polizeilichen Zeugen, kann ein lebenswichtig geheimzuhaltendes Daten sein - und auch wenn die Schutzbedürftigkeit vom konkreten Verwendungszusammenhang abhängt: Es gibt Daten, die schon wegen ihres Inhaltes **besonders schutzbedürftig** sind. Hierzu gehören z.B. Angaben über die genetische Veranlagung, über die Sexualität oder über die Gesundheit. Informationen, die im Rahmen eines besonderen Vertrauensverhältnisses, z.B. gegenüber einem Arzt oder einem Anwalt, offenbart wurden, müssen einem strengeren Regime unterliegen als Daten, die ein Mensch selbst veröffentlicht hat. Neben einem zusätzlichen rechtlichen Schutz ist bei solchen Daten auch ein weitgehender technischer Schutz notwendig. So ist es z.B. nicht akzeptabel, dass Ärzte Patientengeheimnisse unverschlüsselt per Internet austauschen, so dass alle Beteiligten im Netz mitlesen können. Für besonders sensible Bereiche, wie z.B. für die Verarbeitung von Gesundheitsdaten, fordern Bündnis 90/Die Grünen spezielle Datenschutzregelungen.



EIN JEDER HAT SEINE RECHTE IM DATENSCHUTZ
– ER MUSS SIE NUR KENNEN.

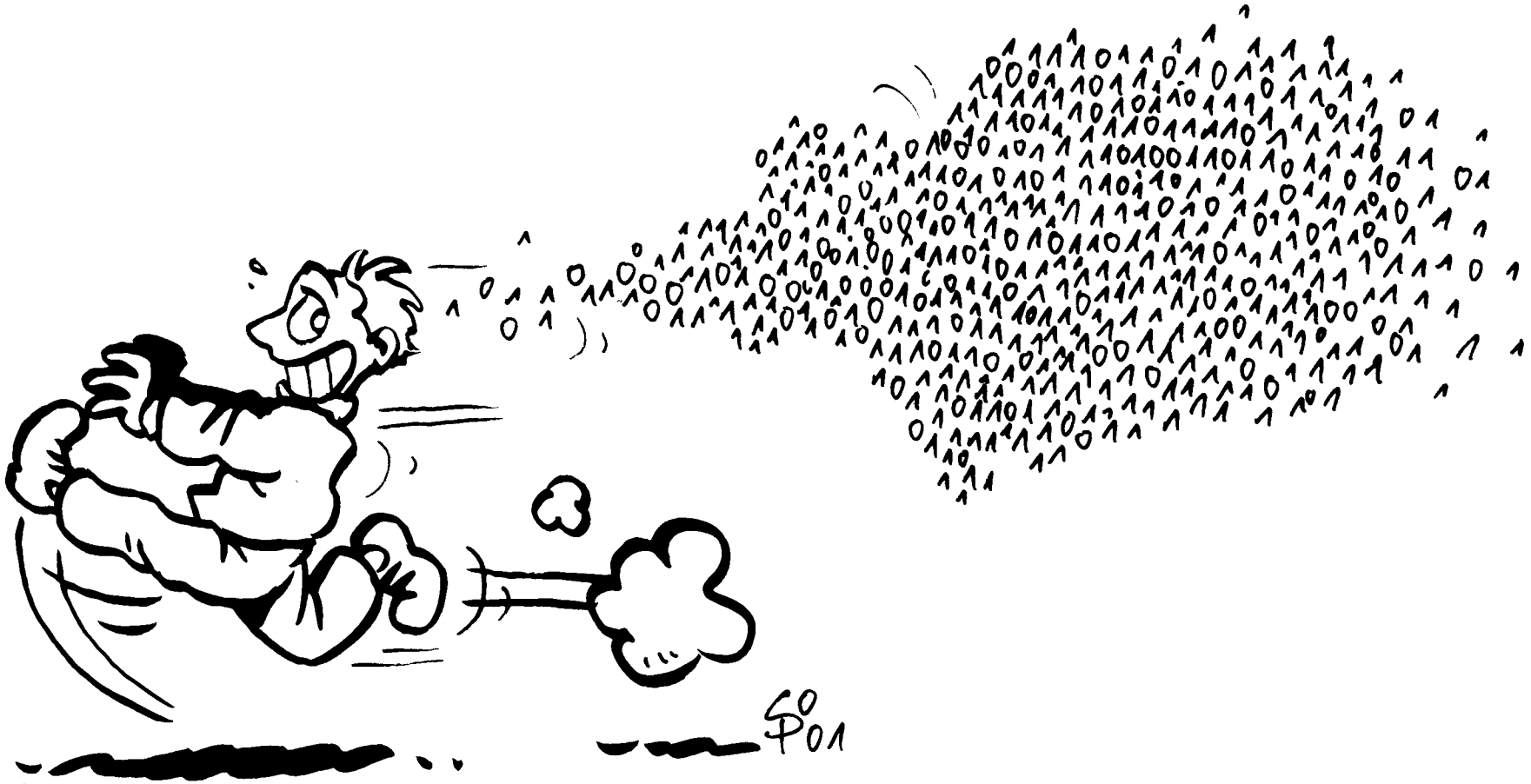
Bisher ist eine Daten verarbeitende Stelle völlig frei bei der Auswahl der eingesetzten Software und Hardware. Ihr wird lediglich auferlegt, allgemein definierte technisch-organisatorische Maßnahmen der Datensicherheit zu ergreifen. Die Verantwortung für die Zulässigkeit der Datennutzung wird regelmäßig der einzelnen Mitarbeiterin bzw. dem Mitarbeiter überlassen. Inzwischen ist es jedoch möglich, in das technische Verfahren Datenschutz systematisch zu integrieren. Ein solcher **Systemdatenschutz** stellt sicher, dass die elektronischen Datenverarbeitungsanlagen, die verarbeitenden Stellen und deren Bedienstete nur die Daten verarbeiten, wozu sie rechtlich befugt sind.

