

**Internationales Symposium  
Informationsfreiheit und Datenschutz**

25./26. Oktober 1999 in Potsdam

Veranstaltung des  
Landesbeauftragten für den Datenschutz  
und für das Recht auf Akteneinsicht  
in Zusammenarbeit mit der  
Alcatel SEL Stiftung für Kommunikationsforschung

Dokumentation

## **Impressum**

Herausgeber: Der Landesbeauftragte für den Datenschutz und  
für das Recht auf Akteneinsicht Brandenburg  
Stahnsdorfer Damm 77, Haus 2  
14532 Kleinmachnow

Juli 2000

Telefon: 03 32 03 / 356-0  
Fax: 03 32 03 / 356-49

e-Mail: [Poststelle@LDA.Brandenburg.de](mailto:Poststelle@LDA.Brandenburg.de)  
Internet: <http://www.lda.brandenburg.de>

Fingerprint: 0DD70C8A 65508B73 2A53EFEE AC857D66

Druck: Brandenburgische Universitätsdruckerei und  
Verlagsgesellschaft Potsdam mbH

## Inhalt

	Seite
Vorwort	7
Dr. Alexander Dix	
Eröffnung / Opening	9
Dr. Dieter Klumpp	
Grußwort zur Eröffnung / Greeting	13
Claus-Henning Schapper	
Ein allgemeines Informationszugangsgesetz für die Bundesrepublik Deutschland? / A general Information Access Act for the Federal Republic of Germany?	17
Prof. Dr. Shizuo Fujiwara	
Das neue japanische Informationszugangsgesetz / The new Japanese Information Access Act	27
Dr. Robert Gellman	
Das Informationsfreiheitsgesetz in den Vereinigten Staaten: Von den Akten bis zum Internet / Freedom of Information Act in the United States: From Paper Records to the Internet	39
Prof. Dr. David H. Flaherty	
Die Balance zwischen transparenter Verwaltung und Schutz der Privatsphäre: Kanadische Erfahrungen / Balancing open government and privacy protection: Some Canadian experiences	51

Viktor Monachov

Die Entwicklung des Informationsrechts in Russland / The development of information law in Russia 61

George Papapavlou

Das Grünbuch der Europäischen Kommission "Informationen des öffentlichen Sektors - eine Schlüsselressource für Europa" / The EU Commission Green Paper on "Public Sector Information - a key resource for Europe" 81

Bettina Sokol

Grundrechtliche Aspekte des Informationszugangs / Fundamental rights aspects of access to information 107

Prof. Dr. Alexander Roßnagel

Das Datenschutz-Audit / The Privacy Audit 117

Prof. Dr. Hansjürgen Garstka

Datenschutz und Informationsfreiheit - zwei Bausteine für ein Informationsgesetzbuch / Data Protection and Freedom of Information - two elements for an Information Code 139

Dr. Thilo Weichert

Für ein bürgerfreundliches Datenschutz- und Informationszugangsrecht / The case for citizen-friendly data protection and access to information-law 149

Welf Schröter

Arbeit 21: Der mobile Multimedia-Arbeitsplatz / Work 21: The mobile multimedia workplace 159

Arend Steenken

Das Landesverwaltungsnetz - Chancen für eine  
bürgernahe Verwaltung / The State Administration  
Network - opportunities for open government

179

Dr. Hans-Jürgen Lemle

Elektronische Akteneinsicht in einer brandenburgischen  
Stadtverwaltung / Electronic Access to Information in a  
Brandenburg local authority

191



## Vorwort

"Der Sonnenschein der informierten Gesellschaft kann sowohl den Rost der Korruption, als auch den Schimmel der Inkompetenz in der Tätigkeit der Staatsmacht und Selbstverwaltung wirkungsvoll bekämpfen." Diese markante Formulierung stammt von Viktor Monakhov, dem Mitglied des Gerichts für Informationsstreitigkeiten beim Präsidenten der Russischen Föderation. Er beschreibt damit in erster Linie die Situation in seinem Heimatland, wenngleich auch in anderen Ländern Verwaltungstransparenz als ein Mittel zur Bekämpfung der Korruption angesehen wird. Robert Gellman, ehemals Berater im amerikanischen Kongress, hebt hervor, dass der freie Informationszugang zu Verwaltungsinformationen nicht immer zur Aufdeckung von Skandalen führen muss, sondern eine unspektakuläre, aber wichtige Voraussetzung für bürgerschaftliches Engagement vor Ort ist.

Damit sind beispielhaft zwei sich ergänzende Positionen beschrieben, die bei dem von uns gemeinsam mit der Alcatel SEL Stiftung für Kommunikationsforschung im Oktober 1999 veranstalteten Internationalen Symposium "Informationsfreiheit und Datenschutz" in Potsdam vertreten wurden. Da dieses Symposium das erste seiner Art war und bundesweit Beachtung gefunden hat, dokumentieren wir die gehaltenen Vorträge in diesem Band und wollen damit einen weiteren Anstoß für die Diskussion um die Verzahnung von Datenschutz und Informationsfreiheit geben. Richtig verstandener Datenschutz wird von einer modernen "öffentlichen" Verwaltung nicht als Vorwand dafür benutzt, um den Bürgerinnen und Bürgern die Informationen vorzuenthalten, die sie zur Mitgestaltung ihres Gemeinwesens auf gemeindlicher oder staatlicher Ebene benötigen. Umgekehrt bleibt das Recht des Einzelnen auf informationelle Selbstbestimmung ein Grundrecht, das mit dem Grundrecht auf Informationszugang nach der Verfassung des Landes Brandenburg in jedem Einzelfall abzuwägen ist. Beiden Grundrechten soll dabei eine größtmögliche Wirksamkeit zukommen.

Mit dieser Dokumentation beginnen wir zugleich die neue Publikationsreihe der "Potsdamer Materialien zu Akteneinsicht und Informationszugang", in der wir in unregelmäßigen Abständen weitere

Dokumente zu diesem Thema veröffentlichen wollen. Für entsprechende Anregungen sind wir dankbar.

Dr. Alexander Dix  
Landesbeauftragter für den Datenschutz  
und für das Recht auf Akteneinsicht

## **Dr. Alexander Dix**

Landesbeauftragter für den Datenschutz und  
für das Recht auf Akteneinsicht Brandenburg

### **Eröffnung des Internationalen Symposiums**

Ich begrüße Sie ganz herzlich zu unserem Internationalen Symposium in Potsdam und freue mich besonders, dass unsere Einladung eine so breite Resonanz gefunden hat.

Das Thema "Informationsfreiheit und Datenschutz", mit dem wir uns in den kommenden beiden Tagen befassen wollen, ist ein neues Thema in der deutschen Diskussion. Während der Datenschutz seit fast dreißig Jahren in den alten Bundesländern und seit der Vereinigung auch in den neuen Ländern seinen festen Platz hat, ist der allgemeine Zugang der Bürgerinnen und Bürger zu Informationen in der öffentlichen Verwaltung ein Grund- und Menschenrecht, das erstmals in der Verfassung des Landes Brandenburg von 1992 verankert wurde.

Aber ist die Pflicht der Verwaltung, ihr Handeln gegenüber den Bürgerinnen und Bürgern transparent zu gestalten, wirklich so neu? Die brandenburgische Verfassung sieht im allgemeinen Akteneinsichtsrecht eine Voraussetzung zur politischen Mitgestaltung. Damit wird der Informationszugang in den Zusammenhang des Demokratieprinzips gestellt, das im Grundgesetz und sinngemäß auch in allen Länderverfassungen in den Worten "Alle Staatsgewalt geht vom Volke aus" seinen Ausdruck findet. Zugang zu Informationen auf der Ebene der Gemeinden, der Landkreise und der Landesverwaltung ist eine entscheidende Voraussetzung dafür, dass der demokratische Prozess sich nicht auf die Teilnahme an Wahlen beschränkt.

Gegenwärtig wird vielfach an die friedliche Revolution erinnert, die vor fast genau zehn Jahren in diesem Teil Deutschlands stattgefunden hat. Auch die verfassungsrechtliche Verankerung des Rechts aller Menschen, Einsicht in Akten und amtliche Unterlagen der Behörden zu erhalten, ist zu einem wesentlichen Teil der Bürgerbewegung zu verdanken, die dieses Anliegen auf ihre Fahnen geschrie-

ben hatte.

Zugleich hat das Land Brandenburg mit diesem Grundrecht und dem im vergangenen Jahr in Kraft getretenen Akteneinsichts- und Informationszugangsgesetz als erstes Land der Bundesrepublik den Anschluss an die internationale Rechtsentwicklung hergestellt, die seit langem in vielen demokratischen Staaten den Grundsatz der Informationsfreiheit und der transparenten Verwaltung anerkannt hat. Deshalb ist es an der Zeit, sich die umfangreichen ausländischen Erfahrungen zunutze zu machen, die etwa in Nordamerika gesammelt worden sind. Auch in Ländern mit so unterschiedlichen politischen Systemen wie Japan und Russland gewinnt der Grundsatz der Verwaltungsöffentlichkeit in der Gesetzgebung immer mehr an Bedeutung. Die Europäische Kommission hat eine Initiative zur Nutzung der Informationsbestände des öffentlichen Sektors ergriffen, über die wir morgen Näheres hören werden.

Auch in Deutschland macht das Brandenburger Beispiel Schule. Die benachbarte Bundeshauptstadt hat im zweiten Anlauf ein Informationsfreiheitsgesetz beschlossen, dem Landtag in Schleswig-Holstein liegen entsprechende Gesetzentwürfe vor, und auch die Bundesregierung und die sie tragenden Parteien haben die Bedeutung dieses Themas offenbar erkannt. Auch wenn das Akteneinsichts- und Informationszugangsgesetz vielleicht kein Brandenburgischer "Exportschlager" sein kann, so hat es doch zu einer Entwicklung beigetragen, die jetzt zunehmend an Fahrt gewinnt. Umgekehrt werden wir in Brandenburg die Entwicklung des Informationszugsrechts im In- und Ausland aufmerksam beobachten müssen, um daraus Lehren für die notwendige Weiterentwicklung des in einzelnen Punkten verbesserungsbedürftigen Akteneinsichts- und Informationszugangsgesetzes zu ziehen. Ich erhoffe mir gerade auch von unserem Symposium in dieser Richtung wertvolle Hinweise.

Wir haben bewusst die Informationsfreiheit in der Verknüpfung mit dem Datenschutz an erster Stelle im Thema dieser Veranstaltung genannt haben, um die jetzt erforderliche grundlegende Veränderung im Verhältnis zwischen den Bürgerinnen und Bürgern einerseits und der Verwaltung andererseits hervorzuheben. Aber natürlich tritt der Datenschutz dadurch nicht etwa in den Hintergrund. Das Akteneinsichtsrecht findet im Grundsatz seine berechnigte Grenze im

Recht auf informationelle Selbstbestimmung, das von der Landesverfassung ebenfalls mit Grundrechtsqualität versehen worden ist.

Darüber hinaus befinden wir uns gegenwärtig aber auch beim Datenschutz in einer Umbruchsituation, weil auf Bundesebene die Angleichung an europäischen Mindeststandard noch aussteht; mehr noch: es ist inzwischen allgemein anerkannt, dass über grundlegend neue Datenschutzkonzepte nachgedacht werden muss. Kasuistische bereichsspezifische Regelungen waren nötig, um für die Bürgerinnen und Bürger Eingriffe in ihr Grundrecht auf Datenschutz transparent und überprüfbar zu machen. Aber inzwischen wird immer deutlicher, dass derartige Regelungen im Zeitalter des Internets nicht mehr ausreichen, um den einzelnen Menschen effektiv in seiner Privatsphäre zu schützen. Datenschutzfreundliche Technologien und Selbstschutzmöglichkeiten müssen ergänzend gefördert und publik gemacht werden, damit die Chancen der neuen Informationsangebote und Kommunikationsmöglichkeiten bei gleichzeitiger Kontrolle der Risiken genutzt werden können.

Das neue Brandenburgische Datenschutzgesetz vom Dezember vergangenen Jahres greift bereits einige dieser neuen Ansätze auf, indem es etwa zum erstenmal in Deutschland ein Datenschutz-Audit im Bereich der öffentlichen Verwaltung ermöglicht und ausdrücklich den Grundsatz der Datensparsamkeit verankert. Auch die behördlichen Datenschutzbeauftragten, von denen heute erfreulicherweise viele hier im Saal sind, hat der Gesetzgeber mit bestimmten Aufgaben betraut. Dennoch halte ich die Struktur der Datenschutzkontrolle in unserem Land für verbesserungsbedürftig. Die Teilung der Aufsicht im öffentlichen und im privaten Bereich zwischen verschiedenen Behörden ist in meinen Augen überholt und sollte aufgegeben werden. Bei der Novellierung des Landesdatenschutzgesetzes im letzten Jahr ist diese Frage bis zur Verabschiedung des neuen Bundesdatenschutzgesetzes zurückgestellt worden. Ich werde mich weiter dafür einsetzen, die Datenschutzaufsicht beim Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht zu konzentrieren, damit die Bürgerinnen und Bürger *eine* Anlaufstelle in Sache Datenschutz haben. Dafür gibt es zunehmend positive Beispiele auch in anderen Bundesländern.

Informationszugang und Datenschutz können als zwei sich schneidende Kreise verstanden werden: es gibt viele Fragen des Akteneinsichtsrechts, die keine Berührung zu Datenschutz haben, und es gibt zahlreiche komplizierte datenschutzrechtliche Probleme - ich nenne nur als Stichworte die Gesundheitsreform 2000 oder die Schleierfahndung -, die über das allgemeine Informationszugangsrecht weit hinausgehen. Die Schnittmenge zwischen diesen beiden Kreisen kann zu einer schwierigen Abwägung zwischen den grundrechtlich geschützten Positionen im Einzelfall führen. Das ist aber für den Datenschutz nichts neues, denn solche Abwägungen waren auch bisher schon zum Beispiel im Bereich der Forschung nötig.

Entscheidend ist vielmehr, dass weder der Datenschutz noch Geheimhaltungsinteressen des Staates pauschal eine Verweigerung des allgemeinen Informationszugangs rechtfertigen. Umgekehrt wird der Datenschutz durch das Akteneinsichtsrecht nicht etwa insgesamt relativiert. Informationsfreiheit und Datenschutz hindern auch nicht - wie zuweilen eingewandt wird - die Verwaltung an ihrer Aufgabenerfüllung, sondern sie sind im Gegenteil geradezu Qualitätsmerkmale einer modernen öffentlichen Verwaltung. Erst mit den Grundrechten auf Informationszugang und Datenschutz werden die Bürgerinnen und Bürger zu Subjekten einer zivilen Informationsgesellschaft.

Meine Damen und Herren,  
mit diesen einleitenden Bemerkungen sollen nur einige der vielfältigen Probleme angerissen werden, zu deren Lösung unser Symposium beitragen kann. Ich hoffe auf ertragreiche Diskussionen heute und morgen.

## **Dr. Dieter Klumpp**

Geschäftsführer der Alcatel SEL Stiftung für Kommunikationsforschung

### **Grußwort zur Eröffnung**

Es gibt im Bereich des Rechts prinzipiell zwei Möglichkeiten, mit Innovationen umzugehen, wie sie zum Beispiel das jahrzehntelange Feuerwerk der Kommunikations- und Informationstechnik fast im Monatstakt hervorbringt.

Die erste ist, der Innovation freien Lauf zu lassen und die Bürger als Messfühler dafür zu nehmen, ob sich die Innovation in den Rechtsrahmen oder in die Gewohnheiten einfügt. Ganz ohne Zweifel ist dies der bessere Weg für die Innovation. Die Verfechter dieses Weges führen zu Recht an, dass es prinzipiell sehr schwierig ist, künftige Innovationen a priori juristisch zu regeln, weil die Zukunftsentwicklung der Technik sich weder um Gesetze noch um Gewohnheiten kümmert. Man kann, so sagen die entsprechenden Juristen, nur beim ersten Präzedenzfall für Rechtsverstöße regulierend eingreifen. Dieser Weg passt sehr gut zur gesamten Rechtsphilosophie der angelsächsischen Länder, weshalb es nicht verwundern darf, dass zum Beispiel amerikanische Techniklieferanten am liebsten ihre Rechtsordnung gleich mitliefern würden. Ein gewisses Problem resultiert daraus, dass Messfühler in der Technik etwas sehr robustes sind, der Bürger im Rechtsstaat ist dies nicht.

Der zweite Weg, juristisch mit Innovationen umzugehen, ist die Rahmensetzung, an die sich die technische Entwicklung anzupassen hat. Ganz ohne Zweifel ist dies der bessere Weg für die Juristen. Denn mit der Erarbeitung des auch im Detail präzisen gesetzlichen Rahmens kann der Rest von der Judikative und der Exekutive abgearbeitet werden. Diese Vorgehensweise ist als der traditionelle mitteleuropäische Weg zur rechtlichen Behandlung von Innovationen anzusehen. Ein gewisses Problem resultiert daraus, dass die Erarbeitung eines detaillierten rechtlichen Rahmens manchmal länger dauert als der Lebenszyklus der Innovation.

Es muss auffallen, dass es den ersten Weg in völliger Perfektion nirgends auf der demokratischen Welt gibt. Denn kein demokratisches Land und keine Rechtsordnung lässt ein so überzogenes laissez-faire zu. Gewisse Grundregeln werden beachtet, ob das Recht nun kodifiziert ist oder nicht. Man kann vereinfachend sagen, dass der erste Weg im großen und ganzen in der Pionierphase einer Innovation funktioniert, und dass erst über der Zeitachse Probleme auftauchen. Diese können zum einen aus den "verflixten Details" herrühren, aber auch auf plötzliche Freisetzung eines aufgestauten Problems. So ist zum Beispiel in USA der Gebrauch der Kreditkarte in vielerlei Hinsicht anders als in Europa: Zum einen ist mittlerweile der statistische Durchschnittsamerikaner mit rund vier Monatsgehältern verschuldet, zum anderen hat es noch nie ein Problem mit der Kreditkartenabrechnung gegeben, das sich nicht mit Kulanz hätte lösen lassen. Nur: Wenn einmal die Kulanzgrenze (deren Höhe nur die Kreditkartenemittenden kennen) drastisch überschritten sein sollte, dann wäre ein systembedrohender Dammbbruch - im Minimum der Zusammenbruch des e-commerce - die Folge.

Es muss hingegen auch auffallen, dass es den zweiten Weg sehr wohl in völliger Perfektionierung gibt, Deutschland kämpft hier mit seinem inhärenten Perfektionsstreben regelmäßig um Platz 1. Und wo es diesen ersten Platz nicht erreicht, zum Beispiel bei der Zahl der – übrigens in Italien viel zahlreicheren - Umweltschutzregeln, schafft Deutschland regelmäßig und stolz die Weltmeisterschaft bei der Implementierung. Wenn es in Deutschland irgendwo so etwas wie eine "Erfinderstube" gibt, dann müsste sie voller juristischer Loseblattsammlungen stehen oder besser gleich an eine Hotline bei JURIS angeschlossen sein.

Es kann eigentlich wenig Zweifel darüber geben, dass beide extremen Wege gerade für die Dynamik der Innovationen auf den technischen Feldern der Innovations- und Kommunikationstechnik nichts taugen.

Der puristische Weg des *Präzedenzfalls* führt viel zu schnell (und meist nicht zufällig) in die unterste Hierarchie der Jurisdiktion, die dann auch erwartbar mit der Grundsatzbedeutung des von ihnen erwarteten Urteils überfordert ist. Was geschieht einem Internet-Provider vor dem bayrischen Landgericht? Was wird denn ein Ge-

richt in Colorado mit dem ersten Computerkid tun, das massiv gegen das Strafrecht verstößt?

Der puristische Weg der *antizipierenden Rechtsnormen* führt zwingend zu Expertenkommissionen, deren Behandlungsgegenstand sich schneller ändert, als die Zwischenberichte geschrieben werden können; sie führt auch zu Abschlussberichten bzw. Gesetzeswerken, in deren Begleittext steht, dass die Praxis innerhalb von zwei Jahren unbedingt noch einmal überprüft werden müsse.

Der Mittelweg, wie ihn zum Beispiel auch das IuKDG in Deutschland versucht, ein Weg, der ganz pragmatische Einsprengsel auf einem innovationsgetränkten Regulierungsgebiet versucht, ist als "goldener" Weg nicht möglich. Denn die Mitte ist fest in Händen von sogenannten bzw. selbsternannten Pragmatikern, die von "klaren Rahmenbedingungen" reden, aber diejenige Rahmenbedingung als die klarste ansehen, die bei genauer Betrachtung nur eine Wolke ist. Manche dieser "Praktiker" aus Wissenschaft, Wirtschaft und Politik (nicht zu vergessen: der Publizistik!) – hätten am liebsten überhaupt kein Gesetz, das aber im Fall der eigenen Betroffenheit gar nicht genug Paragraphen haben kann.

Es bleibt ein "steiniger" Mittelweg, bei dem sich die verschiedenen Rechtsauffassungen gegenseitig befruchten müssen und nicht bekämpfen dürfen. Unsere Konferenz hier soll – trotz aller Bequemlichkeit des Ambiente – also eine Zwischenstation auf sehr steinigem Terrain sein.

Erschwerend kommt hinzu, dass beim Datenschutzbeauftragten gerade hier in Brandenburg nicht nur wie überall sonst die technische und wirtschaftliche Innovation Gegenstand ist. Es geht in einem Bundesland mit dem "Recht auf Akteneinsicht" auch um eine bedeutende gesellschaftliche Innovation, die in den USA mit dem Right-to-Information-Act angestoßen wurde. Für gesellschaftliche Innovationen gilt das, was ich über die technischen Innovationen gesagt habe, in noch viel höherem Masse. Denn gesellschaftliche Innovationen brauchen keine günstigen Rahmenbedingungen, sie entstehen sogar unter sehr schlechten Rahmenbedingungen, wie man hier in Potsdam und anderswo in der DDR vor zehn Jahren mit beweiswürdiger Evidenz sehen konnte.

Deswegen schlieÙe ich mit einem Hinweis auf die spannende Konstellation, die sich beim Recht auf Akteneinsicht in den USA, aber auch hier ergibt: In der Sprache der pragmatischen Techniker ist das Recht auf Akteneinsicht eine bedeutsame Spielart des "Hungers nach Bandbreite", die er auf Anforderung zu stillen vermag. In der Sprache der pragmatischen staatlichen Verwalter ist es ein "inhärenter Zwang zur Verlässlichkeit und Qualität von Kommunikationssystemen", die allem Anschein nach nur er – innerhalb der gegebenen internationalen Marktdynamik - sicher stellen kann. Beide, Techniker in Unternehmen wie Verwalter in Behörden, treffen sich bei Max Webers axiomatischer Feststellung, dass ein Wirtschaftssystem ohne eine "Berechenbarkeit des Rechts" auf Dauer nicht erfolgreich sein kann.

Allein schon diese Konstellation verspricht einen spannenden Verlauf unserer Tagung, was hoffentlich nicht nur bei mir apriorische Freude hervorruft. Die Alcatel SEL Stiftung hat seit Mitte der achtziger Jahre gerade auch auf dem Datenschutzgebiet immer wieder helfen können, wenn es darum ging, aufkeimende Konfrontationen abzufangen und zu einer antizipierenden Gestaltung beizutragen, Als Fördergrund reicht die gesicherte Vermutung aus, dass Gestaltung die beste Form der Regulierung darstellt. Viel versprechende Ansätze der Wirtschaft und Verwaltung für e-commerce und e-ministration brauchen diese Gestaltung, weil der "trial-and-error" zu lange den Zustand der "Nicht-Berechenbarkeit" aufrecht erhalten könnte.

## **Claus-Henning Schapper**

Staatssekretär im Bundesministerium des Innern

### **Ein allgemeines Informationszugangsgesetz für die Bundesrepublik Deutschland?**

Die Bundesregierung verfolgt das Leitbild des "aktivierenden Staates". Sie will den Bürger stärker als bisher am staatlichen Leben teilhaben lassen und ihn ermutigen, mehr Verantwortung zu übernehmen. Wirklich effektiv können Bürgerrechte nur dann wahrgenommen werden, wenn die behördlichen Entscheidungen transparent sind. Dies wiederum setzt voraus, daß der Bürger Zugang zu Behördeninformationen hat. Eine solche Zugangsmöglichkeit ist in einer repräsentativen Demokratie von essentieller Bedeutung, zumal der Informationsvorsprung der öffentlichen Verwaltung dank der modernen Informations- und Kommunikationstechniken ständig wächst. In der Koalitionsvereinbarung von SPD und Bündnis90/Die Grünen ist daher vorgesehen, allen Bürgern Informationszugangsrechte durch ein Informationsfreiheitsgesetz zu verschaffen. Der Datenschutz soll und muß dabei berücksichtigt werden. Der Grundsatz eines freien Zugangs zu Behördeninformationen macht detaillierte Bestimmungen zu den unabdingbar schützenswerten personenbezogenen Daten Dritter erforderlich. Andererseits darf aber der Datenschutz nicht der Verwaltung als willkommener Vorwand dafür dienen, dem Bürger Informationen zu verweigern. Beides, das Recht auf informationelle Selbstbestimmung in seiner datenschutzrechtlichen Ausprägung und die Gewährleistung eines freien Zugangs zu Informationen sind wesentliche Voraussetzungen für die Teilhabe des einzelnen an der demokratischen Gesellschaft.