Je mehr sich die Bürgerinnen und Bürger um ihren Datenschutz selbst kümmern (können), um so mehr werden staatlichen Kontrollen überflüssig. Das bisher von einigen Datenschutzbehörden und einigen privaten Unternehmen entwickelte **Angebot zum Selbstdatenschutz** muss systematisch weiterentwickelt und ausgebaut werden. Dieses Angebot muss folgende Bestandteile aufweisen:

- Vermittlung von Datenschutzkompetenz: Dies beginnt mit der Ausbildung in der Schule (Entwicklung und dem Einsatz von adäquaten Lehr- und Lernmitteln, Sensibilisierung der Lehrkräfte) und geht bis zur allgemeinen Erwachsenenbildung (im Rahmen des Computerführerscheins, Volkshochschulangebot, Informationen in Bibliotheken und insbesondere im Internet),
- Bereitstellung von technischen Mitteln (tools) und der technischen Infrastruktur zum Selbstschutz, z.B. Prepaid-Karten, Verschlüsselungs-Software, Anonymitäts- und Pseudonymitätsangebote (z.B. anonyme Nutzung des Internet in öffentlichen Stellen, Anonymitätsserver), Identitätsmanagern,
- Schaffung der rechtlichen Voraussetzungen für Selbstschutz (Regelung eines Verfahrens für digitale Signaturen, Zulassung von Verschlüsselung),
- Herstellung von Datenverarbeitungstransparenz und Wahlfreiheit: Eine wichtige Funktion können insofern die Datenschutzbehörden erfüllen mit ihren Tätigkeitsberichten und ihrem sonstigen Informationsangebot, in dem sie nicht nur Einzelfälle, sondern systematisch Abläufe und Verfahren und mögliche Handlungsoptionen für die Bürgerinnen und Bürger darstellen. Einen wichtigen Beitrag können auch die verarbeitenden Stellen selbst leisten, indem sie verpflichtet werden, ihre Datenschutzpolitik (privacy policy) und Wahlmöglichkeiten offen zu legen. Unterstützt werden kann dies durch gemeinsame technische Standards (z.B. Platform for Privacy Preferences - P3P).

Ein Ziel moderner Datenschutzpolitik muss darin bestehen, **marktwirtschaftliche Anreize** für die Respektierung des Persönlichkeitsrechtes zu schaffen. Anbietern wie Konsumenten ist zu vermitteln, dass sich Datenschutz für sie lohnt: “Privacy sells”. Durch die Verpflichtung der verarbeitenden Stellen, ihre Datenschutzpolitik, ihr Datenschutzmanagement wie auch die Struktur der praktizierten Datenverarbeitung in einer veröffentlichten Datenschutzerklärung allgemein verständlich zugänglich zu machen, wird die Bereitschaft zu konsumentenfreundlicher Datenverarbeitung gestärkt. Die Nutzung ökonomischer Anreize kann nur gelingen, wenn die Transparenz für die Verbraucher und deren Marktmacht gestärkt werden.

Deutschland hat die weltweit längste und wohl auch die am weitesten entwickelte Datenschutzkultur. Dieses kann sich die informationstechnische Wirtschaft zu Nutze



WHO'S AFRAID OF Ø AND 1 ?

machen, indem sie **datenschutzfreundliche Produkte** entwickelt. Um deren Akzeptanz auf dem Markt zu sichern, sind diese in einem vertrauenswürdigen Zertifizierungsverfahren auf ihre Wirksamkeit hin zu auditieren. Ebenso wie eine Zertifizierung von informationstechnischen Produkten ist auch eine Auditierung von ganzen Verfahren oder Betrieben möglich und gesetzlich vorzusehen. Ein praktikables, d.h. unbürokratisches, aber dennoch vertrauenswürdiges Gesetz über ein **Datenschutzaudit** sollte vorsehen, dass die Begutachtung des Datenverarbeitungsmanagements in einem geregelten öffentlichen Verfahren unter Einbeziehung von externen Sachverständigen erfolgt.

Dort, wo Datenschutz durch die Verwaltung bzw. die Wirtschaft effektiv selbst realisiert wird, können sich Datenschutzkontrollbehörden zurückhalten. Staatliche Kontrolle hat nur eine subsidiäre Auffangfunktion. Vorrang sollten Instrumente der **Selbstregulierung** haben. Hierbei spielen die behördlichen bzw. betrieblichen Datenschutzbeauftragten eine zentrale Rolle. Deren Kompetenzen und Unabhängigkeit muss weiter gestärkt werden. Im Rahmen der Vorabkontrolle haben diese präventiv neue Verfahren auf ihre spezifischen Gefahren hin zu überprüfen. Ergänzt wird diese interne Datenschutzinstanz durch Auditierungs- und Zertifizierungsverfahren.

Als unternehmensübergreifende Form der Selbstregulierung werden **Verhaltensrichtlinien** (codes of conduct) gefördert, die die Aufgabe haben, die notgedrungen allgemeinen gesetzlichen Regelungen branchenspezifisch zu präzisieren. Die Wirksamkeit der Verhaltensrichtlinien hängt davon ab, dass diese für verbindlich erklärt werden, über Veröffentlichungen allgemein zugänglich sind und damit von den Bürgerinnen und Bürgern auf ihre Einhaltung hin kontrolliert werden können.

Die **datenschutzrechtlichen Betroffenenrechte** haben sich bewährt. Durch die Ansprüche auf Auskunft und Akteneinsicht sowie das Recht auf Berichtigung, Sperrung und Löschung haben die Menschen die Möglichkeit, Kenntnis von ihren gespeicherten Daten zu erlangen und unzulässige Formen der Verarbeitung zu korrigieren. Über die Europäische Datenschutzrichtlinie wurde nunmehr als weiteres Instrument das Recht eingeführt, besonderen Formen der Datenverarbeitung zu widersprechen und dadurch eine Prüfung zu initiieren. Auch die Möglichkeit, sich - ohne Nachteile befürchten zu müssen - an die zuständige Datenschutzkontrolle zu wenden, ist weitgehend anerkannt. Dieses Anrufungsrecht sollte ausdrücklich auf den betrieblichen bzw. behördlichen Datenschutzbeauftragten übertragen werden.