### **Bisherige Rechtslage in Deutschland**

Informationszugang kann durch Auskunftserteilung oder durch Akteneinsicht ermöglicht werden. Das bestehende Recht in Deutschland ist gekennzeichnet durch die Grundsätze der Vertraulichkeit der Verwaltung und der beschränkten Aktenöffentlichkeit, Grundsätze, die übrigens nicht nur dem "Schutz der Verwaltung vor dem Bürger"

dienen, sondern umgekehrt auch die Vertraulichkeit der bei der Verwaltung vorhandenen personenbezogenen Informationen gewährleisten. Entsprechend diesen Prinzipien besteht bisher ein Anspruch auf Informationszugang nur aufgrund spezieller Regelungen, die ganz überwiegend besondere Voraussetzungen vorsehen, gleich ob der Informationszugang in Form der Auskunftserteilung oder der Akteneinsicht erfolgt.

Beispiele:

- Innerhalb eines Verwaltungsverfahrens besteht ein Anspruch auf Akteneinsicht nur für den Beteiligten und auch nur dann, wenn die Aktenkenntnis zur Geltendmachung oder Verteidigung seiner rechtlicher Interessen erforderlich ist (§ 29 VwVfG);
- Die Einsicht in Personenstandsbücher ist nur bei rechtlichem Interesse möglich (§ 61 Abs. 1 Satz 3 PStG), die Einsicht in das Grundbuch nur bei berechtigtem Interesse (§ 12 GBO);
- Einsicht in Archivgut wird erst nach Ablauf langjähriger Schutzfristen gewährt (§ 5 BArchG).

Weitergehende Rechte gibt es auf Bundesebene bisher nur in besonderen Bereichen. Im Öffentlichen Recht gibt es hierzu bereichsspezifische Regelungen im Stasi-Unterlagengesetz und im Umweltinformationsgesetz. Freie Einsicht besteht bei Registern mit zivilrechtlichem Inhalt, etwa dem Handels-, Vereins- und Güterrechtsregister.

## **Rechtsvergleichung**

Allerdings ist außerhalb des Anwendungsbereichs der genannten Vorschriften der Zugang zu behördlichen Informationen in Deutschland nicht ausgeschlossen. Denn die Behörde hat entsprechende Anträge nach pflichtgemäßem Ermessen zu bescheiden. Im Einzelfall unterscheiden sich daher die faktischen Möglichkeiten des Informationszugangs oft nur geringfügig von den Möglichkeiten in Staaten mit einem gesetzlich verankerten Informationsanspruch, der dann durch zahlreiche Ausnahmen zum Schutz persönlicher Daten,

von Betriebsgeheimnissen oder in staatlichem Interesse eingeschränkt wird.

Durch eine Umkehrung des jetzigen Regel-Ausnahme-Verhältnisses würden jedoch die Transparenz staatlichen Handelns und die Beteiligung der Bürger gefördert. Ein gesetzlich geregelter Anspruch auf Informationszugang würde das Verhältnis zwischen Staat und Bürger weniger obrigkeitsstaatlich als vielmehr partnerschaftlich begreifen. Zudem entspräche ein solcher Anspruch europäischen, internationalen und innerstaatlichen Entwicklungen.

In fast allen westeuropäischen Nachbarstaaten gibt es mittlerweile Informationszugangsgesetze, in Schweden bereits seit 200 Jahren. Auch in Großbritannien, das lange Zeit als "verschlossenste" aller westlichen Demokratien galt (so der frühere Premierminister Edward Heath), wird seit 1996 an einem freedom-of-information-act gearbeitet. In den USA gibt es ein solches Gesetz seit 1966.

Auf EU-Ebene hat der Bürger ein in Art. 255 EGV verankertes allgemeines Zugangsrecht zu den Dokumenten des Europäischen Parlaments, des Rates und der Kommission. Die Kommission hat erkannt, daß der Zugang zu Informationen nicht nur in demokratisch-rechtsstaatlicher Hinsicht, sondern auch in wirtschaftlicher Hinsicht von Bedeutung ist. Vor einigen Monaten hat die EU-Kommission ein „Grünbuch über die Informationen des Öffentlichen Sektors in der Informationsgesellschaft“ herausgegeben. ... Es befaßt sich mit der Wettbewerbsfähigkeit der europäischen Wirtschaft angesichts der Möglichkeiten, öffentliche Informationen kommerziell zu nutzen. Zur Zeit werden die Ergebnisse einer in diesem Zusammenhang durchgeführten Umfrage bei Unternehmen und Bürgern der einzelnen Mitgliedstaaten ausgewertet.

Auf der Ebene des Europarats hat das Ministerkomitee bereits 1981 eine Empfehlung zum freien Zugang zu amtlichen Informationen verabschiedet. Seit drei Jahren erarbeitet eine Arbeitsgruppe des Lenkungsausschusses für Menschenrechte beim Ministerkomitee des Europarats den Entwurf einer konkretisierten Empfehlung.

International spielt der Zugang zu Informationen vor allem im Umweltbereich eine wichtige Rolle. Ein Beispiel hierfür ist das Über-

einkommen der Wirtschaftskommission der Vereinten Nationen für Europa über den Zugang zu Informationen, die Beteiligung der Öffentlichkeit an Entscheidungsverfahren und den Zugang zu Gerichten in Umweltangelegenheiten. Deutschland hat diese sogenannte Aarhus-Konvention im Dezember 1998 gezeichnet; sie bedarf noch der Ratifikation.

Nicht zuletzt entspricht eine Erweiterung der Informationszugangsrechte auch innerstaatlichen Entwicklungen. Hier in Brandenburg existiert seit eineinhalb Jahren gemäß einem Auftrag der Landesverfassung ein Akteneinsichts- und Informationszugangsgesetz. Auch das Berliner Abgeordnetenhaus hat vor wenigen Wochen ein Informationsfreiheitsgesetz verabschiedet, das noch in diesem Jahr in Kraft treten soll. In Schleswig-Holstein hat der Südschleswigsche Wählerverband kürzlich einen entsprechenden Gesetzentwurf eingebracht.

Das Recht auf Informationszugang steht in einem Spannungsverhältnis zum Datenschutz, auf das ich noch näher eingehen werde. Bei der Konzeption eines Informationsfreiheitsgesetzes muß deshalb sichergestellt werden, daß das Recht auf informationelle Selbstbestimmung ebenso gewahrt bleibt wie etwa das Betriebs- und Geschäftsgeheimnis sowie das Steuer- und Statistikgeheimnis.

### **Umsetzung durch Regelung in einem eigenständigen Gesetz**

Nach den Vorstellungen des Bundesinnenministeriums soll für die Informationszugangsrechte ein eigenständiges Gesetz geschaffen werden. Einzelfallregelungen in den jeweiligen Fachgesetzen zu treffen, wäre unpraktikabel. Eine ebenfalls denkbare erweiternde Änderung des Verwaltungsverfahrensgesetzes halte ich schon aus rechtssystematischen Gründen nicht für sinnvoll. Denn das allgemeine Informationszugangsrecht soll gerade auch außerhalb laufender Verwaltungsverfahren gelten. Außerdem kann ein eigenständiges Informationsfreiheitsgesetz Regelungen mit größerer Detailliertheit treffen, und zwar einschließlich der erforderlichen Ausnahmebestimmungen zum Schutz von Daten Dritter.

Ohne Zustimmung des Bundesrates kann der Bund allerdings nur eine Regelung für die bundeseigene Verwaltung und die Bundesauftragsverwaltung erlassen. Nun liegt der Schwerpunkt der Verwaltungstätigkeit in Deutschland bei der landeseigenen Ausführung von Bundesgesetzen. Es wäre daher wünschenswert, ein zustimmungsbedürftiges Gesetz zu schaffen, das auch für den Vollzug von Bundesrecht als eigene Angelegenheit der Länder gilt. Darüber hinaus sollte eine Simultangesetzgebung von Bund und Ländern erwogen werden. Damit könnte man einheitliche Informationszugangsrechte auch für den Vollzug von Landesrecht schaffen. Selbst wenn sich dies jedoch nicht verwirklichen lassen sollte, hätte ein Informationsfreiheitsgesetz des Bundes zumindest Modellcharakter für die Länder. Ein Gleichklang zwischen Landes- und Bundesrecht ist aus Gründen der Rechtsvereinfachung – wie bei den Verwaltungsverfahrensgesetzen – erstrebenswert, nicht aber zwingend erforderlich.

Zum jetzigen Zeitpunkt empfiehlt es sich meiner Meinung nach – jedenfalls im Moment – nicht, das Datenschutzrecht in ein Informationsgesetz zu integrieren, wie dies auf dem 62. Deutschen Juristentag im letzten Jahr unter dem Stichwort „Informationsgesetzbuch“ diskutiert wurde. Das BDSG betrifft, anders als es bei einem Informationsfreiheitsgesetz der Fall wäre, nicht nur den öffentlichen Bereich. Zudem würde das Gesetzgebungsverfahren unnötig belastet, wenn beide Materien miteinander verknüpft würden. Das BDSG wird zur Zeit mit dem Ziel novelliert, die EU-Datenschutzrichtlinie umzusetzen. Der Abstimmungsprozeß zwischen den Beteiligten hat sich wegen der Komplexität der Materie als sehr langwierig und kompliziert erwiesen. Die fällige "große" Revision des Datenschutzrechts steht ohnehin noch aus. Die praktischen Erfahrungen zeigen, daß das BDSG wegen seiner Struktur nicht gerade anwenderfreundlich und fast nur noch für Experten beherrschbar ist. Daher soll noch in dieser Legislaturperiode eine umfassende Neukonzeption des BDSG erarbeitet werden, die das Gesetz modernisiert, vereinfacht und in seiner Lesbarkeit erhöht.

Die aktuellen Probleme im Datenschutzrecht würden verstärkt, wenn man das BDSG mit dem geplanten Informationsfreiheitsgesetz zusammenführen würde. Längerfristig könnte allerdings erwogen werden, ein Informationsgesetzbuch als übergreifende, rechtsbereinigende und harmonisierende Kodifikation des Informationsrechts des

Bundes zu konzipieren. Einerseits stehen Informationszugangsrechte und Datenschutzrechte in einem Spannungsverhältnis zueinander. Durch einen uneingeschränkten Informationszugang zugunsten des einen Bürgers können die Datenschutzrechte eines anderen Bürgers verletzt werden. Informationszugangsrechte und Datenschutzrechte sind andererseits aber auch zwei Seiten derselben Medaille. Denn um seine Daten aktiv schützen zu können, muß sich der Bürger über diese Daten informieren. Das Recht auf informationelle Selbstbestimmung hat nicht nur eine Abwehrfunktion, sondern dient auch der Kommunikations- und Handlungsfähigkeit. In Brandenburg und Berlin hat man dem Zusammenhang zwischen Informationszugang und Datenschutz dadurch Rechnung getragen, daß die Aufgabe des neu bestellten "Beauftragten für das Recht auf Akteneinsicht" in Personalunion vom Landesbeauftragten für den Datenschutz wahrgenommen wird.

Bereits jetzt müssen die informationstechnischen Entwicklungen berücksichtigt werden. Mit der Entwicklung neuer Informations- und Kommunikationsdienste kommen auf den öffentlichen Dienst ohnehin weitere Anforderungen zu. In zunehmendem Maße müssen Behörden elektronische Verwaltungsdienstleistungen erbringen, sei es durch aktive, sei es durch passive Informationspolitik. Daher muß geprüft werden, ob der Informationszugang mittels neuer Medien wie des Internets einen selbständigen Regelungsbedarf begründet.

## **Probleme**

Da ein Informationsfreiheitsgesetz ein Novum im deutschen Verwaltungsrecht wäre, ist es nur natürlich, daß wir uns im Vorfeld mit Einwänden und Befürchtungen verschiedenster Art auseinandersetzen müssen. Teilweise werden sogar verfassungsrechtliche Zweifel daran geäußert, ob ein Informationsfreiheitsgesetz mit dem Gewaltenteilungsgrundsatz und dem Repräsentativsystem vereinbar ist. Diese Bedenken teile ich nicht. Eine rechtsvergleichende Betrachtung zeigt, daß allgemeine Informationszugangsgesetze auch und gerade in den Staaten existieren, die die gleichen Verfassungsprinzipien haben.

Auch traditionelle Rechtsprinzipien wie die Amtsverschwiegenheit und das Berufs-, Steuer-, Sozial-, Statistik-, Adoptionsgeheimnis werden ebenso wie in anderen Staaten nicht gefährdet sein. Ihnen kann durch Ausnahmetatbestände Rechnung getragen werden.

Weniger rechtlicher als verwaltungspraktischer Natur ist die Befürchtung, mit einem Informationsfreiheitsgesetz sei ein erheblicher Verwaltungs- und Kostenmehraufwand verbunden. Damit dürfte aber die Neugierde der Bürger überschätzt werden. Meines Wissens haben sich jedenfalls in Brandenburg entsprechende Befürchtungen bisher nicht bestätigt. Es ist allerdings damit zu rechnen, daß die Bewohner von Großstädten wie Berlin ihre Informationsrechte in einem höheren Maße in Anspruch nehmen werden. Die Gefahr, daß die Behörden "Aktenhygiene" betreiben und die wirklich interessanten Informationen nur noch in unzugänglichen Handakten aufbewahren, läßt sich durch verwaltungsorganisatorische Maßnahmen bannen.

Grundsätzliche Probleme bei der Schaffung eines Informationsfreiheitsgesetzes gibt es daher nach meiner Auffassung nicht. Richtig ist allerdings, daß die Einzelheiten eines solchen Gesetzes vertiefter Prüfung bedürfen. Hierzu kann man auf die Regelungen in anderen Staaten zurückgreifen. Auch das brandenburgische AIG und demnächst das Berliner Informationsfreiheitsgesetz liefern natürlich Hilfestellungen. Um Ihnen einen Eindruck des gegenwärtigen Diskussionsstandes zu vermitteln, möchte ich Ihnen einige Beispiele für Detailprobleme geben.

- So ist klärungsbedürftig, ob das Informationszugangsrecht als Bürgerrecht oder als Jedermannsrecht, als Individual- oder auch als Verbandsrecht gewährt werden soll.
- Auch der Adressatenkreis, also die Frage, welche Behörden zur Informationserteilung verpflichtet sind, muß sorgfältig geprüft werden. Sollen es nur Exekutivbehörden der unmittelbaren und eventuell der mittelbaren Staatsverwaltung sein oder auch Parlamente und Justizbehörden?

- Dann muß das Verhältnis zu den Spezialgesetzen geklärt werden, insbesondere die Frage, ob sie auch dann bestehen bleiben sollen, wenn sie den Informationszugang an bestimmte, enge Voraussetzungen knüpfen. Klargestellt werden muß ferner das Verhältnis zu den Archivgesetzen – Informationen, die vor ihrer Archivierung zugänglich waren, sollten es auch danach bleiben.
- Ebenfalls von Bedeutung ist der Begriff der zugänglich zu machen den Daten. So ist fraglich, ob auch vorbereitende Dokumente wie Entwürfe und Notizen zugänglich gemacht werden sollen. Dagegen spricht, daß etwaige behördeninterne Meinungsunterschiede, Willensbildungsprozesse und unter Umständen auch sachlich falsche Informationen an die Öffentlichkeit gelangen würden. Damit könnten nicht nur persönliche Interessen der Bearbeiter verletzt werden; auch die Öffentlichkeit könnte durch Desinformation in die Irre geführt werden. Außerdem könnte der behördliche Entscheidungsprozeß durch Zugänglichmachen vorbereitender Dokumente in den Fällen beeinflußt oder gestört werden, in denen ein Verwaltungsverfahren noch nicht abgeschlossen ist.
- Weiterer zentraler Punkt ist die Gestaltung der Ausnahmetatbestände. Sie sind denkbar sowohl in Form von Generalklauseln als auch in Form erschöpfender Ausnahmetatbestände. Damit zusammen hängt die Frage, für welche Bereiche Ausnahmetatbestände geschaffen werden müssen. Selbstverständlich ist, daß dazu der Datenschutz, der Schutz von Berufs- und Amtsgeheimnissen sowie der Schutz staatlicher Güter wie Landesverteidigung, Schutz der Strafverfolgung und Rechtsdurchsetzung, Gemeinwohlinteressen und Umweltschutz gehören. Aber sollen auch Informationen geschützt werden, die vertraulich übermittelt wurden oder die aus laufenden (Verwaltungs-) Verfahren stammen? Und wann ist ein Verfahren überhaupt abgeschlossen?
- Von Brisanz ist die Frage, ob Informationen kostenfrei oder nur gegen Kosten- oder Auslagenerstattung zugänglich gemacht werden sollen. Sie wissen vielleicht, daß die EU-Kommission gegen die Bundesrepublik ein Vertragsverletzungsverfahren beim Europäischen Gerichtshof anhängig gemacht hatte, in dem sie die mangelhafte Umsetzung einer EU-Richtlinie durch das Umweltinformationsgesetz rügte. Diese Klage betraf vor allem die Kosten-

regelung im UIG. In seinem vor wenigen Wochen erlassenen Urteil hat der EuGH diese Kostenregelung nicht für generell unvereinbar mit EU-Recht erklärt. Er hat aber entsprechend dem Wortlaut der Richtlinie festgestellt, daß die Gebühren angemessen sein müssen und nicht das Recht auf freien Zugang zu Umweltinformationen faktisch beschränken dürfen. Vollständig kostendeckende Gebühren seien daher nicht zulässig. Auch müsse die Erhebung von Gebühren auf die Fälle beschränkt werden, in denen tatsächlich eine Übermittlung von Informationen stattgefunden habe. Sie sei daher unzulässig, wenn ein Antrag auf Informationszugang von der Behörde abgelehnt werde.

Nun müssen bei der Konzeption eines allgemeinen Informationsfreiheitsgesetzes anders als beim Umweltinformationsgesetz (noch) keine verbindlichen europarechtlichen Vorgaben berücksichtigt werden. Und davon abgesehen dient der Zugang zu amtlichen Informationen im Umweltrecht in besonderem Maße dem öffentlichen Interesse, ein Aspekt, der in anderen Bereichen nicht generell durchgreift. Gleichwohl sollte auch dort zumindest geprüft werden, ob bereits bei Ablehnung eines Antrags Kosten erhoben werden sollten.

- Neben den genannten materiellen Gesichtspunkten muß über verfahrensrechtliche Fragen nachgedacht werden. Dies betrifft vor allem Regelungen des Verwaltungsverfahrens zu Fristen, zur Beteiligung Dritter u.ä. Von Bedeutung ist auch die prozessuale Problematik, wie es dem Gericht im Falle einer gerichtlichen Auseinandersetzung ermöglicht werden kann, das Vorliegen eines Geheimhaltungstatbestandes zu prüfen – und zwar ohne daß der auf Informationszugang klagende Bürger schon vor Erlaß des Urteils die begehrten Informationen aufgrund des gerichtlichen Akteneinsichtsrechts erhält.
- Weitere Probleme wie das Verwertungs- und Kommerzialisierungsproblem, das Erstellen von Informationsverzeichnissen und die Einrichtung eines Beauftragten für Informationsfreiheit will ich - abschließend - nur am Rande erwähnen.

Sie sehen, daß es vor der Umsetzung des geplanten Informationsfreiheitsgesetzes noch vielfältigen Klärungsbedarf gibt, sowohl in

juristischer als auch in rechtspolitischer Hinsicht. Trotzdem bin ich zuversichtlich, daß dieses Gesetz noch in dieser Legislaturperiode verwirklicht werden kann.

**Prof. Dr. Shizuo Fujiwara**  
Kokugakuin University, Tokyo

## **Das neue japanische Informationszugangsgesetz**

Zunächst möchte ich kurz die Position der Informationszugangsregelungen im Rechtssystem und die Politik der Information der Öffentlichkeit referieren. Danach werde ich auf das neue japanische Akteneinsichts- und Informationszugangsgesetz eingehen und mit einem Resümee bzw. Ausblick enden.

### **I. Das Datenschutzrecht, Akteneinsichts- und Informationszugangsgesetz unterscheidet sich wie auch das Verwaltungsverfahrensgesetz grundlegend von dem materiell-rechtlichen Gedanken in Japan und Deutschland.**

Diese drei Regelungen haben nämlich gemeinsam, dass sie die bisherige Verwaltungsauffassung verändern, dabei haben diese drei Regelungen verschiedene verfassungsrechtliche Grundlagen, unterschiedliche Rahmen und Einschränkungen. Im Vergleich zu anderen haben diese drei relativ jungen Rechtsregelungen neue oder fremde Elemente: sie sind transparent, offen im Zugang und bieten die Möglichkeit der Selbstbestimmung und Kommunikation durch Gemeinbesitz von Informationen.

Die vergleichende Untersuchung über diese drei Rechtsregelungen, wie zum Beispiel der Vergleich zwischen Akteneinsichts- und Informationszugangsgesetz und dem Verwaltungsverfahrensgesetz ist sehr interessant. Aber da ich aus Zeitgründen hier nicht auf Einzelheiten dieses Problems eingehen kann, möchte ich nur auf zwei Punkte hinweisen.

Erstens, jede dieser drei Rechtsregelungen hat sich in allen Ländern unterschiedlich entwickelt. Zum Beispiel wurde in Deutschland das Datenschutzgesetz und das Verwaltungsverfahrensgesetz fast gleichzeitig erlassen. Aber es gibt kein Akteneinsichts- und Informationszugangsgesetz auf der Bundesebene, das jedermann den Zugang zu für die Allgemeinheit wichtigen Informationen eröffnet. Al-

lerdings hat Brandenburg kürzlich ein solches Gesetz erlassen. Und man legt allgemein in Deutschland großes Gewicht auf den Datenschutz.

In den U.S.A. scheint es so, dass der Informationszugang den Vorrang vor allem anderen hat.

In Kanada ist, meiner Ansicht nach, das Verhältnis zwischen Datenschutz und Informationszugang ausbalanciert.

In Japan war zuerst das Datenschutzgesetz, und danach kam eine städtische Anordnung zum Thema Informationszugang. Als letztes kam das Verwaltungsverfahrensgesetz<sup>1</sup>. Obwohl ein Akteneinsichts- und Informationszugangsgesetz erst unlängst verabschiedet wurde, hat sich der Gedanke vom Informationszugangsrecht des Bürgers durch die städtische Anordnung gut entwickelt.

Aber das japanische Datenschutzgesetz gehört zur alten Generation, denn es fehlt ihm an Regelungen über den nicht öffentlichen Bereich und nicht automatisierte Dateien. Gerade jetzt hat die japanische Regierung mit den Änderungsarbeiten begonnen.

Zweitens: man sagt oft, dass Datenschutz und Informationszugang zwei Seiten einer Medaille sind<sup>2</sup>. Aber genauer gesagt, ist diese Metapher nicht ganz korrekt. Denn der Datenschutz betrifft unmittelbar den nicht öffentlichen Sektor. Im Gegensatz dazu liegt der Kernpunkt des Informationszugangs darin, dass er den Anspruch des Bürgers gegen die öffentliche Gewalt gewährleistet. Hier ist die Größe der Vorderseite und die der Rückseite verschieden.

## **II. Die Politik der Information der Öffentlichkeit**

Wenn man an die Information der Öffentlichkeit denkt, kann man dies mit sehr unterschiedlichen Formen oder Modellen verbinden. Eine erinnert an den Freedom of Information Act in den USA, eine andere begreift dies nicht als Auskunftsanspruch, also als subjektiv-öffentli-

---

<sup>1</sup> Das Datenschutzgesetz trat am 1. Oktober 1989 und das Verwaltungsverfahrensgesetz am 1. Oktober 1994 in Kraft.

<sup>2</sup> Siehe dazu Bericht von Sokol in diesem Dokument.

ches Recht, sondern interpretiert dies lediglich als einen Anspruch auf fehlerfreie Ermessensausübung. Darüber hinaus kann man die Informationspolitik auch so verstehen, dass Verwaltungsorgane nur in bestimmten Fällen, in denen Leben oder Gesundheit u.s.w. von Menschen betroffen sind, zur Veröffentlichung von Dateninformationen verpflichtet sind.

Ich möchte diese Modelle schlagwortartig wie folgt umschreiben:

- freiwillige Informationserteilungspolitik der Verwaltung
- Anspruch der Bürger auf freien Zugang zu Verwaltungsinformationen
- Verpflichtung der Verwaltung zur Informationserteilung ohne Antrag des Bürgers

Hier muss man die Tatsache berücksichtigen, dass, je umfangreicher die freiwillige Informationserteilungspolitik der Verwaltung wird, desto geringer der Anspruch der Bürger auf freien Zugang zu Verwaltungsinformationen wird.

Im folgenden möchte ich hauptsächlich darlegen, inwieweit der Anspruch der Bürger auf freien Zugang zu Verwaltungsinformationen im japanischen Akteneinsichts- und Informationszugangsgesetz verwirklicht ist.

### **III. Das neue japanische Akteneinsichts- und Informationszugangsgesetz**

1. Normen, die das Recht auf Einsicht in die bei den Verwaltungsorganen vorliegenden Daten jedermann unabhängig von seinem Motiv zubilligen, bestehen schon seit 1982.

Im Jahre 1982 war es Kanagawa, die als erste Präfektur eine städtische Anordnung zum Thema Informationszugang beschlossen hat. Dabei hat man sich eng an den amerikanischen Freedom of Information Act angelehnt. Seitdem erließen andere kommunale Körperschaften ähnliche Anordnungen nach dem Vorbild Kanagawas. Zum

Stand vom 1.4.1999 haben 894 kommunale Körperschaften städtische Anordnungen erlassen - bei einer Gesamtzahl von ca. 3300 kommunalen Körperschaften in Japan. Mittlerweile haben alle 47 Präfekturen und alle 12 großen Städte, die durch Kabinettsverordnung besondere Befugnisse erhalten haben, und viele Gemeinden ähnliche städtische Anordnungen verfügt.

Und diese 17jährige Erfahrung auf der lokalen Ebene war eine der Triebkräfte für die Gesetzesinitiative der japanischen Regierung.

2. Bereits im Jahre 1974 wurde auch auf der staatlichen Ebene ein derartiges Gesetz für erforderlich gehalten. Dies geschah aus Anlass der sog. Lockheed-Affäre, in der es um die Aufklärung der rechtswidrigen Amtsführung des damaligen Premierministers ging. Aber tatsächlich ist das Informationszugangsgesetz erst in den letzten fünf Jahren nach der Bildung der Koalitionsregierung intensiv erarbeitet worden. In diesem Sinn kann man nicht zu unrecht sagen, dass das Gesetz dem Machtwechsel der Regierung zu verdanken ist<sup>3</sup>.

Der Erlass des Informationszugangsgesetzes ist als ein Glied in der Kette der Verwaltungsreform in Japan zu sehen. Deshalb hat das Verwaltungsreformkomitee ein spezielles Gremium<sup>4</sup> eingerichtet. Dort wurde der Entwurf des Gesetzes im wesentlichen verfasst. Ende 1996 wurde dieser Entwurf fast unverändert von der Regierung ins Parlament eingebracht. Nachdem der Entwurf dreimal im Parlament vorgelegt wurde und diskutiert worden war, hat das Parlament das Gesetz am 7. Mai 1999 verabschiedet. Es tritt Anfang 2001 in Kraft.

3. Das Gesetz enthält folgende Kernpunkte:

1) Zweck des Gesetzes

- (1) Das Gesetz beruht auf dem verfassungsrechtlichen Prinzip, dass die Staatsgewalt von Volk ausgeht (Souverän)
- (2) Das Gesetz verleiht den Bürger einen Rechtsanspruch auf

---

<sup>3</sup> Auf lange Sicht haben auch Bürgerinitiativen eine bestimmte Rolle gespielt.

<sup>4</sup> Der Verfasser war ein Mitglied dieses Gremiums. In diesem Gremium wurden sowohl die Erfahrungen auf der lokalen Ebene in Japan berücksichtigt als auch gesetzlichen und rechtlichen Zustände fast aller Länder untersucht, die ein Akteneinsichts- und Informationszugangsgesetz einschließlich eines Umweltinformationsgesetzes haben.

Veröffentlichung der Verwaltungsunterlagen.

- (3) Das Gesetz soll sicherstellen, dass die bei den Verwaltungsorganen vorhandenen Informationen veröffentlicht werden. Damit soll es dazu beitragen, dass die Regierung ihrer Rechenschaftspflicht (accountability) nachkommt und die Verwaltung zu einer gerechten und demokratischen Amtsführung angehalten wird.

Hier ist die Tatsache bemerkenswert, dass der Begriff accountability (also "Rechenschaftspflicht") statt des "Rechts auf Wissen" (Right to know) benutzt wird. Dieser Begriff accountability ist das Schlüsselwort für die Legitimität der Informationszugangsgesetze in den verschiedenen Ländern<sup>5</sup>.

Der Begriff von Recht auf Wissen wird in der Zweckbestimmung nicht vorgeschrieben, weil die Meinungen über ihr Ausmaß und ihre verfassungsrechtliche Grundlage sich noch widersprechen.

2) Jeder hat Anspruch auf Information, und zwar unabhängig von Nationalität oder Wohnsitz. Ich denke, dass dieser Gedanke vom Jedermannsrecht für Deutsche immer noch fremd ist, die mit einem vollkommenen Rechtssystem des subjektiv-öffentlichen Rechts vertraut sind. Diese Tatsache dürfte ein Grund dafür sein, dass es in Deutschland bisher noch kein solches Gesetz gibt.

3) Alle Verwaltungsorgane sind auskunftspflichtig. Die oberste Polizeibehörde, das Verteidigungsministerium und das Auswärtige Amt sind in gleicher Weise verpflichtet. Allerdings gelten hier andere Ausnahmetatbestände als bei den allgemeinen Verwaltungsbehörden. Bei Informationen über die öffentliche Sicherheit oder Internationale Beziehungen u.s.w. kann das Gericht im Verwaltungsprozessverfahren nicht de novo prüfen, ob die Erteilung oder Einsicht der gewünschten Informationen die Schutzgüter des Ausnahmetatbestandes gefährden würde, sondern nur prüfen, ob die Beurteilung der Obersten Behörde rechtswidrig ist. Hier gibt es eine unterschiedliche Kontrolldichte zwischen solchen Informationen und den allgemeinen Informationen. Mit anderen Worten kann man sagen, dass hier die

---

<sup>5</sup> So etwa in den USA, in Kanada und Australien. Siehe dazu Riley, Accountability of Government: an international perspective, Freedom of Information Review 1987, S. 54.

Balance zwischen dem Geheimhaltungsinteresse der Verwaltung und dem Informationszugang gehalten wird.

4) Der Gegenstand des Informationsanspruchs sind öffentliche Akten. Nach dem Gesetz fallen darunter:

- (1) Akten, zeichnerische Darstellungen und elektromagnetische Dokumente, die von den Beamten oder Angestellten dienstlich angefertigt bzw. erlangt und
- (2) die von den betreffenden Verwaltungsorganen aufbewahrt werden, damit sie dienstlich und organisatorisch benutzt werden können.

Deshalb sind zum Beispiel die persönlichen Notizen eines Beamten zu einer bestimmten Angelegenheit grundsätzlich nicht zu den öffentlichen Akten zu rechnen. Akten, die gerade Bestandteil eines laufenden Verfahrens sind, sind nicht unbedingt von der Veröffentlichung ausgeschlossen, sondern erst dann, wenn einer der Ausnahmetatbestände erfüllt ist.

5) Obwohl das Informationszugangsgesetz die Gerechtigkeit und die Transparenz der Verwaltungsführung fördern soll, dürfen andere schutzwürdige Interessen von diesem System nicht einseitig beeinträchtigt werden. Folglich besteht die Notwendigkeit einer Grenzziehung zwischen den zu veröffentlichenden Informationen und solchen, die vertraulich bleiben müssen. Das Gesetz normiert 6 Ausnahmetatbestände bzw. Ausschlussgründe.

Die 6 Ausnahmetatbestände sind:

- (1) personenbezogene Informationen,
- (2) juristisch-personenbezogene Informationen,
- (3) Informationen, die die Sicherheit des Staates, oder seine Beziehungen zu anderen Ländern und internationalen Organisationen betreffen,
- (4) Informationen, die den Schutz der öffentlichen Sicherheit tangieren,
- (5) Informationen, die Bestandteil von Beratungen und Besprechungen innerhalb der staatlichen Organe oder zwischen staatlichen und lokalen Organen sind,

- (6) Informationen, die sich auf die Amtsführung der staatlichen und lokalen Verwaltungsorgane beziehen.

Hier will ich nur die personenbezogenen Informationen und die juristisch-personenbezogenen Informationen erwähnen.

Die personenbezogenen Informationen haben die gleiche Bedeutung, wie sie im Datenschutzrecht benutzt werden. Die Bestimmbarkeit einer Person ist der springende Punkt. Während des Gesetzgebungsprozesses wurde ein anderes Modell untersucht. Das ist nämlich die Möglichkeit der Annahme des Begriffs "Privatsphäre (Privacy)". Aber die mit der Gesetzgebung Befassten befürchteten, dass die Privatsphäre der Bürger gerade durch die Annahme des Begriffs Privatsphäre einer Gefahr ausgesetzt wird. Denn die Beurteilung, was Privatsphäre ist, ist schwieriger als die, welche Angaben die betreffende Person bestimmbar machen. Die Aufnahme des Bestimmbarkeitsmodells in das Gesetz ist für den Datenschutz günstiger<sup>6</sup>.

Nach § 5 Nr. 2 des Gesetzes wird der Anspruch auf Informationen eingeschränkt, wenn deren Bekanntgabe das Recht des betreffenden Unternehmens, die Wettbewerbsfähigkeit und sonstige berechnete Interessen des Unternehmens gefährdet.

Und auch die Informationen, die Verwaltungsorganen unter der Bedingung der Geheimhaltung zur Verfügung gestellt werden, dürfen nicht veröffentlicht werden, wenn die Bedingung nachvollziehbar und einsehbar ist.

Allerdings können solche Informationen veröffentlicht werden, deren öffentliche Bekanntgabe zum Zweck des Schutzes des Lebens, der Gesundheit und des Vermögens als erforderlich betrachtet werden.

Hier möchte ich nur über sog. "freiwillig offengelegte Informationen" reden. In bezug auf diesen Streitpunkt sind zwei amerikanische Urteile bekannt: es sind diese das National Parks oder das Morton

---

<sup>6</sup> Allerdings gilt für Amtsträgern eine Sonderregelung. Die persönliche Daten von Amtsträgern, wie Name, Funktion, können erteilt werden, wenn diese in ihrer amtlichen Funktion betroffen würden.

Urteil<sup>7</sup> und das Critical Mass Urteil<sup>8</sup>. In Japan ist der Gesetzestext über die Geheimhaltung von den freiwillig offengelegten Informationen an sich als Folge der langen und heftigen Diskussionen ein wenig strenger als der Maßstab des Critical Mass Urteils geworden.

Als letzten besonderen Ausnahmetatbestand möchte ich eine neue Kategorie nennen. Das sind die Informationen, die nicht mit "Ja" oder "Nein" beantwortet werden dürfen. Anders ausgedrückt, es gibt Informationen, von deren Existenz oder Nichtexistenz nicht gesprochen werden darf.

Diese Kategorie stammt aus den sog "Glomar denials"<sup>9</sup>, die sich in der Praxis des FOIA entwickelt haben. Obwohl man von den "Glomar denials" hauptsächlich beim Thema Staatssicherheit spricht, gibt es ähnliche Situationen in anderen Bereichen. Zum Beispiel kann eine Krankenkarte einer Person, die in einem Fachkrankenhaus gelegen hatte, in das Zugangs- und Informationsrecht des Bürgers mit einbezogen werden können.

Das japanische Akteneinsichts- und Informationszugangsgesetz schreibt diesen Tatbestand als § 8 vor: wenn nur die Beantwortung, ob die gewünschte Aktenexistenz oder Nichtexistenz dazu führen würde, dass die durch die Ausnahmetatbestände geschützten Informationen erteilt würden, kann der Leiter eines Verwaltungsorgans diesen Antrag ablehnen. Natürlich ist diese Ablehnung als ein Verwaltungsakt zu betrachten und anfechtbar. Hier hätte der Gesetzgeber noch eine andere Möglichkeit gehabt, die in Japan nicht umgesetzt wurde. Er könnte nämlich einwilligen, dass ein zuständiger Beamter immer mit "Nein" antworten dürfe.

6) Das Gesetz schreibt auch eine Sonderregelung bei umfangreichen Akten bzw. komplexen Rechtsangelegenheiten vor. Der Bescheid über ein Informationsanspruchs ist grundsätzlich innerhalb von 30 Tagen nach dem Antrag zu erlassen und gegebenenfalls

---

<sup>7</sup> National Parks and Conservation Association v. Morton, 498 F.2d 765(D.C.Cir. 1974).

<sup>8</sup> Critical Mass Energy Projekt v. NRC, 975 F.2d 871 ( D.C. Cir. 1992), cert. Denied, 507 U. S. 984(1993); FOIA Update, Spring 1993, at 1.

<sup>9</sup> Phillippi v. CIA, 546 F.2d 1009 ( D.C. Cir 1976). Glomar ist der eines Rettungsschiffes, das spezielle nach einen Atom-U-Boot sucht. Die Antwort, ob das Schiff läuft aus, ist die Antwort dafür, ob ein Atom-U-Boot sinkt.

kann diese Frist noch um 30 Tage verlängert werden, wenn es einen berechtigten Grund gibt (§10 des Gesetzes). Das ist die Allgemeinregelung. Aber nach den Erfahrungen mit den Städtischen Anordnungen auf der lokalen Ebene hat die Tatsache, dass mitunter einzelne Bürger immer wieder Auskunftsansprüche<sup>10</sup> erhoben und damit die Verwaltungsarbeit blockierten die Aufmerksamkeit des Gremiums erregt. Es ist sehr schwer, fristgerecht eine Sache zu erledigen, wenn die Akten zum Beispiel sehr umfangreich sind oder der Beamte in verschiedenen Akten einen Anspruch bearbeiten muss. Besonders viel Zeit kostet es, wenn der Verwaltungsbeamte zur Teilbekanntgabe viele Textstellen unkenntlich machen muss. In diesen Fällen ist der Leiter eines Verwaltungsorgans nur verpflichtet, innerhalb von 60 Tagen über die wesentlichen oder bedeutenden Teile der Akte einen Bescheid zu erlassen. Über die restlichen Teile muss er den Bescheid in angemessener Frist erteilen, wenn die Akten umfangreich sind und die Ausführung der Routinenangelegenheiten der zuständigen Behörde erheblich beeinträchtigt würde.

In diesem Fall hat der Leiter selbstverständlich die Gründe und den Termin des zweiten Bescheids schriftlich mitzuteilen. Hier rechnet der Gesetzgeber damit, dass ein Kompromiss mit dem Antragsteller nach dem ersten Bescheid eingegangen wird.

7) Auch über die Gebühren gab es heiße Diskussionen. Diese schließlich führten dazu, dass Gebühren erhoben werden, die nicht abschreckend wirken, sondern benutzerfreundlich sind. Deshalb werden die Gebühren sehr niedrig gehalten. Bei Anträgen, die mit der Erfüllung eines öffentlichen Interesses begründet werden, ist die Herabsetzung der Gebühren oder eine Befreiung<sup>11</sup> nicht eingeführt worden, weil der Inhalt des öffentlichen Interesses nur schwer festgelegt werden kann. Was diese Gebühren betrifft, müssen wir erst das Ausmaß der kommerziellen Nutzung abwarten.

8) Als Rechtsmittel hat das Gesetz ein neues Komitee, das aus 3 Senaten besteht, eingerichtet. Jeder der Senate hat 3 Mitglieder und in bestimmten Fällen sind alle 9 Mitglieder als ein Kollegialkomitee tätig. Wenn ein Verwaltungsorgan in der Frage des Informations-

---

<sup>10</sup> Diese Auskunftsansprüche an sich sind nicht immer die Rechtsmissbrauch.

<sup>11</sup> Ähnliche Systeme sind in den USA, in Kanada und Australien gesetzlich geregelt.

anspruchs einen negativen Bescheid gibt und der Betroffene sich darüber beschwert, dann muss das Verwaltungsorgan grundsätzlich das Komitee zu diesem Widerspruch befragen. Das Komitee untersucht den Fall, berät ihn und erstattet ein Gutachten.

Ich möchte die Tatsache betonen, dass das Komitee die Befugnis zur sog. "In-Camera-Inspektion"<sup>12</sup> hat, um seine Aufgabe effektiv wahrzunehmen. In diesem Verfahren hat das Komitee ein Einsichtsrecht in jene Akten, deren Offenlegung gerade verweigert wurde. Auf der anderen Seite darf der Bürger selbst die Akten nicht einsehen. Die „In-Camera-Inspektion“ wird in den USA und in Kanada vom Gericht angeordnet. Wie Sie wissen, wird in Deutschland und auch in Japan über die Einführung dieses Systems im Zusammenhang mit dem Grundsatz der Öffentlichkeit der Verhandlung heftig diskutiert. Deshalb hat das japanische Gesetz das System im Widerspruchsverfahren angesiedelt und ein spezielles Komitee mit der Aufgabe betraut.

Selbstverständlich haben wir den "Vaughn Index"<sup>13</sup> angenommen, damit die "In-Camera-Inspektion" gut und effektiv funktioniert.

---

<sup>12</sup> Vgl. Gurliit, Die Verwaltungsöffentlichkeit im Umweltrecht, 1989; Mengel, Akteneinsicht in Verwaltungsverfahren, DV 1990, S. 377; Ziekow, Die Pflicht der Behörde zur Gewährung von Informationen an die Verwaltungsgerichte, BayVBl. 1992, S. 132; Blumenberg, Die Umwelt-Informations-Richtlinie der EG und ihre Umsetzung in das deutsche Recht, Natur und Recht 1992, S. 8; Engel, Der freie Zugang zu Umweltinformationen nach der Informationsrichtlinie der EG und der Schutz von Rechten Dritter, NVwZ 1992, S. 111; Cosack/Tomerius, Betrieblicher Geheimnisschutz und Interesse des Bürgers an Umweltinformationen bei der Aktenvorlage im Verwaltungsprozeß, NVwZ 1993, S. 841; Theuer, Der Zugang zu Umweltinformationen aufgrund des Umweltinformationsgesetzes (UIG), 1995; Kollmer, Klage auf Umweltinformation nach dem neuen Umweltinformationsgesetz (UIG), NVwZ 1995, S. 858; Sokol, Datenschutz versus Informationszugang?, DuD 1997, S. 380.

<sup>13</sup> Allerdings ist die Tatsache zu berücksichtigen, dass in den USA der sog. "Vaughn-Index" eine große praktische Rolle spielt. Erfahrungsgemäß funktioniert die "In-Camera-Verfahren" erst dann gut, wenn dabei der "Vaughn Index" beachtet wird. Der "Vaughn Index", benannt nach dem Namen eines Klägers, ist ein Beweismittel, das in der amerikanischen Rechtsprechung (Vaughn v. Rosen, 484 F.2d 820; D.C. Cir.1973) festgelegt worden ist. Dieser Index ist ein sehr flexibles Mittel, da er keine bestimmte Formel hat. Üblicherweise hat er folgenden Inhalt: Verwaltungsorgane stellen einen Index auf und legen ihn dem Gericht vor. Der Index enthält eine Beschreibung der Kategorien der Informationen, die sie nicht bekanntgeben wollen, und der Ausnahmetatbestände sowie die Begründung dafür. Es hängt von der Natur der betreffenden Information und des jeweiligen Ausnahmetatbestandes ab, wie ausführlich Verwaltungsorgane einen Index beschreiben müssen.

Ich würde noch einige Anmerkungen zur Arbeit des Komitees machen. Dieses Komitee wurde aufgrund der Erfahrungen mit den städtischen Anordnungen auf der lokalen Ebene gegründet. Die Tätigkeit des Komitees wird wegen seiner Neutralität relativ hoch geschätzt. Bei seiner Prüfungstätigkeit stößt das Komitee häufig auf die Behauptung der Verwaltung, bei den Informationen handele es sich um einen Willensgestaltungsprozesses der Verwaltung. Diese erfüllten den Ausnahmetatbestand. Diese Begründung wird vom Komitee jedoch nicht ohne weiteres akzeptiert, sondern vielfach erst dann, wenn die Verwaltung sehr konkret den Beweis führt, dass die Preisgabe der Informationen den Willensgestaltungsprozesses der Verwaltung gefährden würde. In vielen Fällen trifft das Komitee Entscheidungen zugunsten des Bürgers.

Obwohl ein Gutachten des Komitees nicht rechtsverbindlich ist, ist die Verwaltung bisher den Gutachten in fast 100% der Fälle gefolgt. Diese Tatsache hat auch der aktuelle Gesetzgeber im Sinn gehabt.

#### **IV. Resümee und Ausblick**

Das Informationszugangsgesetz bildet den Schwerpunkt der Verwaltungsreform in Japan. Der eigentliche Sinn und Zweck dieses Gesetzes ist der "informierte Bürger" (Informed Citizenry) und die Klarstellung, dass die Verwaltung ihrer Rechenschaftspflicht (accountability) nachkommen muss.

Denn die Bürger können an einem Entscheidungsprozess oder einem Bürgerentscheid erst dann effektiv teilnehmen, wenn sie über den Gegenstand gut informiert sind und gleichen Zugang zu den relevanten Informationen haben.

Diese Vorstellung wird bestimmt Einfluss auf alle Gebiete der Verwaltung ausüben und eventuell eine Veränderung der Verwaltungspraxis und eine Verwaltungsreform zur Folge haben. Ich bin selbst gespannt, welche Entwicklungen die Zukunft für die Verwaltung bringen wird.



## **Dr. Robert Gallman**

Former Chief Counsel Sub-Committee on Government Information,  
Washington D.C

## **Das Informationsfreiheitsgesetz in den Vereinigten Staaten: Von den Akten bis zum Internet**

The Freedom of Information Act in the United States:  
From Paper Records to the Internet

### **Introduction**

I have been involved with the American Freedom of Information Act (FOIA) for nearly twenty-five years. For most of that time (1977-1994), I served on the staff of the House Committee on Government Operations' Subcommittee on Government Information, Justice, and Agriculture.<sup>1</sup> The Subcommittee had legislative responsibility for FOIA, the Privacy Act of 1974, Government in the Sunshine Act, Federal Advisory Committee Act, and the National Archives and Records Administration. The Subcommittee' broad jurisdiction over federal information policy matters gave it a unique perspective. I will focus my remarks on the FOIA, but other laws and policies that bear on access to government information and on privacy will also be discussed.

### **FOIA Basics**

The FOIA establishes a mechanism that permits any person to request any record in the possession of a federal agency.<sup>2</sup> The FOIA did not become law easily. It took eleven years of hard work before the bill became law in 1966. Political support originally came mostly from journalists, who constantly fought with government agencies over access to documents. It may be surprising to those not familiar with the U.S. governmental structure, but the concerns of journalists resonated with many Members of Congress, who also routinely have

---

<sup>1</sup> The Subcommittee changed its name several times during my tenure.

<sup>2</sup> 5 U.S.C. §552 (1994).

fighters with the executive branch of government over record access. Congressional investigators often must struggle to obtain the information they need to oversee agency activities.

Under the FOIA, not all records must be disclosed in response to a request. Nine exemptions permit the withholding of records to protect legitimate government or private interests. Thus, national security information, trade secrets, law enforcement investigative files, personal data, pre-decisional, and some other records can be withheld.<sup>3</sup>

Any person can make a request under the FOIA. A request by an individual for his or her own file may also be made under the Privacy Act, and the request will be processed under both laws. Because the two laws have different exemptions, information not available under one law may be disclosable under the other. Many other countries have learned from the United States that having completely separate access procedures under privacy and access laws does not make much sense.

I want to highlight five features of the FOIA. First, the Act sought to establish a culture of disclosure for government records. Changing the view of the bureaucracy toward openness was not easy to accomplish, and it took years for this culture to take root. Bureaucrats are not always happy about requirements to disclose information about their activities. Political appointees, who tend to serve in government for only a few years, are often more unhappy about government disclosure policies because the policies do not apply to private companies. However, the FOIA has become part of the standard toolkit for reporters, activists, knowledgeable citizens, and even some elected officials. Government workers are aware of this, and the mere availability of the FOIA sometimes results in voluntary disclosure of information without a formal request.

Second, the FOIA makes government agencies accountable for disclosure decisions. Agencies must consider all requests received under the Act, and they must state a reason when denying access.

---

<sup>3</sup> 5 U.S.C. §552(b). One of the exemptions recognizes other laws that direct the withholding of information, and there may be several hundred of these other laws. For example, specific laws required that census and income tax records be withheld.

The burden of justifying withholding belongs to the agency. Before enactment of the FOIA, disclosures were largely discretionary. An agency could withhold a record arbitrarily and without explanation. This is no longer possible. A decision to withhold can now be appealed to the head of the agency and ultimately to the courts. The courts have been effective in enforcing fair implementation of the law. Third, until the 1995 Electronic FOIA Amendments, the FOIA generally did not require agencies to disseminate records in the absence of a request.<sup>4</sup> The distinction between access and dissemination is a useful one. In this context, *access* refers to the process of making records available in response to a request. Without a request, no records are released. *Dissemination* refers to affirmative publication of information in the absence of a request. The FOIA was conceived of mostly as an access law. It is evolving into a mixed access and dissemination law.

Fourth, the FOIA permits agencies to charge fees for responding to a request. The fee structure is complex, but fees for most users are limited to the cost of searching and copying.<sup>5</sup> In other words, fees cannot exceed the direct cost of providing the records and cannot be based on the market value of the information. The law is not intended to recover all costs of processing, and fee waivers are supposed to be liberally granted. Federal government records cannot be copyrighted,<sup>6</sup> and this is a major limitation on the ability of federal agencies to control disclosure and use of information and to establish high prices for data. Government copyright and access to records laws may be fundamentally incompatible.

Finally, the FOIA became law long before the era of electronic data.

---

<sup>4</sup> Agencies must publish general information about administrative organization, procedures, rules, statements of general policy, and final decisions. See 5 U.S.C. §552(a) (1) & (2) (1988). This is an important requirement, but it covers only a small percentage of agency records.