Bei aller Ausrichtung auf die Technik: Auch **konventionelle Datenverarbeitung** kann zu massiven Beeinträchtigungen führen. Es bleibt wichtig, den Datenschutz nicht nur bei der elektronischen Datenverarbeitung, sondern auch im konventionellen Umgang mit Akten sicherzustellen. Die Menschen müssen die Gewissheit haben, dass ihre Privatsphäre umfassend geschützt wird. Auch darf nicht aus den Augen verloren werden, dass es in unserer Gesellschaft immer einen Teil der Bevölkerung geben wird, der kein Interesse oder **keinen Zugang zur Informationstechnik** hat. Diesen Menschen müssen die Ansprüche und Rechte des Datenschutzes unabhängig davon gewährt werden, ob sie selbst Informationstechnik nutzen.

Eine zentrale Ursache dafür, dass der Datenschutz oft nicht beachtet wird, liegt darin, dass Verstöße nicht zu wirksamen **Sanktionen** führen. Die bestehenden strafrechtlichen Regelungen sind dadurch ein stumpfes Schwert, dass sie weitgehend als Privatklagedelikte ausgestaltet sind, für deren Verfolgung kein öffentliches Interesse angenommen wird. Verfolgungsvoraussetzung ist zudem, dass ein innerhalb einer kurzen Frist (3 Monate) vom Betroffenen ein Strafantrag gestellt wird. Bündnis 90/Die Grünen treten auf

der einen Seite dafür ein das Datenschutzstrafrecht zu entkriminalisieren. Als Ordnungswidrigkeiten sollten auf der anderen Seite dafür Verstöße um so nachhaltiger verfolgt werden (können).

Eine positivere Wirkung für die Beachtung des Datenschutzes als jede Strafandrohung hat jedoch die Einräumung von Schadensersatzforderungen für die Betroffenen im Fall von Rechtsverstößen. Die bestehenden Haftungsregelungen haben sich bisher als unwirksam erwiesen, weil der geforderte kausale materielle Schaden nur schwer nachweisbar ist und immaterielle Schäden regelmäßig nicht ersetzt werden müssen. Bündnis 90/Die Grünen setzen hier auf eine Verbesserung "marktwirtschaftlicher" Elemente: Bei rechtswidriger Datenverarbeitung ist den Betroffenen ein von einem Schaden unabhängiger **Bereicherungsanspruch** zuzugestehen. Dies hätte zur Folge, dass jedes Unternehmen, das mit illegalen Methoden persönliche Daten verarbeitet, den erlangten Gewinn herausgeben müsste.

Eine Stärkung des Datenschutzgedankens kann auch dadurch erreicht werden, dass **Verbraucher- und Datenschutzverbänden** eigenständige Beteiligungs- und Klagerechte zugestanden werden. Die positiven Erfahrungen mit der Verbandsbeteiligung im Wettbewerbs-, Verbraucher- und Umweltrecht lassen sich auf den Datenschutz übertragen. Bisher sind Verbände auf Öffentlichkeits- und Bildungsarbeit beschränkt. Dadurch können sie schon beachtliche Wirkungen auslösen, wie etwa die Verleihung des "Big Brother Award" an Stellen, die sich für die Beeinträchtigung der Privatsphäre besonders "verdient" gemacht haben, zeigt. Mit einer Formalisierung der Verbandsbeteiligung können einerseits die Datenschutzbehörden entlastet, können andererseits die Betroffenen von Klagerisiken befreit werden.

Dringend einer Reform an Haupt und Gliedern unterworfen werden müssen die **Datenschutzbehörden**. Deren Konzeption als Kontrollverwaltung war in den Frühzeiten des Datenschutzes sinnvoll. Inzwischen lässt sich die Beachtung der Gesetze angesichts der Qualität und der Dimension personenbezogener Datenverarbeitung nicht mehr allein mit Kontrollen durchsetzen. Hauptaufgabe der Datenschutzbehörden muss es werden, **präventiv** tätig zu sein. Dabei eröffnet sich ein gewaltiges Aufgabenspektrum, das von Bildungsangeboten über die Beratung von Betroffenen und Anwendern, über die Beteiligung bei Zertifizierungs- und Auditverfahren bis hin zu Kontrollen und Öffentlichkeitsarbeit reicht.