<sup>5</sup> Fees for representatives of the news media and for educational or noncommercial scientific institutions are limited to copying costs only. Fees for commercial requesters include search, copy, and review costs. All others pay only search and copy costs. All fees can be waived if disclosure of information is in the public interest. 5 U.S.C. §552(a)(4)(A)(ii) & (iii) (1988).

<sup>6</sup> 17 U.S.C. §105 (1994).

The law implicitly assumes that all records are maintained on paper<sup>7</sup>. Since that is no longer true, uncertainties arose over the status of electronic records. The 1995 Electronic FOIA Amendments resolved some, but not all, of these uncertainties. The rapid and continuous evolution of the Internet is one reason information laws always trail behind information technology.

## **History of Implementation**

The original FOIA as enacted in 1966 was somewhat of a failure. Some of the original exemptions, especially for law enforcement records, were too broad. The law did not specify procedures or time limits, and agencies were very slow to respond to requests. Judicial review was limited and mostly ineffective.

The 1974 amendments made the FOIA a truly useful access tool. Once requesters realized that the law worked, the number of FOIA requests increased enormously. Lengthy backlogs developed at many agencies as requests flooded in under the revitalized law. Before the amendments, the Federal Bureau of Investigation received a handful of requests each week. The FBI now receives thousands of requests each year, and its backlog is measured in months and years.

Another consequence of the 1974 amendments was an increase in litigation. The courts took a protective attitude toward the FOIA. They generally interpreted the poorly drafted law to facilitate disclosure in accordance with congressional intent. The role of the courts was crucial in the period following the 1974 Amendments.

The FOIA never included any form of centralized administration, ombudsman, or commissioner. Denials of requests can be appealed to the head of the agency that considered the request. If that administrative appeal is denied, the requester's only recourse is to

---

<sup>7</sup> This is a common unstated assumption in many U.S. laws about records. Records were maintained almost exclusively on paper for 200 years. Laws and programs for archival preservation also tend to be centered around paper records. Some of the archival problems presented by new information technology were explored in a recent congressional report. See Committee on Government Operations, Taking a Byte Out of History: The Archival Preservation of Federal Computer Records, House Report 101-978, 101st Congress, 2d Session (1990).

file a lawsuit in federal court. The courts provide the most important oversight of agency FOIA processing, but few requesters are able to file lawsuits. Still, over the years, we have had thousands of court cases and judicial opinions. American FOIA jurisprudence is extensive.

In 1987, my Subcommittee began an inquiry to see if the users of the FOIA wanted to have an alternative to the courts for hearing appeals or conducting agency oversight. For the most part, people were against anything that would prevent immediate access to the courts.<sup>8</sup> Americans just love litigation. They also are afraid that any administrative process would be subject to the political interests of the current President of the United States. The FOIA community may have opposed a central FOIA office in the mid-1980s partly because the administration of President Ronald Reagan was hostile to the FOIA. America does not have a tradition of independent access or privacy commissioners, although at least one experiments at the state level (Connecticut) has been successful.

The FOIA has been directly amended about every ten years. This is the result of happenstance rather than any formal legislative review process. The law passed in 1966. In 1974, the law was amended. It was amended again in 1986. The modest 1986 amendments were all that remained of an attempt by the Reagan Administration to make the FOIA useless. After a six-year battle, Congress finally agreed to a few changes, lowering fees and slightly broadening exemptions.

The next set of changes did not occur until 1996. The rhetoric accompanying the Electronic FOIA Amendments of 1996<sup>9</sup> suggested that the changes brought the law into the computer age. That sounded nice, but it really was not true. For the most part, agencies and requesters had already adapted to computer technology. As agencies initially made the transition to electronic information, some refused requests for information on computer tapes or disks. Over time, however, as everyone became used to the technology, requesters and agencies usually found a way to work out access procedures for most computer records.

---

<sup>8</sup> *FOIA: Alternate Dispute Resolution Proposals*, Hearings before a Subcommittee of the House Committee on Government Operations, 100th Congress (1987).

<sup>9</sup> Public Law No. 104-231, 110 Stat. 2422 (1996).

Some of the 1996 changes were administrative. The law allows agencies to maintain separate queues for different types of requests. For example, requests for a few pages might be in one queue and requests for many pages in another. Agencies used this type of processing technique before passage of the 1996 amendments.

The new law also recognized that some requests may require faster processing than others, and the law directs agencies to accept requests for expedited processing. Expedited processing was a major demand of press users of the law. After a few years of experience, it is not clear that the expedited processing procedure has made much of a difference. However, no one has done a full study of the effects. The legislative standard for expedition -- "urgency to inform the public concerning actual or alleged Federal Government activity" -- is rather mushy.

In order to accommodate requests for expedited access, the time limits for all requests were lengthened. The 1974 law imposed a ten-day limit for processing requests. While that was unrealistic in many respects, some agencies complied with it. The 1996 amendments changed the time limits to twenty days. Agencies that did not comply with the ten-day limit were not likely to comply with a twenty-day limit. For example, requesters must wait *years* for the processing of requests by the Central Intelligence Agency. The change in the time limits made no one better off, but it did allow some agencies that complied with the ten-day limit to take longer to process requests. With the change, however, there was now enough room in the processing timetable to allow for ten-day to decide on requests for expedited access.

The 1996 amendments made some changes that directly affected the processing of electronic records. Some court decisions that permitted agencies to withhold records in computer formats were expressly overturned. This change was useful, although the cases had mostly been discredited.<sup>10</sup> In addition, agencies were expressly directed to search electronic databases when responding to FOIA requests. This change clarified the law, but agencies were already

---

<sup>10</sup> See SDC v. Mathews, 542 F.2d 1116 (9th Cir. 1976); Dismukes v. Interior, 603 F.Supp. 760 (D.D.C. 1984). See also Robert Gellman, *Twin Evils: Government Copyright and Copyright-Like Controls Over Government Information*, 45 *Syracuse Law Review* 999 (1995).

searching through electronic records for the most part. A troubling feature of the 1996 amendments was the provision that allows agencies to refuse to search electronic databases if the search would significantly interfere with the operation of the agency's automated information system. No comparable withholding authority exists for paper records so the result is that electronic records may be treated more restrictively than paper records. So far, however, I am not aware of any abuses of this new wholly *procedural* withholding authority.

The most interesting part of the 1996 amendment came from the emphasis placed on dissemination. The law added a requirement that agencies prepare a guide for requesting records under the FOIA, including an index of major information systems, a description of locator systems, and a handbook for obtaining information. Giving the public more information about agency record keeping activities is useful, although other types of finding aids for government records have tended to remain unused. In the Internet era, people want records more than finding aids. Further, it is not apparent why each of a hundred federal agencies must publish a separate guide on using the FOIA.

The more significant dissemination requirement is the provision directing agencies to make available for public inspection and copying any records released under the FOIA that are likely to become the subject of subsequent requests. This is a good idea made even better by the additional requirement that records be made available electronically. The goal is to prevent duplicative requests for the same documents.

Some agencies have begun to put requested records on their web sites. A good example is the Federal Bureau of Investigation.<sup>11</sup> Some records released under previous requests that are the subject of significant public interest can be read online. Subjects of available files are Leon Trotsky, Pablo Picasso, Rudolph Nureyev, Elvis Presley, Frank Sinatra, and the Hindenberg Disaster. No one has to make a FOIA request any more for these records.

---

<sup>11</sup> See <[www.fbi.gov](http://www.fbi.gov)>.

In retrospect, it is not clear that a change in the law was truly necessary to encourage agencies to put popular documents on the Internet. By 1996 when the Electronic FOIA Amendments finally passed after years of congressional inaction, agencies were beginning to discover the Internet. In fact, some agencies have been aggressively putting documents and other information resources online. The disclosures often go far beyond anything required under the 1996 amendments.

Use of the Internet for agency documents has affected the FOIA process. At some agencies, so many documents are available online that the volume of FOIA requests has dropped. At the Environmental Protection Agency, requests are less than half of what they were a few years ago, and the agency believes that the Internet is responsible. The interest in agency information has not diminished, but the demand can now be filled in a simpler and less expensive manner. Federal agency use of the Internet is still evolving.

## **The Future of FOIA**

I believe that the Internet will continue to diminish the importance of the request-and-response model for government information disclosure that is at the heart of the FOIA. People who want government documents tend to want them immediately, and an agency can anticipate some requests by making records directly available on the Internet. The number of formal FOIA requests should continue to diminish, but the FOIA process will never lose its importance. Agencies will rarely voluntarily release information that is embarrassing or politically sensitive. A process that allows citizens to request information that they want -- as opposed to the information that the agencies want them to have -- will always be necessary.

A reduction in FOIA volume may have some political implications. As fewer people use the law, it may lose political support. As the percentage of difficult requests increases because the Internet will provide access to non-controversial documents, agency complaints may increase. Fewer useful documents will be released through the FOIA process, and supporters will have fewer victories. Conflicts over disclosure will be more sharply drawn, and opponents of the FOIA will use these conflicts as a reason for undermining the law.

Supporters of disclosure will have to remain vigilant if these developments occur.

The Internet is already being used as an excuse for additional secrecy. The argument is that if safety information is available on the Internet, it can be used by terrorists all over the world. Industry and the police have already had some success with this argument over information about possible chemical disasters. The chemical industry appears to be motivated primarily by concern about embarrassing publicity and by the fear of citizen demands for better safety. The result of the coalition between industry and police was a temporary restriction on the availability of safety information that Congress previously determined to belong in the public domain but that was not yet released.<sup>12</sup> A final determination will not come for another year. The possibility that the Internet will provide a new justification for withholding public domain documents is a troublesome development that requires watching.

Another aspect of the FOIA and the Internet that calls for more study is the effect of Internet use by government workers on the availability of public information. No one has explored the FOIA consequences of networks. For example, what do we do when agencies routinely access information on a network that they do not maintain? Is that information available under the FOIA? Should it be? Can agencies use networks to evade public access requirements? Can requesters use the FOIA to monitor network use by agencies? Some of these questions will be difficult to answer.

Other network-based access and disclosure questions arise as well. What is the status of electronic mail under the FOIA? When is email official and when is it personal? Can Internet usage records of government officials be requested under the FOIA? Examples are browser bookmarks, cookies, cache, and history files. These files will offer a citizen a new perspective on what a bureaucrat read and considered during the course of making decisions. Should this type of detailed internal information be routinely available to the public? Unfortunately, the 1996 Electronic FOIA Amendments may have

---

<sup>12</sup> See the Chemical Safety Information, Site Security and Fuels Regulatory Relief Act, Public Law 106-40 passed in 1999.

brought the FOIA into the computer age, but the amendments did not bring the law into the Internet age. Too many network access questions remain unexplored and unanswered. The worst part of the 1996 amendments is that they probably foreclosed legislative review of the FOIA for the next decade.

Finally, I want to discuss another important American law about dissemination of federal agency information. In 1995, Congress amended the Paperwork Reduction Act by adding, among other things, general requirements for agency information dissemination activities. These provisions offer an interesting perspective on information policy in the era of electronic data. The paperwork amendments also reflect a legislative response to bureaucratic control of information even in the face of contrary laws and policies.

The requirements are set out in four short paragraphs of the law.<sup>13</sup> The first paragraph directs agencies to ensure that the public has timely and equitable access to the agency's public information. This is to be accomplished by encouraging a diversity of public and private sources for government public information and by providing timely and equitable access to data maintained in electronic formats. The second paragraph tells agencies regularly to solicit and consider public input on agency information dissemination activities.

The law becomes more specific in the third paragraph, which requires agencies to provide adequate notice when starting, substantially changing, or ending significant information dissemination products. The statute creates an opportunity to identify and consider conflicts that may arise when information programs change. Public notice and comment serves everyone's interest, except possibly the bureaucrat's, and that is the point.

The fourth paragraph prohibits agencies from engaging in four separate restrictive dissemination practices. This provision is a major contribution of the law. General statutory encouragement to disseminate data is a nice idea. Over the years, however, federal agencies have found ways to circumvent existing laws and policies in order to maintain control over their information and its users. The

---

<sup>13</sup> 44 U.S.C. § 3506(d)(1)-(4) (1996 Supp.).

1995 paperwork amendments were expressly designed to prevent agencies from playing these games.

The first restriction prevents an agency from establishing an exclusive, restrictive, or other distribution arrangement that interferes with timely and equitable availability of public information to the public. This means no monopolies, governmental or private. The government can release data directly or through a vendor, but it cannot establish or tolerate a monopoly.

The second restriction prevents an agency from restricting or regulating the use, resale, or redissemination of information. The ability to control secondary use is an important right of a copyright holder. Despite the inability to copyright data, some government agencies licensed government data users and kept them from redistributing the data to others. The practice flies in the face of the no-copyright policy for federal information, and Congress decided to stop it.

The third restriction prohibits fees or royalties for resale or redissemination of public information. This goes hand-in-glove with the second restriction. The goal is to ban downstream controls of any sort.

The final restriction prevents an agency from establishing a user fee exceeding the cost of dissemination. The policy of the FOIA is that a requester is charged no more than the cost of responding to a request. Some agencies established separate dissemination methods and charged higher fees. If there were no other sources, users had to pay what the agencies asked. These agencies behaved like a copyright holder, but they cannot do this anymore.

These provisions of the Paperwork Reduction Act stop agencies from engaging in information control practices that might otherwise be used for electronic information. The intellectual origin of the policies came from work that began in 1985 in the House Subcommittee on Government Information.<sup>14</sup>

---

<sup>14</sup> See Electronic Collection and Dissemination of Information by Federal Agencies: A Policy Overview, House Report No. 99-560, 99th Congress, 2d Session n.151 (1986).

## **Conclusion**

The paperwork law, the FOIA, the Privacy Act, and the Copyright Act together illustrate the complexity of American government and of the congressional process. The laws also illustrate the diversity of statutory sources for establishing information policy in the modern world. The FOIA is an important part of that information policy, but it is no longer the only part.

As we proceed further into the Internet age, information, information technology, information policy, and the statutes that regulate them are certain to grow richer and more complex.

## **Prof. Dr. David H. Flaherty**

Information and Privacy Policy Consultant Victoria, British Columbia, Canada

## **Die Balance zwischen transparenter Verwaltung und Schutz der Privatsphäre: Kanadische Erfahrungen**

### **Balancing open government and privacy protection\***

Speaking Notes of Professor David H. Flaherty Privacy and Information Policy Consultant Victoria, British Columbia, Canada\*\*

I start with the fact that I only ceased to be Information and Privacy Commissioner for the Province of British Columbia, Canada, on July 31, 1999. During a six-year time period, I wrote approximately 3,000 pages of decisions that sought to balance the **competing values** of data protection and open government. At this point, I do not have any distance or perspective on my recent work, nor has it been the subject of academic analysis, which I regard as essential.

### **Being More Transparent**

1. The statutory goals of the B.C. *Freedom of Information and Protection of Privacy Act* (the Act) are to “make public bodies more accountable to the public and to protect personal privacy....” (Section 2; statute and decisions available on [www.oipcbc.org](http://www.oipcbc.org)) These dual purposes create an inherent tension, so **balancing** is always required. In practice, I found few problems achieving such a balance during my six-year term of office as Information and Privacy Commissioner for British Columbia (1993 – 1999).

My conscious goal in the 322 decisions that I wrote was to promote open, accountable government. My secondary goal in decision-writing and, especially, policy advice was to encourage a privacy-friendly environment. I readily admit that I regard the promotion of Freedom of Information as the dominant value in this equation.

2. The process of promoting open and accountable government, put simply, involved me interpreting, and my professional colleagues applying, the language of the Act in literally thousands of cases, since the Legislature itself established the standards to be used in balancing the competing interests at stake. Of course, I enjoyed some discretion and latitude in my decisions, subject to judicial review, which I regard as an important check on the power entrusted to a Commissioner in a regulatory model.

3. I found over the course of my term that it was beneficial, when balancing competing interests, to have a single person serving as Information Commissioner and as Privacy Commissioner, as is the model for the Canadian provinces and territories (but not the federal government). Thus I applaud the UK decision to make the Data Protection Commissioner (Registrar) responsible as well for the oversight of the draft Freedom of Information Bill.

4. Some of my decisions essentially sacrificed the traditional privacy interests of individuals to the goal of promoting open government.

- For example, the decision to disclose to the media severance payments made to individual staff during the closure of Shaughnessy Hospital in Vancouver. (Order No. 24-1994, September 27, 1994) My basic guiding principle, as displayed here, was that the public has a right to know how its money is being spent. Similarly, I ordered the disclosure of the specific amount of a severance payment made to a terminated fire chief, but not the personal details of the settlement beyond that amount, i.e., pension allocation, payment for counselling services, etc. (Order No. 173-1997, July 14, 1997)
- A more delicate and complex example of balancing is found in Order No. 27-1994, October 24, 1994. There I found that a protected “core of privacy” surrounding the suicide of a young girl while in the custody of the state should prevent the disclosure of her diary to the media. However, I did allow for the disclosure of information that revealed the nature of the review of her death conducted by the institution in question, because of the obligation

of accountability of a psychiatric institution to the public under the Act.

5. Because of my background as a privacy advocate, commentators on my appointment thought that I would be biased towards privacy protection. I believe that an objective review of my decisions would indicate that this did not prove to be the case. I give first priority to openness and accountability for general information held in records, subject to the protection of individual privacy set out in section 22 of the Act. My goal was to promote the disclosure of **general** government information while protecting the privacy interests of individuals.

Because section 22 is so important a guide for decision making under the Act, I present here a brief statement of what it says, lest you think that the process is very subjective. Whether in civil or common law jurisdictions, the goal has to be to obtain a strong *Freedom of Information and Protection of Privacy Act* and then apply it to concrete situations that arise.

Section 22 has three (admittedly confusing) categories of criteria for establishing if a disclosure of personal information would be an unreasonable invasion of the privacy of a third party.:

- Section 22(2) sets out eight categories that the head of a public body must consider as "relevant circumstances" in determining whether an unreasonable invasion of privacy may exist. Three examples of sub-sections provide the flavour of them:
  - (c) the personal information is relevant to a fair determination of the applicant's rights,
  - (d) the third party will be exposed unfairly to financial or other harm,
  - (e) the personal information has been supplied in confidence.

- Section 22(3) specifies disclosures of personal information that are “presumed to be an unreasonable invasion of a third party’s personal privacy...”
  - (a) the personal information relates to a medical, psychiatric or psychological history, diagnosis, condition, treatment or evaluation,
  - (b) the personal information was compiled and is identifiable as part of an investigation into a possible violation of law,...
  - (d) the personal information relates to employment, occupational or educational history,

6. Many of my decisions involved the application of section 22 to personal information found in general records in dispute. This requires a balancing of competing interests, subject to the specific statutory provisions already outlined.

- Thus the salaries, expense accounts, and job descriptions of public servants at all levels of government are public information, but not job performance, resumés, etc. In Order No. 161-1997, May 1, 1997, I found that personal details concerning an individual could be severed from expense accounts, such as movies watched in a hotel room or telephone numbers that were called.
- I also decided that a School District did not have to disclose to parents the specific disciplinary measures taken against a teacher (Order No. 62-1995, November 2, 1995). However, if a professional body, such as the College of Physicians and Surgeons, takes disciplinary action against a member, then that information is to be made public. (See Order No. 221-1998, April 16, 1998)
- My goal was to promote a **privacy-friendly environment** in the province by not disclosing intimate or salacious details of any individual, especially to the media. Our advisory work on the public reports of the Children’s Commission about deceased children is a model in this regard. ([www.childservices.gov.bc.ca](http://www.childservices.gov.bc.ca)) I am

pleased to report that neither the Children's Commission nor my office were criticized for our work in this regard.

7. There is a public interest test for disclosure of personal information under section 25, titled "Public Interest Paramount," which supersedes any other exception in the Act. To date, I have simply required public bodies to show evidence that they have considered this exception in reaching a decision. Some critics believe that I should have myself ordered disclosure of information on the basis of this section. The legal advice that I received was that I could not so act.

This section, or section 33(p) [A public body may disclose personal information only if the head of the public body determines that compelling circumstances exist that affect anyone's health or safety....], is primarily used by law enforcement bodies, including the Corrections Branch, to notify the public, either generally or in very specific circumstances, such as parents of children living near a particular school, of the presence of a predatory sex offender in the community. Our role was to examine the evidence promoting disclosure in advance of its occurrence. My impression is that the incidence of such disclosures was between six and twelve times per year.

I considered this issue of balancing confidentiality versus disclosure in Order No. 221-1998, April 16, 1998, which involved the CBC's request for access to records from the College of Physicians and Surgeons about allegations of misconduct against a physician that had become public knowledge. I wrote in a thirty-page decision:

I agree fully with the College with respect to the following: 'The determination of what information should be made public requires an appropriate balance to be struck between the rights of the public to know, to the extent necessary to ensure their protection, and the rights of the physician to a fair level of protection of privacy and due process according to the specific circumstances of each case.'  
(Submission of the College, paragraph 51)

That is essentially the approach that I am required to take in reaching my decision. My role under the Act is to act as a check on the balance that the College strikes in a particular case, as I proceed to do below by applying the Act.

It is worth emphasizing, for a substantial decision like this one, that my personal views on the desirability of disclosure in a particular case very much subordinate to the specific requirements of the Act, but I did subject the disciplinary procedures and practices of the College to a thorough review from the perspective of the Act.

8. I think it would best illustrate my approach to balancing privacy and open government to discuss my Order No. 309-1999, April 22, 1999, in more detail. Essentially, I upheld a decision of the West Vancouver Police Department not to release the name of an accident victim to a reporter for a local newspaper. In summary form, here is what happened:

The police refused to release the name of the 86 year-old victim on the grounds that disclosure would be an unreasonable invasion of her privacy. Additionally, the police argued that disclosure would invade the privacy of the victim's family, who did not want the name released.

At the written inquiry, the reporter questioned the degree to which a deceased person has privacy rights, as well as the motives of the next of kin in not wanting the name released. The reporter also argued that the victim's name should be released on public interest grounds, stating: "I respectfully suggest that a car accident that results in a person's death on a public street relates to community safety and is of public interest...I suggest that the name of a deceased person in a traffic accident is an important component of the full facts of a news story..."

I agreed with the Police Department's argument that disclosure of the name of the deceased does not further, and is not necessary for, the promotion of public health or safety. It is sufficient that the details concerning the location and circumstances of the accident were disclosed. "I do not accept that a newspaper story is less credible simply because the name of the victim has not been disclosed." I

also concluded that the deceased does have privacy rights and that the privacy of the deceased's family may be compromised by release of the victim's name.

I am pleased to be able to inform you that the press did not take the Office to judicial review on this decision (at least so far). In addition, I made a very particular decision that reflected the emotive power of an *in camera* submission from a close relative of the deceased. I did not pontificate as to what particular set of circumstances should militate in favour of disclosure of accident victim information, for example, preferring, as was my custom, for the municipal police forces in the province to make that decision on their own, reflecting their own best practices and experiences.

I also made this specific decision against the media, so to speak, with full understanding and new-found appreciation of the central importance of the media, in all its forms, for the promotion of an open accountable society. In this connection, I would like to quote what I wrote about the importance of the media in my final message as Information and Privacy Commissioner for British Columbia:

I wish to close on a note of high praise for the media in this country, in at least partial response to the recurrent attacks on them by politicians in particular. I am not thinking here of the issue of trying to balance competing interests of accountability and privacy in the dozens of decisions that I have made in response to media requests for access to information. Nor am I selfishly reflecting my strong sense that the media would have had to be my ultimate defenders, as surrogates for the public, if the politicians and government of this province had chosen to turn against the Act by, for example, abolishing it. There have been times when I did not regard this as an idle threat. At the end of the day, my privileged vantage point of the past six years has fully persuaded me that a free press is absolutely fundamental to the preservation and advancement of an open and democratic society in British Columbia and Canada as a whole. Becoming fully persuaded of what may strike some as a truism has been an added benefit and lesson from my experience of public office. It has been worth it.

## 9. Conclusion

I take considerable satisfaction in being able to say, after six years in public office, that "I did it my way," in the words of the late lamented Frank Sinatra. I made decisions in specific cases that were highly unusual (one in ten) in the sense that my professional staff of Portfolio Officers had not mediated them. In particular, I limited my decisions to the specific circumstances before me, and I avoided overly-broad language that might come back to haunt me at a later date. I also had the very important benefit of receiving detailed submissions from applicants and public bodies on the application of specific sections of the Act. The specialists in the Legal Services Branch of the Ministry of Attorney General were especially thorough and perceptive in this regard in representing central government. They reminded me of both my own precedents, or those of other Canadian provincial Information and Privacy Commissioners (especially Ontario), and of the general principles of statutory interpretation applicable to my work as a decision maker. More importantly, they made cogent statements of facts and coherent arguments.

In terms of the theme of this presentation, I will admit that it took me some time to accept the limits of what personal information I could disclose to "worthy" applicants. In the Saturna Island decision, I thought that the name of an anonymous complainant against the Recycling Committee of the Saturna Island Community Club should be disclosed to the "aggrieved" or perceived victims, because of what I thought were "peculiar" circumstances. The Supreme Court of British Columbia decided otherwise. (Order No. 36-1995, March 31, 1995); (*J. Doe v. British Columbia* (Information and Privacy Commissioner), [1996] B.C.J. No. 1950 (B.C.S.C)). In another decision, I ordered disclosure of the identity of an "expert" to a female applicant, who had complained to a public body against a psychiatrist. My implicit rationale was that a judge should pass judgment on what had transpired. The judge who reviewed the same records decided not to do so, or perhaps that she could not do so. (See Order No. 144-1997, January 17, 1997); (*Greater Vancouver Mental Health Services v. British Columbia*, (Information and Privacy Commissioner), [1999] B.C.J. No. 198 (B.C.S.C.)).

A final brake on my decision making and balancing activities deserves mention. My Office functioned in a highly-collegial manner. After I drafted a decision, for example, I asked a specific staff person and, usually, outside counsel to review my draft. Occasionally, more than ten or fifteen drafts emerged from this process. At a certain point in the process, every professional staff member had the opportunity to review the draft text of an order. There were lengthy debates on occasion and very detailed and sometimes emphatic "suggestions" for revision. I think that I changed my mind completely on disclosure on at least a few occasions. I say this with considerable pride, because I believe that the end result was practical, common-sense decisions, balancing open government and privacy protection, that were understandable to applicants, public bodies, and the people of British Columbia. Contrary to media headlines, I was not really an Information Czar!

\* I delivered earlier versions of this presentation to the Privacy Laws and Business Conference, Cambridge, UK, July 13, 1998; the 5<sup>th</sup> Annual Conference of the Office of the Information and Privacy Commissioner for B.C., Vancouver, BC, October 30, 1998; and the International Meeting of Privacy and Data Protection Commissioners, Hong Kong, September, 1999.

\*\* David Flaherty, Ph. D., was the first Information and Privacy Commissioner for British Columbia (1993 – 1999). He is a Professor Emeritus, University of Western Ontario and an Adjunct Professor at the University of Victoria. His contact information is: 1939 Mayfair Drive, Victoria, BC, V8P 1R1; [David@Flaherty.com](mailto:David@Flaherty.com)

© Copyright by David H. Flaherty, 1999. All rights reserved.



## **Viktor Monachov**

Mitglied des Gerichts für Informationsstreitigkeiten beim Präsidenten der Russischen Föderation

## **Die Entwicklung des Informationsrechts in Russland**

### **Einführung**

Die vorhandenen Systeme der rechtlichen Regelung gesellschaftlicher Verhältnisse im Bereich der Information müssen heute, am Ende des 20. Jahrhunderts und zweiten Jahrtausends, an die neuen Realitäten der postindustriellen Informationsgesellschaft adaptiert werden.

Cyberspace, virtuelle Realität... Dieses neue Rechtsgebiet, das in Folge der Entwicklung der Informations- und Telekommunikationstechnologien entsteht, bildet den Bedarf an neuen Formen und Verfahren der rechtlichen Regelung der Verhältnisse im Informationsbereich des gesellschaftlichen und staatlichen Lebens heraus. Eigentlich sind wir Augenzeuge einer grundsätzlichen Veränderung des Entwicklungsvektors der internationalen Rechtswissenschaft.

Wenn die Analogie zur Computerentwicklung hier am Platz wäre, könnte man sagen, dass die internationale Rechtswissenschaft sich von der Erfassung und Lösung der rechtlichen "hardware"-Probleme (d.h. der Probleme der Güter- und Vermögensrechte) zur Aneignung der subtileren und komplizierteren Probleme der rechtlichen "Software" entwickelt. Darunter wären folgende Schwerpunkte zu nennen:

- Bestimmung und Feststellung der Besonderheiten der rechtlichen Regelung der Information als Gegenstand des öffentlichen und/oder privaten Rechts.

- Solche gesetzliche Regelung der Informationsverhältnisse<sup>1</sup>, welche den entsprechenden Schutz der Unverletzlichkeit des privaten Lebens, des privaten und familiären Geheimnisses, anderer gesetzlich geschützter Geheimnisse; der Ehre, Würde, des guten Rufes, darunter des geschäftlichen Rufes; der Ergebnisse der intellektuellen Tätigkeit (darunter der ausschließlichen Rechte darauf, d.h. des intellektuellen Eigentums); des Namensrechts, anderer privater, nicht mit Vermögen verbundener Rechte sowie anderer nichtmaterieller Güter gewährleistet.

Heutzutage verschiebt sich der Interessenschwerpunkt fortschrittlicher Gesetzgeber und Rechtsanwender immer mehr aus dem Bereich der Erarbeitung und Anwendung der gesetzgeberischen Regelungen, welche die Verhältnisse hinsichtlich Personen, Güter, Energien und ähnlicher Gegenstände des Rechts regeln, in den Bereich der Schaffung und Anwendung der Regelungen, welche gesellschaftliche Verhältnisse hinsichtlich aller möglichen Informationen regeln sollen.

Nach Berechnungen unserer Experten wurden etwa 500 normative Rechtsakte, die solche gesellschaftlichen Verhältnisse regeln, in Russland allein in der Zeitspanne von 1991 bis zum Juli 1995 verabschiedet. Darunter sind 75 Rechtsakte vollinhaltlich diesen Fragen gewidmet, in die restlichen sind nur einzelne Regelungen, welche Informationsverhältnisse regeln, einbezogen<sup>2</sup>. Zwar sollten wir nicht vergessen, dass die große Anzahl der Rechtsregelungen an und für sich nicht immer so gut ist. Daran erinnert uns Tacitus in seiner berühmten Maxime: In dem verdorbenen Staat gibt es zahlreiche Gesetze.

Aber solche gesetzgeberischen Neuerungen sind doch kein bloßer Tribut an den hochaktuellen Gegenstand des Rechts, d.h. an die Information. Davon hängt es heute ab, ob wir in die internationale Gemeinschaft der Informationsgesellschaften aufgenommen werden

---

<sup>1</sup> Die Konzeption der bedingten Absonderung der Informationsverhältnisse im Verwaltungsbereich und der Erscheinung ihrer rechtlichen Form, d.h. der Informationsrechtsverhältnisse, wurde zum ersten Mal 1972 vom Prof. Dr. habil. jur. A. B. Vengerov erarbeitet. Siehe: Венгеров А.Б. Право и информационное обеспечение АСУ. – “Советское государство и право”, 1972, т 8

<sup>2</sup> Siehe: Копылов В.А. О структуре и составе информационного законодательства. - “Государство и право”, 1996, т 6, с. 101

dürfen. In Europa gibt es schon ernsthafte völkerrechtliche Beschränkungen für Outsider-Staaten, d.h. für die Staaten, die noch keine neue Informationsgesetzgebung verabschiedet haben. Ein Beispiel: Gemäß den Richtlinien der Europäischen Union 95/46/CE vom 24.10.98 verirken die Länder, die den entsprechenden Schutz der persönlichen Daten (im weiteren PD) nicht gewährleistet haben, das legitime Recht auf den Erhalt jeweiliger PD aus den Ländern der Europäischen Union. Gemäß Art. 6 der seit dem 1.10.1985 gültigen Konvention des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten dürfen die sogenannten "intimen Daten" (über Vorstrafen, Nationalität, Gesundheit oder sexuelle Orientierung) nur in solchen Konventionsteilnehmerstaaten in Computern bearbeitet werden, in welchen das nationale Recht die entsprechenden Schutzgarantien gewährleistet.

Solche informationsrechtliche Regelungen gestalten neue öffentliche und private Informationsrechtsverhältnisse, die zur Grundlage des Rechtssystems der internationalen Informationsgesellschaft des 21. Jahrhunderts und dritten Jahrtausends werden sollen.

## **1. Informationsrecht in Russland: Begriff und Inhalt**

Womit begann die Geschichte der Herausbildung des Informationsrechts in Russland und was beinhaltet bei uns dieser Begriff? Einer der ersten Artikel, mit dem der Versuch gemacht wurde, das Informationsrecht als einen selbständigen Zweig zu begründen, wurde in Leningrad in den späten 70er Jahren veröffentlicht<sup>3</sup>.

Diese Einstellung wurde aber von Kollegen gar nicht unterstützt. Es lag daran, dass es damals noch kein entwickeltes und selbständiges System der informationsrechtlichen Einwirkung auf gesellschaftliche Verhältnisse in unserem Lande gab. Gleichzeitig waren entsprechende westliche Veröffentlichungen, darunter auch deutsche<sup>4</sup>, uns schon

---

<sup>3</sup> Siehe: Еременко И.В., Краснянский В.Э., Старшинов Ю.В., Шепелев Е.Ф. Система правового регулирования структур и процессов управления. – "Проблемы системотехники", вып. 1, ч. 1, "Судоостроение", 1976 г.

<sup>4</sup> Ich meine nämlich folgendes Buch: U.Dammann/M. Karhausen, P.Muller/W.Steinmuller, "Datenbanken und Datenschutz", Frankfurt/New York, 1974g; Por. L Philips, Recht und Information, Freiburg, 1970g; а также Берлинские выпуски "Elektronische Datenverarbeitung im Recht"

bekannt. Sie waren es, welche die Fortsetzung unserer Forschungen auf diesem Gebiet gefördert haben.

Als Gründer der selbständigen informationsrechtlichen Richtung in der sowjetischen und später russischen Rechtswissenschaft gilt mit Recht Prof. Dr. habil jur. A. B. Vengerov, der erste Vorsitzende der Kammer des Informationsgerichtes beim Präsidenten der Russischen Föderation. Leider ist er 1998 schon verstorben.<sup>5</sup>

Einer seiner besten Schüler, Dr. habil. jur. J. M. Baturin erforschte den gleichen Themenkreis und analysierte verschiedene Termini, welche von verschiedenen Autoren in bezug auf diesen Bereich des Rechts verwendet wurden - "Programmrecht", "Rechtsinformatik", "Informatikrecht", "Computerrecht" und "Informations- und Computerrecht"<sup>6</sup>. Der Titel der Monographie, die zur Grundlage seiner Habilitationarbeit geworden ist, zeugt davon, dass er das Fachwort "Computerrecht" für das treffendste und genaueste hält.

Ich glaube aber, dass der Begriff "*Informationsrecht*" für die in vielen Hinsichten noch metaphorische, bildhafte Bezeichnung des ganzen Komplexes - der Regelungen, Institutionen und der Teile dieses sich als Hauptzweig des Rechts im künftigen Informationszeitalter durchsetzenden Zweiges - besser passt. In Russland werden heute solche Teile dieses Zweiges wie Computerrecht und Medienrecht<sup>7</sup> intensiv herausgebildet; es werden Rechtsinstitutionen der Informationsrechte der Bürger und der Medienfreiheit entwickelt.

Einer der größten russischen Rechtswissenschaftler Prof. J. A. Tichomirov hält das "Informationsrecht" auch für einen neuen komplexen Zweig des Rechts, der, seiner Meinung nach, zum öffentlichen Recht gehört<sup>8</sup>. Wenn er vom Inhalt dieses Zweiges spricht, bemerkt er, dass es hier "um Informationsverhältnisse als den Gegenstand der rechtlichen Regelung, um Subjekte der informationsrechtlichen Verhältnisse, um Rechtsverfahren der Erhal-

---

<sup>5</sup> Siehe: Венгеров А.Б., Теория государства и права. Учебник для юридических вузов, М., "Новый Юрист", 1998, 622с.

<sup>6</sup> Siehe: Батурин Ю.М. Проблемы компьютерного права. М., 1991

<sup>7</sup> Hoffmann-Riem W., Monachov V. Rundfunkrecht in Rubland. Auf dem Weg zu einer neuen Medienordnung, Nomos Verlagsgesellschaft, Baden-Baden/Hamburg/St.Petersburg, 1994, 633s.

<sup>8</sup> Siehe: Тихомиров Ю.А. Публичное право. М., "Бек", 1995, 339с

tung, Vermittlung, Aufbewahrung und Nutzung der Information, um Rechtsverfahren der Informationen verschiedenen Inhalts sowie um Nutzung von Datenbanken und -dateien geht".

Der Verfasser des in Russland ersten Lehrbuchs für Informationsrechts A. B. Agapov<sup>9</sup> gibt keine Definition des Informationsrechts. Sein Nachfolger V. A. Kopylov definiert das Informationsrecht als "das System der vom Staat geschützten sozialen Normen und Verhältnisse, die im Informationsbereich, d.h. im Bereich der Herstellung, Verarbeitung und Nutzung der Information entstehen."<sup>10</sup>

## **2. Grundlegende Informationsrechte der Bürger als wichtigste Institutionen des Informationsrechts**

Das Schicksal wollte es, dass ich es war, der als einer der ersten in der UdSSR 1983 während der Verteidigung meiner Dissertation der Rechtswissenschaft die Konzeption der sogenannten grundlegenden Informationsrechte der Bürger (das Recht auf Information und das Recht auf Schutz der privaten Information), sowie die herangereifte Notwendigkeit der Verbriefung dieser Rechte in der Verfassung erklärt und in wissenschaftlicher Polemik behauptet hat<sup>11</sup>.

Acht Jahre später, schon im neuen Russland, wurde diese Doktrin-idee in der Gesetzgebung verankert. In der Deklaration der Rechte und Freiheiten des Menschen und Bürgers, die vom Obersten Rat der RSFSR am 22.11.1991 genehmigt wurde, wurden zwei Artikel (Art. 9 und Art. 13) diesen Rechten gewidmet.

"Sammeln, Aufbewahrung, Nutzung und Verbreitung der Information über das private Leben einer Person ohne ihre Genehmigung ist unzulässig, mit der Ausnahme der im Gesetz festgelegten Fälle" (Art. 9 Abs. 3).

---

<sup>9</sup> Siehe: Агапов А.Б. Основы федерального информационного права России. М., "Экономика", 1995

<sup>10</sup> Siehe: Копылов В.А. Информационное право: учебное пособие. М., "Юристъ", 1997, с.18

<sup>11</sup> Siehe: Монахов В.Н. Государственно-правовые вопросы информационного обслуживания граждан в СССР (конституционный аспект). Автореферат диссертации. М., ВНИИСЗ Министерства юстиции СССР, 1983, 17с.

"Jeder hat das Recht, Information zu suchen, zu erhalten und frei zu verbreiten. Die Beschränkungen dieses Rechts dürfen vom Gesetz nur zum Zweck des Schutzes des privaten, familiären, professionellen, geschäftlichen und staatlichen Geheimnisses sowie der Sittlichkeit festgelegt werden. Die Liste der Daten, die zum staatlichen Geheimnis gehören, wird vom Gesetz festgelegt" (Art. 13 Abs. 2).

Zwei Jahre später, im Dezember 1993, wurden diese Regelungen der Deklaration in der Verfassung verbrieft und in den Artikeln 23, 24, und 29 der geltenden Verfassung Russlands weiterentwickelt.

Natürlich sind die rechtsfestlegenden Ideen, die das Wesen dieser russischen politisch-rechtlichen Regelungen aus den Jahren 1991 und 1993 wie auch ihres doktrinhaften Vorgängers aus dem Jahr 1983 ausmachen, nicht in denselben Jahren entstanden. Sie waren der internationalen Gemeinschaft lange vor dieser Zeit schon bekannt.

So ist zum Beispiel Schweden der Bahnbrecher in der gesetzgeberischen Verbriefung der öffentlich-rechtlichen Vorstellung von dem "Recht des Volkes, zu wissen". In diesem Lande wurde das Öffentlichkeitsprinzip (offenlighetsprincip), das Prinzip der Zugänglichkeit offizieller Dokumente der Machtstrukturen und dadurch die Offenheit und Transparenz der Staatsmacht schon 1776 im Akt über Pressefreiheit auf dem höchsten juristischen Niveau, auf dem Niveau der Verfassung verbrieft. Etwas später leuchtete der kleine Strahl der Informationsfreiheit auch in Russland auf. So verordnete die Kaiserin Katharina II. in ihrem Erlass vom 15.01.1783 "Buchdruckereien anderen Fabriken und Gewerben gleichzusetzen", und infolgedessen durfte "jeder nach seinem Willen solche Druckereien gründen, ohne die Genehmigung von jemandem einzuholen."<sup>12</sup>

Die französische Deklaration der Rechte des Menschen und Bürgers 1789 enthielt auch die Regelungen der Rechte, die als Informationsrechte betrachtet werden können. Es geht hier um die Regelung des Artikels 11 über das Recht jedes Bürgers frei "sich auszudrücken, zu

---

<sup>12</sup> П.С.З.Р.И. (Vollständige Sammlung der Gesetze des Russischen Reiches - Anm. der Übersetzerin)– СПб., 1830, - Т. XXIII.- м 17508

schreiben und zu veröffentlichen" sowie um die Regelungen der Artikel 14 und 15 über das Recht der Bürger, die Aufsicht über die Verausgabung der Steuergelder zu haben und die "Rechenschaft von jeder Amtsperson über ihren Zuständigkeitsbereich" zu verlangen.

Indem wir diese geschichtlichen Wurzeln der modernen Ideologie und Praxis der sozial-politischen Transparenz feststellen, sollen wir nicht vergessen, dass die Verbriefung bestimmter Rechte der Bürger *de jure*, sei es auch eine Verbriefung in der Verfassung, weder in Schweden, noch in Frankreich, noch in Russland ihrer vollständigen und, was besonders wichtig ist, kontinuierlichen Verwirklichung *de facto* nicht gleichzusetzen ist.

Die Informationsfreiheit ist kein statischer *Zustand*, sondern fast immer und überall ein dynamischer *Prozess*. Die Welt kennt einen 30-jährigen und sogar einen 100-jährigen Krieg, aber der "Krieg" um die Wort- und Informationsfreiheit hat kein Ende, weil man in diesem Krieg nicht ein für allemal siegen kann. Dieser Prozess ist dem Radfahren gleich: Sobald man die Pedale nicht mehr tritt, befindet man sich schon auf dem Wegrand und ist man gezwungen, sein Informationsmenü darauf zu beschränken, was jemand anderes einem aufzwingt.

## **2.1 Recht auf Information**

Die russische verfassungsrechtliche Formel dieses Rechts ist fünfgliedrig. Das bedeutet, dass Art. 29 Abs. 4 der Verfassung Russlands fünf Informationsrechte enthält, die ein "jeder" auf dem Territorium der Russischen Föderation hat. Das sind die Rechte, Information auf jedwede legitime Weise frei:

- zu suchen,
- zu erhalten,
- zu vermitteln,
- herzustellen und
- zu verbreiten.

Zum Vergleich kann man bemerken, dass die entsprechende, im Art. 10 der Europäischen Konvention über den Schutz der Menschenrechte verbriefte Formel des analogen Rechts, zweigliedrig ist. Sie verbrieft das Recht jedes Menschen, die Information nur "zu erhalten und zu verbreiten". Das Recht, die Information *zu suchen*, ist in dieser Formel nicht verbrieft. Ich glaube, "nach dem Buchstaben des Gesetzes" könnte das die Informationsaktivität der Bürger des vereinigten Europas unter bestimmten Bedingungen unerwünscht beschränken. Deswegen möchte ich de lege ferenda die Aufmerksamkeit europäischer Kollegen auf die Möglichkeit lenken, diese Formel mindestens bis drei Glieder zu erweitern. Ich meine, dass das Recht, die Information *zu suchen*, auch in diese Formel einbezogen werden könnte.

Die verfassungsrechtliche Basis des Rechts auf Information besteht in Russland nicht nur aus den Regelungen Art. 29 Abs. 4 der Verfassung. Außerdem gehören auch die verfassungsgemäße Garantie der Medienfreiheit und das Zensurverbot (Art. 29 Abs. 5) dazu. Das ist auch das verfassungsmäßige Recht eines jeden auf die "wahrheitsgetreue Information" über den Umweltzustand (Art. 42). Und schließlich ist das auch das Recht eines jeden, "die Einsicht in die Dokumente und Materialien zu haben, welche seine Rechte und Freiheiten unmittelbar betreffen, wenn etwas anderes im Gesetz nicht vorgesehen ist" (Art. 24).

Diese verfassungsrechtlichen sowie völkerrechtlichen Regelungen (gemäß Art. 15 Abs. 4 der Verfassung Russlands "sind allgemein anerkannte Prinzipien und Regelungen des Völkerrechts ... ein Bestandteil des russischen Rechtssystems") werden in Regelungen der gesetzgeberischen Akten verschiedener Rechtszweige weiterentwickelt und konkretisiert. Nämlich in der Strafgesetzgebung. So sieht der Artikel 237 des Strafgesetzbuches "Verheimlichung der Information über die für Leben oder Gesundheit der Menschen gefährlichen Bedingungen" die schroffsten Strafmaßnahmen (Freiheitsstrafe bis zu fünf Jahren!!!) für die "Personen vor, die die Bevölkerung mit der Information über die für Leben oder Gesundheit der Menschen gefährlichen Ereignisse, Tatsachen oder Erscheinungen versorgen sollen, aber solche Information verheimlicht oder verfälscht haben". Der Artikel 140 des Strafgesetzbuches "Weigerung, dem Bürger die Information zur Verfügung zu stellen" stellt das verfassungsmäßige

Recht eines Jeden auf die Einsichtnahme in die Dokumente und Materialien, welche seine Rechte und Freiheiten unmittelbar betreffen, mit Strafmaßnahmen (Geldstrafe oder Entziehung des Rechts auf die Bekleidung bestimmter Posten oder auf die Ausübung bestimmter Tätigkeiten) sicher. Was die Rechte anbetrifft, welche die Transparenz des politischen Prozesses und der Staatsmacht garantieren, so haben diese Rechte eine relativ konkrete gesetzgeberische Form nur hinsichtlich der Medienredaktionen erhalten. Der Artikel 39 des Gesetzes der RF "Über Massenmedien" stellt diese wirkungsvolle "Informationswaffe" für die Verteidigung der Demokratie seit 1992 nur den Medienredaktionen zur Verfügung, d.h. er räumt ihnen das Recht auf Anfrage betreffs die Information "über die Tätigkeit der Staatsorgane und -organisationen, gesellschaftlichen Vereinigungen und ihrer Amtspersonen" ein. Bürger aber besitzen gemäß diesem Gesetz nur das *passive Recht auf den Erhalt* entsprechender Informationen über Massenmedien (Art. 38 des Gesetzes der RF "Über Massenmedien").

Dieses Missverhältnis der Informationsrechte der Medienredaktionen und der Bürger muss der Gesetzentwurf des Föderalgesetzes "Über das Recht auf Information" beseitigen, der vom Präsidenten Russlands noch im Juni 1996 der Staatsduma des Föderalversammlung der Russischen Föderation zur Behandlung vorgelegt wurde. Gemäß den Regelungen dieses Gesetzentwurfes ist es der Bürger, der das Hauptsubjekt dieses Rechts ist.

Es sei zu bemerken, dass dieser Gesetzentwurf schon eine lange und schwierige Geschichte hat. Noch am 12.06.1990 hat der Oberste Rat der UdSSR in seinem speziellen Beschluss zwei seiner Ausschüsse (für Glasnost' und für Wissenschaft) beauftragt, "den Entwurf eines das Recht der Bürger auf Information regelndes Gesetzes vorzubereiten und dem Oberen Rat der UdSSR bis zum 1.01.1991 zur Behandlung vorzulegen". Damals wurde es nicht gemacht.

Der Präsident Russlands B. Jelzin hat im seinem Erlass Nr. 2334 vom Dezember 1993 "Über zusätzliche Garantien des Rechts der Bürger auf Information" die Erarbeitung des Entwurfs des - schon russischen - Gesetzes "Über das Recht auf Information" initiiert. Diesmal wurde der Auftrag, zwar etwas später, erfüllt: Der für das

Schicksal der Demokratie in Russland sehr wichtige gesetzgeberische Akt ist erarbeitet und dem Parlament vorgelegt, wo er im September 1997 seine erste Lesung gehabt hat.

Ich möchte betonen, dass die russische Öffentlichkeit die Erarbeitung dieses Gesetzentwurfes ständig aufmerksam verfolgte. Das ist doch eher ein Gesetz der Gesellschaft und nicht des Staates. Verschiedene im Medienbereich tätige Bürgerrechtsorganisationen (Stiftung zum Schutz von Glasnost', Zentrum "Recht und Medien" der Fakultät für Journalistik der Moskauer Lomonosov-Universität) sowie eine Reihe gesellschaftlicher Organisationen, die sich mit ökologischen Problemen und der Herausbildung der Zivilgesellschaft in Russland beschäftigen organisierten unter der Schirmherrschaft der Moskauer Bürgerrechtsstiftung "Kommission für freien Zugang zur Informationen" (MS "KFZI") mehrmals in den letzten fünf Jahren gesellschaftliche Besprechungen, an denen eine breite Öffentlichkeit und ausländische Experten teilnahmen, und andere Veranstaltungen, in denen sowohl das allgemeine Problem des freien Zugangs der Bürger zu gesellschaftlich relevanten Informationen, als auch dieser Gesetzentwurf erörtert wurden.

Mit Ergebnissen dieser verschiedenartigen und schwierigen Tätigkeit russischer Öffentlichkeit für die grundsätzliche Reformierung des ganzen Systems der Informationsverhältnisse zwischen der russischen Macht, der russischen Gesellschaft und dem Bürger kann man sich in 30 Heften des Bulletins der MS "KFZI" "Das Recht, zu wissen", die in den vergangenen Jahren erschienen, bekannt machen. Diejenigen, die ausführlichere Informationen brauchen, können sie in vier Sammelbänden der Beiträge und Dokumente finden, die in denselben Jahren, betreut von der MS "KFZI", veröffentlicht wurden. Ihre Titel sind selbstredend:

- "Russische Journalistik: freier Zugang zur Information";
- "Freier Zugang zur Information in Russland: rechtliche, organisatorische und professionelle Probleme";
- "Aufsicht der Zivilgesellschaft über informationelle Transparenz der Macht: Theorie und Praxis";
- "Das Recht zu wissen. Russische und internationale Erfahrung der rechtlichen Regelung des Zugang der Bürger zu Regierungsinformationen".