Doch damit nicht genug: Die juristische Ausrichtung dieser Stellen muss durch technische Kompetenz ergänzt werden. Datenschutzberatung und -kontrolle kann nur erfolgreich sein, wenn die Datenschutzinstanzen über das modernste Know-How und die zeitgemäßen technischen Medien verfügen. Das Bild vom Verbrecher im Porsche und dem Polizisten auf dem Fahrrad ist wohl nirgendwo so zutreffend wie bei der Datenschutz-"Polizei". Es geht nicht an, dass Milliardenbeträge in die Förderung der Informationstechnik gesteckt werden und die Stellen, die die Bürgerrechts- und Demokratieverträglichkeit sowie die Sicherheit dieser Technik gewährleisten sollen, nur minimal **technisch und personell ausgestattet** sind.

Neben der Veränderung der Aufgaben und der Verbesserung der Ausstattung ist auch eine **organisatorische Reform** der Datenschutzbehörden von Nöten. Nur über eine - übrigens von der Europäischen Datenschutzrichtlinie geforderte - Unabhängigkeit sowohl von der übrigen Verwaltung als auch von den verarbeitenden Stellen kann die Aufgabe eines vertrauenswürdigen Anwalts bei der Durchsetzung von Bürgerrechten wirksam wahrgenommen werden. Die überkommene Trennung zwischen öffentlichem und privatem Bereich ist

in einer auf Konvergenz angelegten Informationsgesellschaft anachronistisch. Notwendig ist eine Bündelung sämtlicher Datenschutzaufgaben in ortsnahen, aber doch zentralisierten Stellen in jedem Land und sowie im Bund, die untereinander - auch mit modernen Kommunikationstechniken - eng zusammenarbeiten.

Insbesondere: Genetische Selbstbestimmung

Eine besondere Herausforderung stellen die neuen Möglichkeiten der Genomanalyse dar. Nach der weitgehenden **Entzifferung des menschlichen Genoms** (DNA) arbeiten viele Wissenschaftler daran, bestimmten Genabschnitten medizinische Dispositionen, Krankheiten und körperliche Eigenschaften, aber auch persönliche und charakterliche **Anlagen zuzuordnen**. Für diese Zuordnung bedarf es umfangreicher Forschung, wobei festgestellte Eigenschaften bei Menschen mit deren genetischem Material verglichen wird. Die Genomanalyse ist im Hinblick auf viele Anwendungen sehr umstritten. So kann mit Hilfe der Pränataldiagnostik vor einer Geburt festgestellt werden, welche Eigenschaften ein künftiger Mensch haben würde. Sind die Eigenschaften nicht die gewünschten, so kann dies der Anlass für einen Schwangerschaftsabbruch sein. Bei Erwachsenen können Ergebnisse von Genomanalysen bei der Einstellung zu bestimmten Berufen, beim Abschluss von Kranken- und Lebensversicherungen und bei der medizinischen Behandlung von Bedeutung sein. Zur Feststellung von verwandtschaftlichen Beziehungen und Abstammungen und zur Identifizierung von Straftätern wird die DNA-Analyse schon in Massenverfahren genutzt. Inzwischen sind sog. Gen-Chips auf dem Markt erhältlich, mit denen zu erschwinglichen Preisen in einem einfach anzuwendenden Verfahren das Vorliegen definierter genetischer Dispositionen festgestellt werden kann. Kriminalisten fordern auch schon die Untersuchung von Straftätern auf besondere kriminalitätsfördernde Anlagen.