Seit dem November 1998 ist eine Arbeitsgruppe in der Staatsduma der Föderalversammlung der Russischen Föderation tätig, die aus einigen Experten (ich bin auch einer von ihnen - V. M.) und zwei Abgeordneten, J. M. Nesterov und V. N. Lopatin, besteht und den vorliegenden Gesetzentwurf zur zweiten Lesung vorbereiten soll.

Die Hauptrichtung der Vorbereitung ist die Ausstattung des Gesetzentwurfes mit dem möglichst wirkungsvollen Mechanismus der Verwirklichung seiner immer noch (in der Version der ersten Lesung) etwas deklarativen Regelungen. Deswegen mussten wir auch den Titel des Gesetzentwurfes verändern. Anstatt des gewünschten, aber noch nicht erreichten Rechts aus Information ("Über das Recht auf Information") geht es jetzt um das bescheidenere und engere Recht auf Zugang zur Information ("Über das Recht auf Zugang zur Information"). Damit haben wir den Titel in Übereinstimmung mit dem realen Inhalt des Gesetzentwurfes gebracht. Im Gesetz werden doch Verhältnisse hinsichtlich nur der zwei ersten von fünf Informationsrechten behandelt, die in der verfassungsmäßigen Regelung Art. 29 Abs. 4 verbrieft sind, d.h. die Rechte, "Informationen auf jedwede legitime Weise ... zu suchen und zu erhalten".

Der juristische Hauptbestandteil der zur zweiten Lesung vorbereiteten Version des Gesetzentwurfes besteht darin, dass ein solcher organisatorisch-rechtlicher Zugangsmechanismus in ihr verbrieft ist, der, wie wir glauben, es ermöglicht, auf dem Territorium Russlands das Recht *eines jeden* wirklich real zu gewährleisten, die allen zugängliche (d.h. ohne jedwede Beschränkungskategorien) Information, die im Umlauf und in der Zuständigkeit der Staatsmachtorgane, anderer mit Staatsmachtfunktionen bevollmächtigten Strukturen, Organe der lokalen Selbstverwaltung und ihrer Amtspersonen ist, frei zu suchen und zu erhalten.

Die Verabschiedung dieses Gesetzes vom russischen Parlament sicherzustellen, ist gar nicht einfach: Dieses Gesetz soll das Problem der informationellen Transparenz der Tätigkeit der Staatsmachtorgane, Organe der lokalen Selbstverwaltung und ihrer Amtspersonen zum ersten Mal in unserer Geschichte wirklich systematisch, ausführlich und wirkungsvoll lösen. Unsere zahlreiche Beamten-schaft versteht ja die Gefahr solcher Transparenz für ihre eigenen amtlichen oder gar eigennützigen Interessen ganz gut. Und ihre

Befürchtungen sind nicht unbegründet: Der Sonnenschein der informierten Gesellschaft kann sowohl den Rost der Korruption, als auch den Schimmel der Inkompetenz in der Tätigkeit der Staatsmacht und Selbstverwaltung wirkungsvoll bekämpfen. Wie Sie wohl verstehen, ist das nicht für alle wünschenswert. Deswegen gibt es in Russland noch genug Gegner der gesetzgeberischen Verbriefung der wirkungsvollen Regelungen der gesellschaftlichen und staatlichen Transparenz, und ihre widerstrebenden Bemühungen sind leider manchmal erfolgreich. Deshalb ist das Schicksal unseres Gesetzentwurfes nach wie vor schwierig. Aber wir, Autoren und Anhänger dieses Gesetzes, geben nicht auf und glauben, dass wir den Sieg erringen.

## **2.2 Private Information als Gegenstand des Rechtsschutzes**

Die Praxis der gesetzgeberischen Regelung der Verwirklichung eines anderen Informationsrechts des Bürgers, d.h. des Rechts auf die Vertraulichkeit der Informationen über sein Privatleben, entwickelt sich in Russland bis jetzt mit einer gewissen Verzögerung, auch im Vergleich mit der Praxis der Verwirklichung seines Rechts auf Information.

Ich glaube, dass der Grund dieser Verzögerung gar nicht im rechtlichen Bereich zu finden ist. Eher im sozialpsychologischen. Es geht darum, dass die Achtung und Hochschätzung des Wertes, welcher unter dem Begriff "privates und familiäres Geheimnis oder Geheimnis des Privatlebens" verstanden wird, im genetischen Gedächtnis der Russen fehlen, was durch bestimmte historische Bedingungen zu erklären ist.

Das Verhalten gegenüber dem Staatsgeheimnis ist etwas anders. Zwar fehlt auch hier die wirkliche Achtung, aber das Verständnis, dass das Staatsgeheimnis ernsthaft und bedeutend ist, gibt es im Volksbewusstsein bestimmt. Fast dasselbe Verhalten ist gegenüber dem sogenannten Dienstgeheimnis, das manchmal als "Amtszimmergeheimnis" bezeichnet wird, zu beobachten.

Das Recht auf Privatleben selbst und dementsprechend das Recht auf den Schutz seines informationellen Bestandteils ist ein sehr

junges Institut im russischen Rechtssystem. Deswegen sind die Rechte, aus denen dieses Rechtsinstitut besteht, für viele russische Bürger sozusagen exotisch, sie sind, philosophisch definiert, "das Ding an sich", und nicht "das Ding für sich".

Gleichzeitig muss man doch zugeben, dass sich der Prozess der Aneignung der entsprechenden Verteidigungs- und Schutzrechte durch die russische Gesellschaft und den russischen Staat intensiv entwickelt, darunter auch auf dem verfassungsrechtlichen Niveau. Es werden einige aufsehenerregende Strafsachen untersucht, die den Schutz des Privatlebensgeheimnisses mit strafrechtlichen Mitteln betreffen. Das Verfassungsgericht Russlands hat sich schon mehrmals mit dem Problemkreis "Verteidigung und Schutz der persönlichen Information" auseinandergesetzt. Eine bestimmte Rolle für die Entwicklung und den Schutz dieses Rechts und anderer Informationsrechte der Bürger spielt auch die sechs Jahre lange Tätigkeit der Kammer des Informationsgerichtes beim Präsidenten Russlands. Das ist ein eigenartiges Organ der russischen Verwaltungsjustiz, so etwas wie ein kollektiver Ombudsmann im Bereich der öffentlichen Informationsrechtsverhältnisse<sup>13</sup>. Deshalb erlaube ich mir, meine feste Überzeugung auszudrücken, dass das Rechtsinstitut des Schutzes der persönlichen Information in Russland sich unbedingt herausbilden und entwickeln wird.

Die verfassungsrechtliche Basis dieses Instituts bilden die Regelungen des Artikels 23 der Verfassung Russlands: "Jeder hat das Recht auf Unverletzlichkeit des Privatlebens, auf privates und familiäres Geheimnis, auf Schutz seiner Ehre und seines guten Rufes" und "jeder hat das Recht auf die Vertraulichkeit seiner Korrespondenz, Telefongespräche, postalischen, telegrafischen und anderen Mitteilungen. Die Beschränkung dieses Rechts ist nur auf Grund eines Gerichtsbeschlusses zulässig". Dazu gehört auch das verfassungsmäßige Verbot des "Sammelns, der Aufbewahrung, Nutzung und Verbreitung der Information über das Privatleben einer Person ohne ihre Genehmigung", das im Art. 24 Abs. 1 der Verfassung verbrieft ist.

---

<sup>13</sup> Siehe: Монахов В.Н. Информационные права граждан: опыт защиты и развития. В сб.: Право граждан на информацию и защита неприкосновенности частной жизни, ч. 1. Нижний Новгород, 1999, с. 50-61

Seine weitere Entwicklung erhält dieses verfassungsrechtliche Institut in Regelungen verschiedener russischer gesetzgeberischer Maßnahmen der letzten Zeit. So haben die Artikel 2 und 11 des Föderalgesetzes "Über Information, Informatisierung und Informationsschutz" von 1995 zum ersten Mal eine neue Rechtskategorie - persönliche Daten (PD) - in die russische Gesetzgebung eingeführt. Im Sinne dieses Gesetzes werden "Informationen über Bürger (persönliche Daten)" als "Daten zu Tatsachen, Ereignissen und Umständen des Lebens eines Bürgers" verstanden, "die es ermöglichen, seine Persönlichkeit zu identifizieren".

Das Problem des Schutzes der PD wird auch in Russland allmählich aktuell. Einige Dateien, zum Beispiel, die früher geschlossenen Telefonbücher mit Adressenangaben, die Dateien verschiedener Geheimdienste, werden in den letzten Jahren aktiv und aufsichtslos kommerziell und sogar politisch (als kompromittierendes Material!) benutzt. Immer breiter wird auch die nichtsanktionierte kommerzielle Nutzung der Dateien der Versicherungsgesellschaften, Notariate und Kreditinstitute. Andere Dateien (zum Beispiel über Wohnungseigentümer und -besitzer) werden in einigen Großstädten Russlands von Kriminellen aktiv benutzt.

Unter solchen Umständen ist es - sogar für die Machthaber - problematisch, das eigene Informationsprofil gegenüber anderen wirkungsvoll persönlich zu kontrollieren. Es ist nämlich damit verbunden, dass die "Informationsspuren" des Lebens der Bürger, welche die Bürger noch vor kurzem meistens anonym in verschiedenen Dienstbereichen (so gibt es zum Beispiel im elektronischen Einwohnerverzeichnis Sankt Petersburgs 44 solche Bereiche: Steuerpolizei, Polizei, Verwaltung für innere Angelegenheiten, Rentenfonds, Komitee für Wohnraum, Arbeitsamt u.ä.) hinterließen, jetzt eine lesbare und kontrollierbare, personifizierte Form erhalten und elektronisch gespeichert werden. Deswegen kann man die Daten über unser Fernseh- und Videomenü am Tage und in der Nacht, über unsere Wahl der Bücher in der Bibliothek, über Zeitungen und Zeitschriften, die wir abonnieren oder in elektronischer Form erhalten, über Dateieninhalt in unseren Personalcomputern und Anrufbeantwortern und viele andere Daten technisch leicht zusammenbringen, klassifizieren, analysieren und interpretieren, so dass der Bürger

nach allen diesen Manipulationen wirklich "transparent", ja "gläsern" wird.

Natürlich versucht das Rechtssystem Russlands möglichst adäquat auf diese Herausforderungen der heutigen Zeit zu reagieren. So ist das Föderalgesetz "Über individuelle (personifizierte) Registrierung im System der staatlichen Rentenversicherung" verabschiedet und seit dem 1.01.1997 gültig. Am 1.01.1999 ist das Föderalgesetz "Über staatliche daktiloskopische Registrierung in der Russischen Föderation" in Kraft getreten. Als seine Fortsetzung hat die Regierung der Russischen Föderation das "Verzeichnis der Dienststellen, welche die Bürger der Russischen Föderation bekleiden, die der staatlichen daktiloskopischen *Pflicht*registrierung unterliegen" in ihrem Beschluss Nr. 386 vom 6.04.1999 festgelegt. Im Beschluss der Regierung der RF Nr. 226 vom 28.02.96 ist "Die provisorische Verordnung über die staatliche Registrierung und Legitimierung der Dateien und Datenbanken" verbrieft.

Das Ministerium für Arbeit und soziale Entwicklung Russlands hat vor, das nationale Register der Bevölkerung bis zum Jahr 2001 zusammenzustellen und jedem Bürger eine Sozialversicherungsnummer zuzuteilen. Die entsprechende gesetzgeberische Basis für dieses Projekt muss zwischen dem Ende des Jahres 1999 und der ersten Hälfte 2000 geschaffen werden.

Der Beschluss der Regierung der Russischen Föderation vom 10.03.1999 "Über die Führung der allgemeinen staatlichen Steuerzahlerliste" hat die Regeln der Führung dieses Registers sowie das "Verzeichnis der Pflichtangaben, die den Finanzämter für die Führung der allgemeinen staatlichen Steuerzahlerliste vorzulegen sind" festgelegt.

Die geltende russische Gesetzgebung sieht auch bestimmte Arten juristischer Verantwortung für jeweilige Rechtsverletzungen im Bereich des Schutzes PD vor. Dafür werden meistens die Mechanismen der zivil-, straf- und verwaltungsrechtlichen Verantwortlichkeit verwendet. So sehen die Artikel 150, 151 und 152 des Zivilgesetzbuches der RF den Schutz der nichtmateriellen Güter der Bürger, einschließlich der Unverletzlichkeit des Privatlebens, des privaten und familiären Geheimnisses und des guten Rufes vor.

Der diesen Gütern zugefügte Schaden wird als moralischer Schaden bezeichnet und kann sowohl durch eine Geldentschädigung (Art. 151, 1099-1101 des Zivilgesetzbuches), als auch auf dem Gerichtswege durch den Widerruf der Angaben, deren Verbreitung den Schaden gebracht hat (Art. 152 des Zivilgesetzbuches der RF) ausgeglichen werden.

Die Artikel 137, 138 und 155 des Strafgesetzbuches der RF bestimmen die strafrechtliche Verantwortlichkeit für folgende Tatbestände:

- ungesetzliches Sammeln und Verbreiten von Daten über das Privatleben einer Person (private oder familiäre Geheimnisse) ohne deren Genehmigung;
- Verletzung des Geheimnisses von Korrespondenz, Telefongesprächen, postalischen, telegrafischen und anderen Mitteilungen;
- Verletzung des Adoptionsgeheimnisses gegen den Willen des Adoptierenden durch eine Person, welche die Tatsache der Adoption als Dienstgeheimnis zu behandeln hat, oder durch eine andere, aus eigennützigen oder anderen niederen Beweggründen handelnde Person.

Das seit dem 1.01.1997 gültige Strafgesetzbuch der RF enthält ein ganzes Kapitel mit Novellen, die mit Verbrechen im Bereich der Computerinformation verbunden sind. Darunter auch den Artikel 272 "Widerrechtlicher Zugang zur Computerinformation". Gemäß den Regelungen dieses Artikels ist es jetzt möglich, für den widerrechtlichen Zugang zu der gesetzlich geschützten Computerinformation, darunter für deren Kopieren, harte Strafmaßnahmen (Freiheitsstrafe bis fünf Jahren) anzuwenden.

Der Kodex der RSFSR "Über verwaltungsrechtliche Rechtsverletzungen" wurde im April 1995 durch einen neuen Artikel, den Artikel 40 (mit Kennzeichen 3), ergänzt, der die Verantwortung in Form einer Geldstrafe für die Verbreitung falscher Informationen, darunter privater Informationen, über einen Bewerber um eine Abgeordnetenstelle oder ein Wahlamt zum Zweck der Einflussnahme auf das Wahlergebnis vorsieht.

Dieses sich in der russischen Gesellschaft sowie auch im russischen Staat herausbildende soziale Bedürfnis nach der allgemeineren und allseitigen gesetzgeberischen Regelung der komplizierten und für die russische Rechtswissenschaft neuen Probleme der Verteidigung und des Schutzes privater Information bestimmt gleichzeitig die Notwendigkeit der weiteren Entwicklung der russischen Gesetzgebung in diesem Bereich.

Diesem Bedürfnis entsprechen einige Entwürfe der Föderalgesetze über persönliche Daten. Zwei davon sind besonders bekannt. Der erste Gesetzentwurf "Über persönliche Daten", der von der Initiativegruppe mit dem ehemaligen verantwortlichen Mitarbeiter des Sicherheitsrates der RF A. P. Kurilo an der Spitze erarbeitet wurde, wurde leider der Staatsduma offiziell nicht vorgelegt. Der zweite Gesetzentwurf, der Entwurf des Föderalgesetzes "Über private Information", wurde von Abgeordneten O. A. Fin'ko, J. M. Nesterov, G. K. Volkov, R. G. Gabidullin und V. S. Coj, welche Mitglieder des Staatsdumakomitees für Informationspolitik und Meldewesen sind, der Staatsduma als gesetzgeberische Initiative im April 1998 vorgelegt.

Der erste Gesetzentwurf wurde länger, sorgfältiger und offener vorbereitet. Die Arbeitsgruppe hat ihn mehrmals der Öffentlichkeit in beiden russischen Hauptstädten für die Besprechung vorgelegt. Übrigens hatte dieselbe Arbeitsgruppe 1996 den gesetzgeberischen Empfehlungsakt für die Gemeinschaft der Unabhängigen Staaten (GUS), das Rahmengesetz "Über persönliche Daten" erarbeitet, das in der Besprechung im Expertenrat des Sicherheitskomitees der Staatsduma erfolgreich genehmigt wurde.

Die ausführliche juristische Beschreibung dieser Gesetzentwürfe wäre hier nicht angemessen. Kurz könnten sie wie folgt beurteilt werden: Die von der internationalen, und in erster Linie, von der europäischen Rechtswissenschaft erarbeiteten grundlegenden Prinzipien der Verteidigung der PD sind in diese Gesetzentwürfe einbezogen worden. Zugleich fehlen dort die Definitionen der konkreten Regelungen, welche den arbeitsfähigen Mechanismus der Verwirklichung deklarativer Prinzipien in realen Handlungen der Menschen und Gemeinschaften schaffen und in Gang setzen sollen. Nur ein Beispiel dafür: In beiden Gesetzentwürfen fehlen die Regelungen, welche die Spezifik der PD-Behandlung durch solche

"Informationsfabriken" wie Massenmedien bestimmen. Dabei zeugt die neue russische sowie internationale, und in erster Linie deutsche Erfahrung davon, dass es diese Spezifik gibt und dass sie sowohl im Medienrecht als auch im Recht der elektronischen Datenbearbeitung berücksichtigt werden muss. Ich glaube, das Modell der rechtlichen Regelung der PD-Behandlung durch Massenmedien Deutschlands könnte auch in Russland angewandt werden. Das Wesen dieses Modells ist die harmonische Vereinigung der grundlegenden Forderungen des Bundesdatenschutzgesetzes (§§ 41 - 42) und der entsprechenden Regelungen der Rechtsakte, welche die Tätigkeit der elektronischen Presse Deutschlands regeln. Zum Beispiel, der Regelungen des § 47 "Datenschutz" des Rundfunkstaatsvertrags in der Fassung von 1997.

Jedenfalls muss die Erfahrung Deutschlands, das bekanntlich der Bahnbrecher auf dem Gebiet der rechtlichen Regelung der Verhältnisse im Bereich der PD ist, meiner Meinung nach von russischen Gesetzgebern aufmerksam erforscht und bei der Beratung des Föderalgesetzes "Über private Information" im Jahre 2000 berücksichtigt werden.

Zusammenfassend möchte ich den Kollegen die Formel der, meiner Meinung nach wirkungsvollsten Entwicklung sowie des internationalen als auch des nationalen Informationsrechts zur Besprechung vorlegen. Diese Formel besteht in der optimalen Vereinigung von zwei Hauptformen seiner Entwicklung, Verteidigung und seines Schutzes, d.h. den gesetzgeberischen und gerichtsrechtlichen Formen. Wenn unsere Parlamente, indem sie Gesetze geben, die gerichtsrechtliche "Stimmgabel" ihrer gesetzgeberischen Tätigkeit hören können... Wenn die Verbindung zwischen diesen sozialen Instituten nach dem Prinzip von zwei gut kommunizierenden Röhren verwirklicht wird... In diesem Fall bräuchte man sich um die Entwicklung des Informationsrechts sowie anderer Rechtszweige keine Sorgen zu machen.

Wir kennen ein gutes deutsches Beispiel solchen Zusammenwirkens von zwei grundlegenden rechtsregelnden Strukturen - und zwar ausgerechnet im Bereich der PD. Ich meine den bekannten Rechtspruch des Bundesverfassungsgerichts Deutschlands von 1983, welcher die Doktrin der sogenannten informationellen Selbstbestimmung der Persönlichkeit verankert hat, der später zur Grundlage der

Überarbeitung der deutschen Gesetzgebung über den Schutz der PD geworden ist. Dieses Beispiel erinnert an noch einen Faktor der Entwicklung des Informationsrechts - an die Berücksichtigung der entsprechenden ausländischen Erfahrung. Eine solche Erfahrung muss nicht nur einfach für die Vervollkommnung des eigenen nationalen Rechts berücksichtigt werden, sondern auch für eine solche Vervollkommnung, welche seine Harmonisierung mit anderen nationalen und internationalen, in erster Linie europäischen informationsrechtlichen Systemen ermöglichen könnte.

Russland und Deutschland sind wichtige Informationsglieder sowohl des europäischen, als auch des gesamten internationalen Informationssystems. Dementsprechend steht uns und Ihnen eine schwere Arbeit für die Koordinierung und gegenseitige Adaptierung der nationalen Informations- und Telekommunikationsgesetzgebungen bevor. Wollen wir einander viele Erfolge auf diesem Gebiet wünschen und unsere Erfolge, den bekannten Arithmetikregeln entsprechend, addieren und multiplizieren, aber unsere Misserfolge nur subtrahieren.





Potsdam  
October  
1999

**George Papapavlou  
European Commission,  
DG Information Society**



Public sector information:  
A key resource  
for Europe

GREEN PAPER ON PUBLIC SECTOR INFORMATION  
IN THE INFORMATION SOCIETY

<http://www.echo.lu/legal/en/access.html>



European Commission

Green Paper published  
20 January 1999

Events throughout Europe

Discussions with various  
institutions

Numerous replies

# AGENDA

- 
- ◆ **WHAT IS AT STAKE?**
  - ◆ **IMPORTANCE FOR CITIZENS AND BUSINESS**
  - ◆ **WHY TO DEAL WITH THIS TOPIC NOW?**
  - ◆ **SOME ISSUES TO CONSIDER**
  - ◆ **PRELIMINARY IDEAS FOR EU ACTIONS**
  - ◆ **TIMETABLE**

## **WHAT IS AT STAKE**

- ◆ **Digital content is central to the Information Society development**
- ◆ **Public Sector Information is a prime content resource**
- ◆ **Barriers at European level prevent improved access and better exploitation**

# Shift in Importance of Success Factors in the Multimedia Market

Source:  
Bertelsmann  
multimedia



## **IMPORTANT FOR CITIZENS**

- ◆ **Bringing citizens closer to administrations**
- ◆ **Taking advantage of the Internal Market (free movement, consumers)**
- ◆ **Important in the democratic process**
- ◆ **Adding to the quality of life**

## **IMPORTANT FOR BUSINESS**

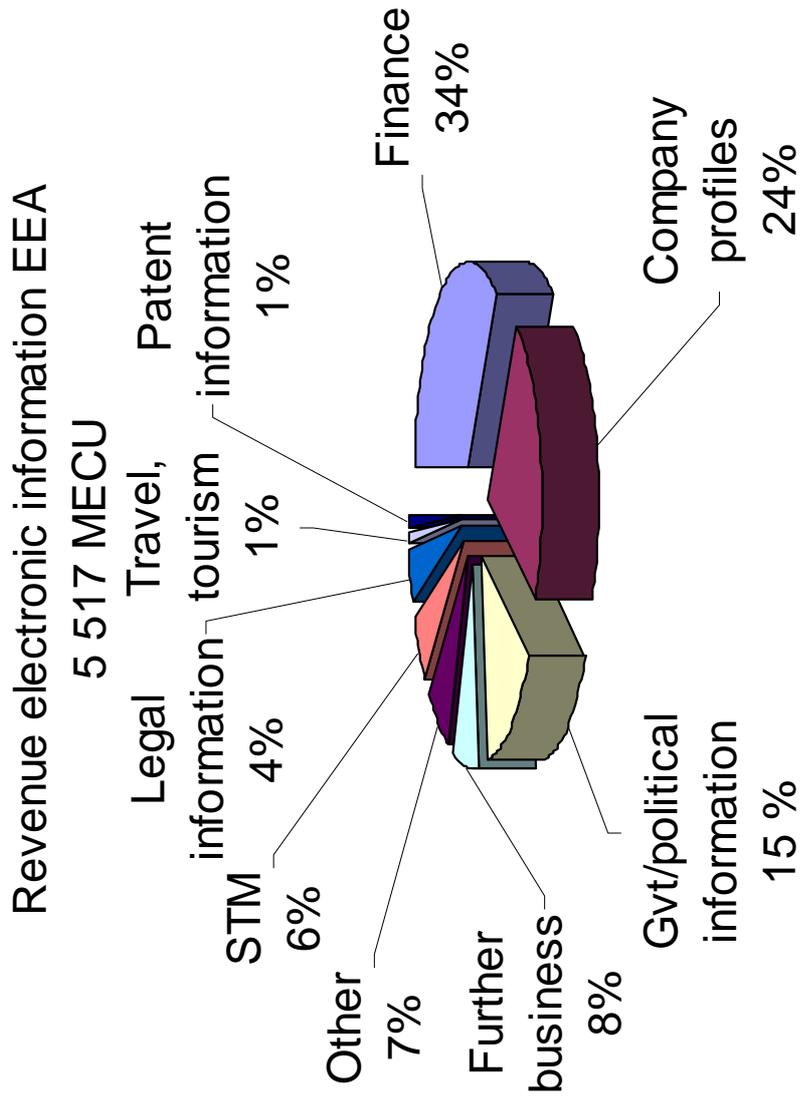
**Important for all firms:**

- ◆ **Essential to make business strategies**
- ◆ **Crucial for taking advantage of the internal market rights**