Bündnis 90/Die Grünen sehen keine Veranlassung die gesamte Human-Genetik zu verteufeln. So mag es möglich sein, mit Hilfe der **Gendiagnostik** auf den Patienten maßgeschneiderte Medikamente zu “designen”. Gegenüber diesen vagen Chancen dominieren jedoch die Risiken. Solange es keine Behandlungs- oder Vorsorgemöglichkeiten gibt, ist die Feststellung einer Veranlagung zu einer - u.U. tödlichen - Krankheit eine für den Patienten nutzlose psychische Belastung. Die Gefahr, dass Menschen je nach genetischer Disposition abgestempelt oder privilegiert werden, ist mit den Händen zu greifen. Es wäre mit dem Gleichheitsgrundsatz und der Menschenwürde nicht vereinbar, den Zugang zu einer Arbeit oder zu einer Lebens- oder Krankenversicherung vom Ergebnis einer obligatorischen Untersuchung abhängig zu machen. Derartiges wird in den USA und in Großbritannien schon praktiziert. Gerade Deutschland hat angesichts des Umstandes, dass in seiner jüngeren Geschichte “minderwertiges” Leben diskriminiert und vernichtet worden ist, eine besondere Verantwortung dafür, dass es in der Zukunft **keine genetische Diskriminierung** gibt.

Bündnis 90/Die Grünen setzen sich dafür ein, die **genetische Selbstbestimmung gesetzlich abzusichern**. Dabei ist klar zu definieren, unter welchen Voraussetzungen Identitäts- und Verwandtschaftsfeststellungen zugelassen werden. Will ein Mensch seine Erbanlagen untersuchen lassen, so muss ihm dies freistehen. Doch darf er nicht gezwungen werden können, dieses Wissen anderen zu offenbaren. Zur genetischen Selbstbestimmung gehört auch, dass jeder Mensch ein “Recht auf Nichtwissen” hat; d.h. niemand darf gegen seinen Willen auf genetische Dispositionen hin untersucht werden.

CHANCEN DURCH GEN-TECHNIK

Eine Vorlage gegenüber Versicherungen und Arbeitgebern muss ausgeschlossen werden. Viel wichtiger als jede einzelne gesetzliche Regelung ist aber, dass eine **öffentliche Debatte** über die ethische, demokratische und rechtsstaatliche Verantwortbarkeit spezieller gentechnischer Anwendungen stattfindet.

Die Informationstechnik birgt **Chancen und Risiken**. Zu den unbestreitbaren Verbesserungen gehört es, dass die Menschen dadurch ein fast unbegrenztes Medium zur Beschaffung von Informationen und zu Äußerung der eigenen Meinung in der Hand haben, dessen Nutzung sich nicht auf wenige Privilegierte beschränkt. Unbestreitbar sind auch die Erleichterungen, die die Informationstechnik bei der Arbeit und im Alltag beschert. Es wäre widersinnig, diese Möglichkeiten zur Verbesserung von Demokratie und Lebensqualität nicht zu nutzen. Daher muss dafür gesorgt werden, dass die bestehenden Risiken eingegrenzt werden. Den Gefahren für die informationelle Selbstbestimmung und die Privatheit soll mit einem modernen Datenschutz begegnet werden. Bündnis 90/Die Grünen werden sich daher auch weiterhin und noch verstärkt dafür einsetzen, dass mit der Entwicklung der Informationsgesellschaft auch der Datenschutz kontinuierlich ausgebaut wird.

Es kann keinen hundert prozentigen Schutz der Privatsphäre geben. Der Datenschutz muss sich permanent den sich verändernden Rahmenbedingungen der Informationsverarbeitung anpassen. Datenschutz bleibt eine **permanente Herausforderung**. Bündnis 90/Die Grünen werden sich dieser Herausforderung dauernd neu stellen.

Die **blinde Technikeuphorie** von CDU, SPD und FDP ist letztendlich schädlich für die technische Entwicklung und für den Standort Deutschland, weil deren rein ökonomische Sichtweise die notwendigen rechtlichen, sozialen und kulturellen Rahmenbedingungen für eine Technikentwicklung im Interesse der Menschen ignoriert. Bündnis 90/Die Grünen sehen sich dagegen - u.a. durch ihr Engagement für den Datenschutz - einem ganzheitlichen Ziel verpflichtet:

Bündnis 90/Die Grünen wollen, dass Sie sich wohl fühlen in der Informationsgesellschaft!