**And in particular for the content industries:**

- ◆ **Source for new information products (aggregation)**
- ◆ **The digital accessibility of public sector information will boost Internet-use**

# EXTENSIVE POTENTIAL FOR EXPLOITATION



## **EXTENSIVE POTENTIAL FOR EXPLOITATION**

- ◆ **Prime information content for the information industry**
- ◆ **As illustrated through replies to the last INFO2000 call for proposals**
  - ◆ 141 proposals
  - ◆ 20 projects selected
  - ◆ EU funding of ECU 8.6 million
  - ◆ a wide range of activities covered

## **EUROPE IS LAGGING BEHIND THE US**

- ◆ **A comprehensive policy in the US aiming at facilitating access to public sector information and stimulating its commercial exploitation**
- ◆ **European information industry faces difficulties in accessing public sector information (internal market issue)**
- ◆ **Strong competition disadvantages vis-à-vis the US**

## **WHY DEALING WITH THIS TOPIC NOW?**

**The topic is not new in itself, but:**

- ◆ **Digitalisation of content resources**
- ◆ **Electronic Government**
- ◆ **Re-engineering of public services**

# ELECTRONIC GOVERNMENT

- ◆ **Information services**
  - ◆ <http://verkeer.anwb.org/haagland/>
- ◆ **Digital communication**
  - ◆ <http://www.antwerpen.be/stad/admin/meldkt.htm>
  - ◆ <http://www.transparant.net/amsterdam/ta.html>
- ◆ **Digital transaction**
  - ◆ <http://www.groningen.nl/form/verhuizing.htm>

**But: attention to access for all**

## **SOME ISSUES TO CONSIDER**

- ◆ **What do we mean by public sector information ?**
- ◆ **What categories of public sector information should be used in the debate ?**
- ◆ **Do different conditions for access create barriers at European level ?**

## **SOME ISSUES TO CONSIDER**

- ◆ **Practical tools for facilitating access at European level ?**
- ◆ **Pricing issues :**
  - ◆ **A large variety of prices and pricing models**
  - ◆ **Internet will lead to changes**
  - ◆ **A number of interests :**
    - **affordable access for all**
    - **exploitation potential**
    - **fair competition**

## **SOME ISSUES TO CONSIDER**

- ◆ **Competition and copyright issues**
- ◆ **Right to information versus right of privacy:  
How should the balance be struck?**
- ◆ **Liability issues**
- ◆ **Policies of EU institutions**

## **PRELIMINARY IDEAS FOR EU ACTION**

- ◆ **Projects to encourage public and private synergy**
- ◆ **Practical mechanisms to facilitate access**
- ◆ **Platform for co-ordination/exchange of experiences**
- ◆ **Awareness and training initiatives**
- ◆ **Regulatory action**
- ◆ **Other ?...**

## **TIMETABLE**

- ◆ **20 January 1999 - Commission adopts green paper**
- ◆ **January 1999 - June 1999 :**
  - ◆ **discussion by Council, EP, ECOSOC, CoR, ISF**
  - ◆ **replies to the Green paper by all interested parties**
- ◆ **Second half of 1999 - Follow-up communication**

## **GREEN PAPER ON PUBLIC SECTOR INFORMATION**

- ◆ **Bring subject to political agenda**
- ◆ **Focus on potential barriers at European level**
- ◆ **Identify areas of common interest**
- ◆ **Build consensus on need for action**

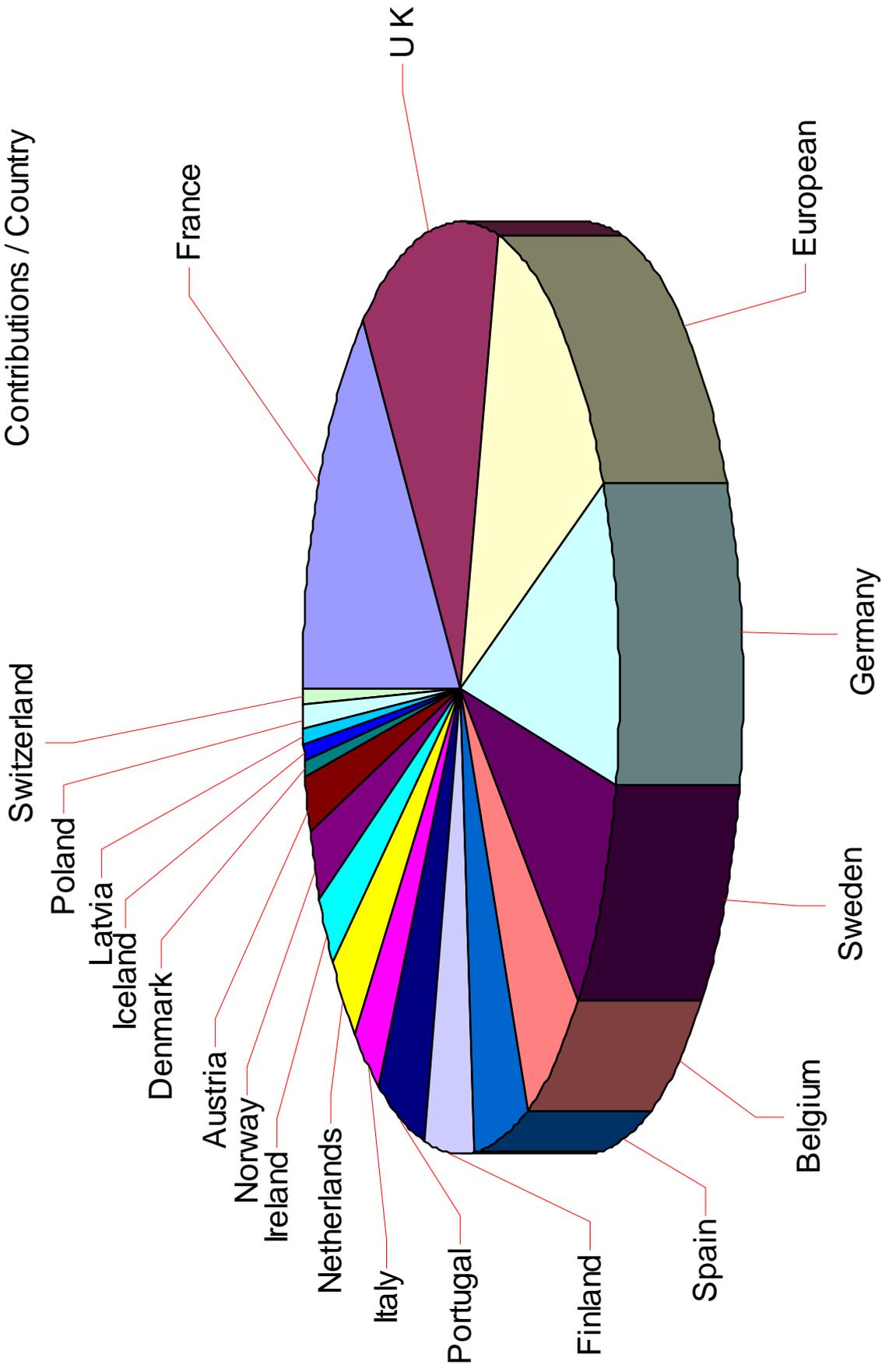
# What the events told us

- Already being debated in many MS
- Interest in the topic
- Strong opinions
- Local solutions, local backgrounds

# The replies

- **180+ replies**
- **Most governments replied**
- **Almost everyone sent electronically**
- **All replies are available for you to see**

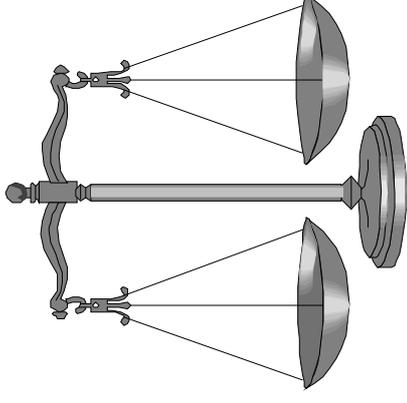
# Green Paper Contributions / Country



# Two very different issues

## ◆ DEMOCRACY

**Citizens have a right to information about their rights and what their governments do**



## ◆ EXPLOITATION

**There is an unrealised potential for using information originating in the public sector**



# **New Commissioner**

“Many replies show that information on experiences and best practices across Europe should be exchanged between all actors concerned. There seems also to be a need to encourage and raise awareness about how to facilitate citizens' access to public sector information in practical terms and in particular through the use of new technologies. Support to demonstration pilot projects should also be pursued.”

***Mr. Liikanen reply to the Parliament, August '99***

## Mr Prodi and the Information Society

**“The key to the future of our Continent is in the hands of hi-tech, knowledge-based industries, at the cutting edge of research.”**

***Mr. Prodi at the EU Parliament, April '99***

# **NOW WHAT?**

## **Possible scenarios for follow-up:**

**Communication on the results of the discussion**

*and/or*

**Follow-up communication with some proposals for action  
at EU level**

*and/or*

**Proposal for a European instrument : general or specific?  
Binding (directive) or not (resolution)**



## **Bettina Sokol**

Landesbeauftragte für den Datenschutz Nordrhein-Westfalen

### **Grundrechtliche Aspekte des Informationszugangs**

In der sich entwickelnden Informationsgesellschaft kommen dem Recht auf informationelle Selbstbestimmung und den Möglichkeiten selbstbestimmter Kommunikation zentrale Bedeutung zu. Voraussetzung ihrer effektiven Wahrnehmung ist es aber auch, sich informieren zu können und beispielsweise Zugang zu den Informationen zu erhalten, über die die Verwaltung verfügt. Demgegenüber richtet sich das Denken in vielen bundesdeutschen Amtsstuben nach wie vor nach dem überkommenen Grundsatz, dass das Handeln der Exekutive generell nicht öffentlich zu sein habe. Das Geheimhaltungsprinzip ist jedoch schon aus rechtsstaatlichen Gründen durchbrochen, um den Schutz individueller Rechte zu gewährleisten. In eigenen Angelegenheiten existieren daher unterschiedlich umfassende Auskunfts- und Akteneinsichtsrechte.<sup>1</sup> Die Transparenz der Datenverarbeitung gegenüber den von ihr Betroffenen gehört zu den wesentlichen verfahrensrechtlichen Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung.<sup>2</sup> So ist es etwa ständige Rechtsprechung des Bundesverfassungsgerichts, dass den Bürgerinnen und Bürgern aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG grundsätzlich ein Anspruch auf Einsicht in Unterlagen zusteht, die sie selbst betreffen.<sup>3</sup> Dies gilt auch im Rahmen konkreter Verwaltungsverfahren. Allein die selbst am Verfahren Beteiligten besitzen allerdings ein Recht auf Informationszugang, und zwar nur, soweit sie die Kenntnis der Akten zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen benötigen.<sup>4</sup> Auch bereichsspezifische Partizipationsmöglichkeiten – wie sie etwa das Planungsrecht vorsieht – ändern an diesem Grundsatz nichts, da sie ebenfalls eine eigene Betroffenheit voraussetzen. Gleichwohl ist es einer Behörde aber nicht verwehrt,

---

<sup>1</sup> Z.B. § 102 c Abs. 1 LBG NW, § 14 VSG NW, § 24 SÜG NW, § 9 Abs. 2 i.V.m. § 2 Abs. 1 Nr. 2 GDSG NW und § 18 DSG NW.

<sup>2</sup> Siehe dazu auch Sokol, Akteneinsicht, Informationszugangsrecht, in: Bäumlner/Breinlinger/Schrader (Hrsg.), Datenschutz von A bis Z, Neuwied 1999, A 800.

<sup>3</sup> Vgl. nur BVerfG (Kammerbeschl. vom 16.09.1998), NJW 1999, 1777.

<sup>4</sup> § 29 VwVfG NW.

auch außerhalb konkreter Rechtsverhältnisse Informationen zu geben.<sup>5</sup> Steht kein gesetzliches Informationsverbot entgegen, hat sie über einen Informationswunsch nach pflichtgemäßem Ermessen zu entscheiden und dabei alle maßgeblichen Umstände zu berücksichtigen.<sup>6</sup>

Ein allgemeiner Informationszugangsanspruch wird auf Bundesebene bislang lediglich im Umweltbereich durch das Umweltinformationsgesetz<sup>7</sup> gewährt, zu dessen Erlass Deutschland gemeinschaftsrechtlich verpflichtet war in Umsetzung der EG-Richtlinie 90/313 über den freien Zugang zu Informationen über die Umwelt. Die Richtlinie ist mit dem Umweltinformationsgesetz allerdings nicht ordnungsgemäß, sondern nur unzureichend umgesetzt worden. Nachdem der Europäische Gerichtshof im Juni 1998 bereits entschieden hatte, wie nach der Richtlinie der Begriff des "Vorverfahrens" zu verstehen ist<sup>8</sup>, hat er in dem von der Kommission angestrebten Verfahren gegen Deutschland unter anderem bestätigend festgestellt<sup>9</sup>, dass der im Umweltinformationsgesetz vorgesehene vollständige Ausschluss des "verwaltungsbehördlichen Verfahrens" vom Informationszugang über die nach der Richtlinie zugelassenen Ausnahmen hinausgeht und Deutschland damit gegen seine gemeinschaftsrechtliche Verpflichtung verstoßen hat.

Bei der Prüfung, ob bereits das Grundgesetz ein über den Umweltbereich hinausreichendes, allgemeines Informationszugangsrecht enthalten könnte, fällt der Blick zunächst auf Art. 5 Abs. 1 GG. "Indem Art. 5 Abs. 1 GG Meinungsäußerungs-, Meinungsverbreitungs- und Informationsfreiheit als Menschenrechte gewährleistet, sucht er zugleich diesen Prozess verfassungsrechtlich zu schützen. Er begründet insoweit subjektive Rechte; im Zusammenhang damit normiert er die Meinungsfreiheit als objektives Prinzip der Gesamtrechtsordnung, wobei subjektiv- und objektiv-rechtliche Elemente

---

<sup>5</sup> Vgl. VG Gießen, GW EzDat 1993, D 11, § 29 VwVfG Nr. 4.

<sup>6</sup> Vgl. BVerwGE 84, 375/386 f.

<sup>7</sup> UIG vom 08.07.1994, BGBl. I, 1490.

<sup>8</sup> EuGH, Urt. vom 17.06.1998, NVwZ 1998, 945.

<sup>9</sup> EuGH, Urt. vom 09.09.1999, NVwZ 1999, 1209.

einander bedingen und stützen".<sup>10</sup> Das Grundrecht der Informationsfreiheit ist seinem Wortlaut nach allerdings ausdrücklich begrenzt auf "allgemein zugängliche Quellen". Akten, Unterlagen, Dokumente und sonstige Materialien der Verwaltungen werden gerade nicht als allgemein zugängliche Quellen angesehen<sup>11</sup>, so dass Art. 5 Abs. 1 GG kein subjektives Recht auf Zugang zu Verwaltungsunterlagen entnommen werden kann. Gleiches gilt im Übrigen für die Art. 5 Abs. 1 GG entsprechenden landesverfassungsrechtlichen Bestimmungen. Subjektive Auskunftsrechte speziell über Umweltdaten normieren zwar die Landesverfassungen von Sachsen<sup>12</sup> sowie Sachsen-Anhalt<sup>13</sup> und in Mecklenburg-Vorpommern<sup>14</sup> gibt es ein landesverfassungsrechtliches Zugangsrecht zu Informationen über die Umwelt, ein allgemeines Einsichtsrecht in Akten und sonstige amtliche Unterlagen der Behörden und Verwaltungseinrichtungen hat aber lediglich Brandenburg<sup>15</sup> verfassungsrechtlich verankert.

Die fundamentale Bedeutung, die das Bundesverfassungsgericht der Informationsfreiheit für eine funktionierende Demokratie und deren politischen Meinungs- und Willensbildungsprozess beimisst<sup>16</sup>, sowie der Kommunikationsbezug, den auch Grundrechte wie etwa die Versammlungs- und die Vereinigungsfreiheit besitzen, können gleichwohl herangezogen werden, um die Notwendigkeit eines Informationszugangsgesetzes zu untermauern. Im Übrigen ist im Koalitionsvertrag der rot-grünen Bundesregierung der Erlass eines solchen Gesetzes festgelegt. Auf Landesebene hat Brandenburg als erstes der deutschen Länder 1998 ein Akteneinsichts- und Informationszugangsgesetz<sup>17</sup> erlassen; Berlin ist 1999 mit einem Informationsfreiheitsgesetz<sup>18</sup> gefolgt.

---

<sup>10</sup> BVerfGE 57, 295/319 f.; vgl. z.B. auch BVerfGE 74, 297/323 und 83, 238/296; aus der objektiv-rechtlichen Funktion der Grundrechte werden grundrechtsspezifisch unterschiedliche staatliche Pflichten abgeleitet, wie etwa gesetzgeberische Regelungs- und Ausgestaltungspflichten, beispielsweise im Hinblick auf Organisations- und Verfahrensgestaltung, aber auch Schutzpflichten sowie Leistungs- und Teilhaberechte.

<sup>11</sup> Vgl. BVerfG (Kammerbeschl. vom 30.01.1986), NJW 1986, 1243.

<sup>12</sup> Art. 34 Verfassung des Freistaates Sachsen.

<sup>13</sup> Art. 6 Abs. 2 Verfassung des Landes Sachsen-Anhalt.

<sup>14</sup> Art. 6 Abs. 3 Verfassung des Landes Mecklenburg-Vorpommern.

<sup>15</sup> Art. 21 Abs. 4 Verfassung des Landes Brandenburg.

<sup>16</sup> Vgl. z.B. BVerfGE 20, 162/174 ff.

<sup>17</sup> AIG vom 10.03.1998, Bbg GVBl. I, 46.

<sup>18</sup> IFG vom 15.10.1999, Bl. GVBl., 561.

In diesem Zusammenhang darf auch eine Entscheidung des Europäischen Gerichtshofs für Menschenrechte (EGMR) aus dem Jahre 1998<sup>19</sup> nicht unerwähnt bleiben. In dem zu entscheidenden Fall ging es darum, dass italienische Behörden es unterlassen hatten, die Bevölkerung nach der Seveso-Richtlinie der Europäischen Gemeinschaft über Gefahren industrieller Aktivitäten, über ergriffene Sicherheitsvorkehrungen, über Notfallmaßnahmen usw. zu informieren. Der EGMR lehnte die Anwendbarkeit der in Art. 10 EMRK verankerten Informationsfreiheit zwar ab, bejahte überraschenderweise jedoch eine Verletzung von Art. 8 EMRK, der den Anspruch auf Achtung der Privat- und Familiensphäre, der Wohnung und des Briefverkehrs normiert. Der EGMR sah – ohne dies für den vorliegenden Fall abschließend entscheiden zu müssen – über die abwehrrechtliche Funktion dieses Menschenrechts hinaus die Möglichkeit, dass auch positive staatliche Verpflichtungen zum wirkungsvollen Schutz des Privat- und Familienlebens darin enthalten sein können. Schwerwiegende Umweltverschmutzung könne das Wohlergehen von Individuen beeinflussen und sie am Genuss ihres häuslichen Lebens derart hindern, dass ihr Privat- und Familienleben beeinträchtigt werde. Dadurch, dass der Staat der Bevölkerung nicht die notwendigen Informationen gegeben habe, die die Risiken eines weiteren Verbleibs an dem betroffenen Wohnort hätten abschätzbar werden lassen, habe er gegen Art. 8 EMRK verstoßen.

Die Entscheidung ist interessant. In der Bundesrepublik Deutschland wäre ihr Gegenstand vermutlich der grundrechtliche Schutz von Leben und Gesundheit und die daraus abzuleitenden staatlichen Schutzpflichten gewesen. Gleichwohl ist es umso anregender, einmal darüber nachzudenken, welche Bedeutung einem solchen Ansatz für das Recht auf informationelle Selbstbestimmung zukommen könnte, zu dessen Bestandteil ja ebenfalls der Schutz der Privatheit zählt.

Für das allgemeine Persönlichkeitsrecht, das – wie das Recht auf informationelle Selbstbestimmung – ebenfalls Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG entnommen wird, hat das Bundesverfassungsgericht schon seit langer Zeit eine staatliche Schutzpflicht anerkannt: "Auch das allgemeine Persönlichkeitsrecht entfaltet direkte Wirkung nur gegenüber dem Staat. Dieser ist aber grundrechtlich gehalten, den

---

<sup>19</sup> EGMR, Urt. vom 19.02.1998, NVwZ 1999, 57.

Einzelnen vor Persönlichkeitsgefährdungen durch Dritte zu schützen."<sup>20</sup>

Vorliegend ist nicht von Bedeutung, ob sich die objektiv-rechtliche Grundrechtskomponente des Rechts auf informationelle Selbstbestimmung als staatliche Schutzpflicht oder als Ausstrahlungswirkung realisiert, im Ergebnis ist entscheidend, dass staatliches Handeln geboten ist, um das Selbstbestimmungsrecht durch Informationsansprüche zu stärken, die zugleich unter anderem eine der Voraussetzungen für eine effektive Wahrnehmung des Rechts auf informationelle Selbstbestimmung bilden. Das Bundesverfassungsgericht benennt die informationelle Selbstbestimmung als eine elementare Funktionsbedingung "eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens".<sup>21</sup> Ein wesentliches Ziel des Rechts auf informationelle Selbstbestimmung besteht daher darin, die Kommunikations- und Handlungsfähigkeit der einzelnen Menschen gegenüber staatlichen Stellen wie auch innerhalb der Gesellschaft sicherzustellen. Wird das Recht auf informationelle Selbstbestimmung nicht auf seine abwehrrechtliche Funktion im Sinne eines als bloßer Geheimhaltungsschutz missverstandenen Datenschutzes begriffen, wird deutlich, dass Informationszugangsrechte und Datenschutz im Grunde genommen die Gemeinsamkeit besitzen, staatlicher Informationsmacht Grenzen zu setzen. Gleichwohl kann es konkrete Einzelfälle geben, in denen auch personenbezogene Daten zum Gegenstand des Informationsinteresses werden. Hier gilt es, die konfligierenden Interessen zum schonenden Ausgleich zu bringen.

Die beiden ersten Landesgesetze, mit denen allgemeine Informationszugangsrechte normiert werden, unterscheiden sich gleichwohl in einigen Punkten. So verzichtet das brandenburgische Gesetz darauf, einen Zweck zu definieren, wohingegen die Berliner Regelung in ihrem § 1 insoweit die Förderung der demokratischen Meinungs- und Willensbildung sowie die Ermöglichung einer Kontrolle des staatlichen Handelns benennt. Der gegenüber dem Berliner Gesetz schmalere Anwendungsbereich des brandenburgischen

---

<sup>20</sup> BVerfG, Beschl. vom 10.11.1998, NJW 1999, 1322/1323 unter Bezug auf BVerfGE 73, 118/201 und 97, 125/146.

<sup>21</sup> BVerfGE 65, 1/43.

Gesetzes<sup>22</sup> sowie der – nicht nur allein von der Textlänge her – umfangreiche Katalog von "überwiegenden öffentlichen Interessen"<sup>23</sup>, bei deren Vorliegen Akteneinsichtsansprüche abzulehnen sind oder abgelehnt werden sollen, sind neben anderen Punkten auch schon im Gesetzgebungsverfahren<sup>24</sup> kritisiert worden.

Nur als Beispiel sei § 4 Abs. 2 Nr. 4 AIG benannt, nach dem ein Akteneinsichtsanspruch vorbehaltlich des Ergebnisses einer sich anschließenden Abwägung abgelehnt werden soll, wenn die ordnungsgemäße Erfüllung der Aufgaben der öffentlichen Stelle erheblich beeinträchtigt würde. Diese Bestimmung offenbart ein Verständnis von Verwaltungsaufgaben, das sich im Widerspruch zum Gesetz selber befindet. Mit dem Akteneinsichts- und Informationszugangsgesetz hat der Landesgesetzgeber der Verwaltung die Pflicht auferlegt, grundsätzlich Akteneinsicht zu gewähren. Das herkömmliche, eingangs genannte Regel-Ausnahme-Verhältnis wurde also gerade umgekehrt. Damit gehört die Akteneinsichtsgewährung zu den Aufgaben der jeweiligen öffentlichen Stelle. Undenkbar wäre etwa als Vergleich ein ablehnender Wohngeldbescheid der zuständigen Stelle mit der Begründung, eine positive Bescheidung hätte die ordnungsgemäße Aufgabenerfüllung erheblich beeinträchtigt. Sich der Aufgabenerfüllung durch die Berufung auf deren erhebliche Beeinträchtigung entziehen zu können, lässt die dahinter stehende unzeitgemäße Differenzierung erkennen zwischen vermeintlich eigentlichen Aufgaben und eher lästigen Zusatzdienstleistungen, die unzutreffend nicht als originäre Verwaltungsaufgaben betrachtet werden.

Im Hinblick auf den Schutz personenbezogener Daten<sup>25</sup> bleibt auf Grund der Verwendung von unbestimmten Rechtsbegriffen und Abwägungsklauseln erst einmal abzuwarten, wie die Anwendungspraxis die Gesetze mit Leben füllt. Hier ist insbesondere von Interesse, welches der unterschiedlichen Konzepte sich als der gelungenerer Ausgleich von Datenschutz- und Informationsinteresse erwei-

---

<sup>22</sup> Siehe § 2 AIG und § 2 IFG.

<sup>23</sup> § 4 AIG.

<sup>24</sup> Die Anhörung am 11.12.1997 ist dokumentiert in: Ausschussprotokoll 2/902-I vom 19.12.1997 des Ausschusses für Inneres des Landtages Brandenburg; dort findet sich auch die zugespitzte Formulierung, bei dem vorgesehenen Gesetz handle es sich eher um ein Akteneinsichtsverhinderungsgesetz.

<sup>25</sup> Siehe § 5 Abs. 2, 3 AIG; § 6 IFG.

sen wird. Da die jeweiligen Landesbeauftragten für den Datenschutz in Brandenburg und Berlin mit den Informationszugangsgesetzen zugleich auch die Aufgabe von Beauftragten für das Recht auf Akteneinsicht<sup>26</sup> übertragen bekommen haben, haben sie auch die Möglichkeit, bei der Gesetzesanwendung in der Praxis auf den schonendsten Ausgleich von Datenschutz- und Informationsinteresse hinzuwirken. Die gesetzlich vorgesehenen jährlichen Berichte<sup>27</sup> können sogar in gewissem Rahmen eine – nicht repräsentative – Gesetzesevaluation leisten, mit der zumindest Tendenzen der Praxis deutlich werden können.

Gesetzestechisch etwas missglückt ist im brandenburgischen § 5 Abs. 2 AIG allerdings, dass selbst bei Zustimmung der betroffenen Personen in die Offenbarung der sie betreffenden Daten ein behördliches Ermessen<sup>28</sup> eröffnet wird. Praktische Bedeutung kann diese Möglichkeit der Verweigerung eines Informationszugangs aus Datenschutzgründen trotz Zustimmung der betroffenen Person jedoch kaum erlangen. Denn die der Stelle obliegende pflichtgemäße Ermessensausübung dürfte in aller Regel von einer Ermessensreduzierung auf Null auszugehen haben.

Deutlicher als im brandenburgischen Gesetz, das selbst insoweit keine Aussage trifft, legt in Berlin § 3 Abs. 1 IFG ein Wahlrecht der Antragstellerinnen und Antragsteller bezüglich einer Akteneinsicht oder einer Auskunft fest. Unter Beachtung der Rechtsprechung des Bundesverwaltungsgerichts zur pflichtgemäßen Ermessensausübung bei der Anwendung des Umweltinformationsgesetzes kann in Brandenburg allerdings keine andere Praxis als in Berlin zu erwarten sein. Das Bundesverwaltungsgericht stellt die Bedürfnisse der informationsbegehrenden Personen im Hinblick auf Auskunft oder Akteneinsicht<sup>29</sup> weitest möglich in den Vordergrund. Da es um einen möglichst effektiven Informationszugang geht, kommt ihren "Vorstellungen und Wünschen hinsichtlich der Modalitäten der Informationsaufnahme bei der erforderlichen Ermessensausübung eine besonde-

---

<sup>26</sup> § 11 Abs. 1 AIG; § 18 Abs. 1 IFG.

<sup>27</sup> § 11 Abs. 3 AIG; § 18 Abs. 3 IFG.

<sup>28</sup> Darauf weist zutreffend Partsch, Brandenburgs Akteneinsichts- und Informationszugangsgesetz (AIG) – Vorbild für Deutschland?, NJW 1998, 2559/2562 hin.

<sup>29</sup> Vgl. BVerwGE 102, 282/286 f.

re Bedeutung zu."<sup>30</sup>

Die Schnelligkeitsanforderung, die das Berliner Gesetz für die Antragsbearbeitung mit einer unverzüglichen<sup>31</sup> Entscheidung fordert, die bei Antragsabweisung innerhalb von spätestens zwei Wochen nach Antragstellung<sup>32</sup> zu ergehen hat, lässt das brandenburgische Gesetz bedauerlicherweise vermissen. Können die Personen, denen ein Informationszugang verweigert wurde, in Berlin bereits nach spätestens zwei Wochen Widerspruch einlegen, so besteht in Brandenburg bei zögerlicher Antragsbearbeitung eher das Risiko, dass den Betroffenen nach drei Monaten nur die Erhebung einer Untätigkeitsklage beim Verwaltungsgericht verbleibt.

Die gerichtliche Durchsetzung eines Informationszugangsanspruchs ist ohnehin – noch – mit grundrechtlichen Problemen ganz eigener Art behaftet. Nach Widerspruch und Klageerhebung ergibt sich ein Dilemma: Legt die Behörde die im Streit stehenden Akten dem Gericht vor, wozu sie nach § 99 Abs. 1 Satz 1 VwGO grundsätzlich verpflichtet ist, so ist ihr Inhalt der Klägerin oder dem Kläger im Wege des den Prozessbeteiligten zustehenden Akteneinsichtsrechts zugänglich und der Prozess überflüssig. Beruft sich die zuständige oberste Aufsichtsbehörde auf die im Ausnahmefall nach § 99 Abs. 1 Satz 2 VwGO gegebene Möglichkeit, die Aktenvorlage zu verweigern, so war es dem Gericht bislang nur möglich, die von der Behörde vorgetragene Gründe für die Verweigerung der Akteneinsicht auf ihre Plausibilität zu prüfen.<sup>33</sup> Dies hat das Bundesverfassungsgericht für unverhältnismäßig und unvereinbar mit Art. 19 Abs. 4 GG erklärt, soweit die Verwaltungsgerichtsordnung die Aktenvorlage auch in denjenigen Fällen ausschließt, in denen die Gewährung effektiven Rechtsschutzes von der Kenntnis der Verwaltungsvorgänge abhängt.<sup>34</sup>

---

<sup>30</sup> BVerwG, Urt. vom 25.03.1999, NVwZ 1999, 1220/1222.

<sup>31</sup> § 14 Abs. 1 IFG.

<sup>32</sup> § 15 Abs. 5 IFG.

<sup>33</sup> Zur Kritik daran im Hinblick auf das Gebot effektiven Rechtsschutzes aus Art. 19 Abs. 4 GG und zur Möglichkeit, für einen begrenzten Prozessabschnitt auf das Informationselement aus Art. 103 Abs. 1 GG zu verzichten, siehe Sokol, Datenschutz versus Informationszugang, DuD 1997, 380/381 f.

<sup>34</sup> BVerfG, Beschl. vom 27.10.1999, 1 BvR 385/90, <http://www.bverfg.de/>.

§ 99 VwGO verkürzt danach den Rechtsschutzanspruch in einem nicht erforderlichen Maße. Geheimhaltungsbedürfnisse und Rechtsschutzansprüche können auf mildere und bessere Weise miteinander in Einklang gebracht werden – etwa durch die Einführung eines "in camera"-Verfahrens. Darunter ist eine gerichtliche Prüfung der Akten ohne Einsichtnahmemöglichkeit der Beteiligten zu verstehen. Dem steht der Anspruch auf rechtliches Gehör aus Art. 103 Abs. 1 GG nicht entgegen. Er verfolgt vielmehr ebenfalls das Ziel, effektiven Rechtsschutz zu ermöglichen. In Fällen, in denen das ungeschmälerete rechtliche Gehör die Effektivität des Rechtsschutzes im Ergebnis herabsetzt statt sie zu stützen, führt der Verzicht auf ein "in camera"-Verfahren zu einer Minderung des Individualrechtsschutzes, die erheblich schwerer wiegt als eine Einschränkung des rechtlichen Gehörs. "Der Anspruch auf rechtliches Gehör, der dem Rechtsschutz des Einzelnen dient, kann diesem nicht entgegengehalten werden, wenn der begrenzte Verzicht darauf seinen Rechtsschutz ausnahmsweise verbessert. Nur unter dieser Voraussetzung, nicht dagegen zur Verminderung der Rechtsschutzposition des Betroffenen ist ein "in camera"-Verfahren mit dem Grundgesetz vereinbar."<sup>35</sup> Zum Problem des Akteneinsichtsrechts der Verfahrensbeteiligten im Verhältnis zum Gebot effektiven Rechtsschutzes hat das Gericht somit eine Beschränkung des Akteneinsichtsrechts nur dann für vereinbar mit Art. 103 Abs. 1 GG erachtet, wenn sich erst durch diese Beschränkung der von Art. 19 Abs. 4 GG gebotene effektive Rechtsschutz ermöglichen lässt. Für die Herstellung eines verfassungsmäßigen Zustandes hat der Gesetzgeber eine Frist bis Ende 2001.

Diese sehr zu begrüßende Entscheidung des Bundesverfassungsgerichts ist zu einem Sachverhalt ergangen, in dem der Informationsanspruch über Daten im Zusammenhang mit der eigenen Person des Beschwerdeführers im Streit stand. Weitreichende Bedeutung wird ihr aber gerade auch für mögliche Gerichtsverfahren zukommen, in denen es um die Durchsetzung der allgemeinen Informationsansprüche nach dem Akteneinsichts- und Informationszugangsgesetz in Brandenburg oder nach dem Informationsfreiheitsgesetz in Berlin geht. Die Rechtsschutzposition der Informationssuchenden ist mit der Entscheidung wesentlich gestärkt worden.

---

<sup>35</sup> BVerfG, Beschl. vom 27.10.1999, 1 BvR 385/90, Abs.-Nr. 95, <http://www.bverfg.de/>.



## **Das Datenschutz-Audit**

### **1. Bestehende und fehlende Regelungen zum Datenschutz-Audit**

Das Datenschutz-Audit ist ein neues Instrument des Datenschutzes, das Elemente der Selbstregulierung und des Wettbewerbs enthält und den ordnungsrechtlichen Ansatz des bisherigen Datenschutzes ergänzt: 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.<sup>1</sup>

Das Datenschutz-Audit ist eine Antwort auf das gestiegene Datenschutzbewußtsein bei der Verarbeitung personenbezogener Daten bei Anwendern und Nutzern. Datenschutz ist inzwischen als ein entscheidender Akzeptanzfaktor für alle Formen des elektronischen Handels und der elektronischen Verwaltung erkannt worden.<sup>2</sup> Für viele Anwendungen mit Verarbeitung personenbezogener Daten wird es künftig darauf ankommen, die Anstrengungen im Datenschutz angesichts der großen Unkenntnis und Verunsicherung zu vermitteln. Für beides - für die Datenschutzanstrengungen und ihre Vermittlung - könnte das Datenschutz-Audit ein hilfreiches Instrument sein. Daher wird seit geraumer Zeit über die Einführung eines Datenschutz-

---

<sup>1</sup> Der Beitrag geht auf ein Gutachten mit Gesetzentwurf zum Datenschutz-Audit zurück, das der Verf. für das Bundesministerium für Wirtschaft und Technologie erarbeitet hat. Eine überarbeitete Form des Gutachtens erscheint in Roßnagel, *Datenschutzaudit*, Vieweg Verlag, Braunschweig 1999.

<sup>2</sup> Dies zeigen alle repräsentativen Umfragen zu diesem Thema, s. z.B. Opaschowski/Duncker *Der gläserne Konsument? Multimedia und Datenschutz*, Hamburg 1998; s. auch weitere Hinweise in Roßnagel (Fn. 1).

Audits diskutiert<sup>3</sup> und es sind sogar bereits erste gesetzgeberische Schritte unternommen worden.

Der am 1. August 1997 in Kraft getretene Mediendienste-Staatsvertrag enthält in § 17 als erstes Datenschutzgesetz eine Programmnorm zur Einführung eines Datenschutz-Audits für Mediendienste.<sup>4</sup> Als erstes Bundesland besitzt Brandenburg seit dem 21. Dezember 1998 eine ähnliche Regelung.<sup>5</sup> 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."*

Diese beiden Regelungen werden allerdings für die breite Realisierung eines Datenschutz-Audits wenig bewirken. Sie gelten nur bereichsspezifisch für Mediendienste oder die öffentlichen Stellen eines Bundeslandes. Mehr zu erwarten für die Umsetzung des neuen Datenschutzinstruments ist dagegen von dem Entwurf der Bundes-

---

<sup>3</sup> Die Idee eines Datenschutz-Audit stieß von Anfang auf viel Sympathie – s. z.B. Ulrich, DuD 1996, 668; Bachmeier, DuD 1996, 673; Engel-Flehsig, DuD 1997, 15; Engel-Flehsig, RDV 1997, 66; Berliner Datenschutzbeauftragter, Datenschutz-Bericht 1996, Berlin 1997, 134f.; 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.

<sup>4</sup> Diese Programmnorm 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 -.

<sup>5</sup> GVBl. I, 243.

regierung für ein neues BDSG.<sup>6</sup> § 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 Verfahrens sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt."*

Alle diese Regelungen sind jedoch nur Programmnormen. Sie stellen ein künftiges Datenschutz-Audit in Aussicht, verweisen aber für seine Durchführung auf ein noch zu erlassendes Gesetz. Ein solches Gesetz, wie es in den Programmnormen angekündigt wird, ist bisher noch nirgendwo erlassen worden. Auch ist weder der Entwurf eines solches Gesetzes noch die Arbeit an einem solchen Entwurf bekannt. Wie könnten ein Datenschutz-Audit und ein dieses regelndes Gesetz aussehen?<sup>7</sup>

Hierzu sollen im folgenden noch einmal die Ziele eines Datenschutz-Audits dargestellt werden (2.), um aus diesen nach einem kurzen Blick auf das Vorbild des Umweltschutz-Audits (3.) das Konzept eines Datenschutz-Audits zu entwickeln (4.) sowie dessen Kriterien (5.) und Verfahrensschritte (6.) zu beschreiben. Der Beitrag schließt mit einem kurzen Ausblick (7.).

## **2. Ziele eines Datenschutz-Audits**

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

---

<sup>6</sup> Zu weiteren Initiativen zur Einführung eines Datenschutz-Audits s. z.B. die Hinweise in Roßnagel, Datenschutz-Audit, in: Sokol, B. (Hrsg.), Neue Instrumente im Datenschutz, Düsseldorf 1999, i.E.

<sup>7</sup> Ein erstes ausgearbeitetes Konzept findet sich in Roßnagel, DuD 1997, 505.

## **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 datenverarbeitende Stellen belohnen, die bei der Konzeption ihres Angebots datenschutzrechtliche Belange berücksichtigen, und für alle anderen marktgerechte Anreize schaffen, dies ebenso zu tun.<sup>8</sup>

## **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 Kon-

---

<sup>8</sup> Begründung zu § 17 des MDStV; ebenso Engel-Flehsig, DuD 1997, 15; Roßnagel, DuD 1997, 507.

trollinstanzen sind die für die Datenverarbeitung geltenden Anforderungen des Datenschutzrechts. Da das Datenschutz-Audit andere Voraussetzungen<sup>9</sup> und Folgen<sup>10</sup> aufweist als die behördliche Datenschutzkontrolle, vermag es diese sehr wohl zu ergänzen, nicht aber zu ersetzen.

### **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.<sup>11</sup> Ebenso sollte das materielle Hauptziel des Datenschutz-Audits die kontinuierliche Verbesserung des Datenschutzes und der Datensicherung sein.<sup>12</sup> 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 prämiieren, und schafft dadurch einen Marktanreiz, sie zu ergreifen. 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. Diese ist gerechtfertigt durch überobligationsmäßige Anstrengungen, die das Unternehmen über den gesetzlichen Minimalstandard hinaus unternimmt.

---

<sup>9</sup> Z.B. die freiwillige Teilnahme versus die Durchsetzung von Kontrollen nach §§ 24, 38 Abs. 1 - 4 BDSG.

<sup>10</sup> Z.B. Nichtzertifizierung der Datenschutzerklärung versus Beanstandungen und Anordnungen nach §§ 25, 38 Abs. 5 BDSG.

<sup>11</sup> Art. 3 lit a) der 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.

<sup>12</sup> So auch Berliner Datenschutzbeauftragter, Datenschutz-Bericht 1996, Berlin 1997, 134; Roßnagel, DuD 1997, 507; Königshofen, DuD 1999, 266 ff.

## 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.<sup>13</sup> Dieser Lernprozeß wird dadurch strukturiert, daß der Datenverarbeiter in einer umfassenden Betriebsprüfung eine Bestandsaufnahme der Verarbeitung personenbezogener 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.<sup>14</sup> 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.

---

<sup>13</sup> S. für das Umweltschutz-Audit z.B. Hemmelskamp/Neuser/Zehnle, ZEW-Wirtschaftsanalysen 1994, 207; Köck, JZ 1995, 646.

<sup>14</sup> S. für das Umwelt-Audit ähnlich Führ, Eigenverantwortung oder Öko-Staat? Sicherung der Selbstverantwortung in Unternehmen, in: Roßnagel, A./Neuser, U. (Hrsg.), Reformperspektiven im Umweltrecht, Baden-Baden 1996, 247.

### 3. Vorbild Umweltschutz-Audit

Die Idee eines Datenschutz-Audits geht zurück auf das Umweltschutz-Audit, das in Form einer Verordnung der Europäischen Gemeinschaft<sup>15</sup> und in Form einer Techniknorm der International Standardization Organisation (ISO)<sup>16</sup> geregelt ist. Die unmittelbar geltende EG-Verordnung wird ergänzt durch das Umweltauditgesetz (UAG)<sup>17</sup> und vier Rechtsverordnungen<sup>18</sup>, die zur ihrer innerstaatlichen Umsetzung ergangen sind.

Durch das Umweltschutz-Audit sollen die Eigenverantwortung des Unternehmens für seine Umweltauswirkungen und sein 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 eingerichtet, das in regelmäßigen Abständen in einer von dem Unterneh-

---

<sup>15</sup> EG-UAVO (Fn. 11).

<sup>16</sup> ISO EN DIN 14.000 vom Oktober 1996 sowie weitere Normen der 14.000er Reihe.

<sup>17</sup> Gesetz vom 7.12.1995, BGBl I, 1591.

<sup>18</sup> 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 Umweltmanagements und die Umweltbetriebsprüfung auf weitere Bereiche (UAG-Erweiterungsverordnung - UAG-ErwV) vom 3.2.1998, BGBl I, 338.

men 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.<sup>19</sup> Ende 1998 waren 1734 Standorte in Deutschland eingetragen.<sup>20</sup> 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 sie 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.<sup>21</sup> Bezieht man die Einspareffekte auf die Auditkosten ergibt sich eine Amortisationszeiten 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 Datenschutzes-Audits genommen werden. Allerdings muß immer wieder geprüft werden, inwieweit es im Detail für die völlig andere Zielsetzung des Datenschutzes als tauglich erscheint.

---

<sup>19</sup> S. "Bericht der Bundesregierung über die Erfahrungen mit dem Vollzug des Umweltauditgesetzes (UAG)" vom 18.6.1998- BT-Drs. 13/11127.

<sup>20</sup> S. Lütkes/Ewer, NVwZ 1999, 20.

<sup>21</sup> S. hierzu die Zusammenfassung im Evaluationsbericht der Bundesregierung, BT-Drs. 13/11127, 7.

## 4. Das Konzept eines Datenschutz-Audits

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

### 4.1 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.<sup>22</sup> 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.<sup>23</sup> Das Datenschutz-Audit soll eine Ressource nutzen, die für den Datenschutz bisher noch nicht genutzt wird, nämlich die Möglichkeiten eines Datenschutzmanagements. Dementsprechend ist das Datenschutz-Audit als System-Audit zu konzipieren.

---

<sup>22</sup> S. für die Datensicherheit z.B. die Produktzertifizierung durch das BSI nach dem BSIG.

<sup>23</sup> 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".

## 4.2. Freiwilligkeit

Das Datenschutz-Audit sollte freiwillig sein.<sup>24</sup> Für die Unternehmensvertreter, die sich bisher zum Datenschutz-Audit geäußert haben ist dies eine essentielle Voraussetzung für die Akzeptanz des Datenschutz-Audits.<sup>25</sup> 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.<sup>26</sup> 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"<sup>27</sup>, sondern ein Instrument der unternehmensinternen Selbstregulierung mit öffentlicher Anerkennung.

## 4.3 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 erkaufte werden. Das

---

<sup>24</sup> Ebenso Entschließungsantrag der SPD-Bundestagsfraktion, BT-Drs. 13/7936, 5; Vogt/Tauss (Fn. 3), 19; Bachmeier, DuD 1996, 680; Roßnagel, DuD 1997, 509; kritisch gegenüber der freiwilligen Teilnahme am Umwelt-Audit Führ, EuZW 1992, 471, und ders., NVwZ 1993, 860.

<sup>25</sup> 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.

<sup>26</sup> Aus diesem Grund enthält § 14 des Allgemeinen Teils des vorgeschlagenen Umweltgesetzbuchs eine Verpflichtung für Großbetriebe, eine Öko-Bilanz durchzuführen.

<sup>27</sup> So aber Drews/Kranz, DuD 1998, 94.

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.

#### **4.4 Umsetzung der Programmnorm des § 9a BDSG-E**

Eine 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 seiner Erfüllung 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 vor: Es ist zum einen ein Spezialgesetz, das nach § 1 Abs. 4 Satz 1 BDSG den Regelungen des BDSG vorgeht. Zum anderen hat es allein schon nach den 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 Anknüp-

fungspunkt 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 ihre 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 mit evaluiert.

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 datenverarbeitende 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 BDSG 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.<sup>28</sup> 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.

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 seine organisatorische Ausprägung und seine Umsetzung durch konkrete Maßnahmen beinhaltet. In diesem Sinn entspricht das Datenschutzkon-

---

<sup>28</sup> 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.

zept der Formulierung einer Datenschutzpolitik, ihrer Konkretisierung in einem Datenschutzprogramm und ihrer 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.

## **5. 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 allen gleichen Maßstab und einen subjektiven, den der einzelne Anbieter nach seinen individuellen Möglichkeiten bestimmt.

### **5.1 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.<sup>29</sup> 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

---

<sup>29</sup> So z.B. der Arbeitskreis "Datenschutzbeauftragte" im Verband der Metallindustrie Baden-Württemberg (VMI), DuD 1999, 281 ff.

einer Werbemöglichkeit prämiieren. Es darf daher 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 Datenschutzerfordernngen 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 MDSStV - 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 der Optimierungen und Abwägungen nicht gerecht. Über die für die Feststellung der Belange und ihre 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 sie ihm präsentiert. Diese werden in der Regel die Konkretisierung des Optimierungsziels oder der Abwägung durch die Stelle 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. Sie hängen ohnehin von der Zumutbarkeit, von der subjektiven Möglichkeit, letztlich von den individuellen Umständen ab. Wenn sie nach subjektiver Leistungsfähigkeit befördert werden, entspricht dies genau dem Charakter und der Zielsetzung des Datenschutz-Audits.

## **5.2 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 "wirtschaftliche 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.<sup>30</sup> Vielmehr bestimmen die Unternehmen selbst, um wieviel sie ihre Datenschutzanstrengungen über das rechtlich geforderte Minimum hinaus verbessern wollen.

---

<sup>30</sup> Dies jedoch unterstellen Drews/Kranz, DuD 1998, 94, und kritisieren diese falsche Annahme.

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.<sup>31</sup> Wer hier einen höheren Aufwand betreibt als andere, 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".<sup>32</sup>

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.

---

<sup>31</sup> S. hierzu für § 3 Abs. 4 TDDSG Bundesrat, BT-Drs. 13/7385, 57; s. allgemein Roßnagel, DuD 1997, 508.

<sup>32</sup> S. provet (Fn. 4), Begründung zu § 11 des vorgeschlagenen Multimedia-Datenschutz-Gesetzes; ebenso Begründung zu § 17 MD-StV; Bachmeier, DuD 1997, 680; Engel-Flechsig, DuD 1997, 15; Vogt/Tauss (Fn. 3), 19.

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.<sup>33</sup> 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 datenverarbeitende Stelle ausrichten, muß aber als Entwicklungskonzept zu einer kontinuierlichen Verbesserung des Datenschutzes überzeugen. Dies festzustellen, ist eine Aufgabe des Datenschutzgutachters. Ihm kommt daher eine besondere Bedeutung für die Vertrauenswürdigkeit des gesamten Auditsystems zu.

## **6. 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:

---

<sup>33</sup> S. die Dokumentation der Prinzipien und Leitlinien in DuD 1999, 285 ff.; s. auch <<http://www.gdd.de>>; <<http://www.ofts.de/mulimed.htm>> und <<http://www.uni-kassel.de/fb10/oeff-recht/>> die Prinzipien und Leitlinien können in der Newsgroup <d.soc.datenschutz> diskutiert 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 Bestandsaufnahmen 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.<sup>34</sup> Denn zwischen seinen Aufgaben und denen des Datenschutz-Audits bestehen viele Parallelen.<sup>35</sup> Das Unternehmen muß sich in seiner Datenschutzpolitik verpflichten, die einschlägigen Datenschutzvorschriften einzuhalten und den Datenschutz kontinuierlich zu verbessern. Die zentrale Aufgabe des betrieblichen Datenschutzbeauftragten gemäß § 37 BDSG ist es, die Einhaltung datenschutzrechtlicher Vorschriften sicherzustellen.<sup>36</sup> Viele Teilaufgaben, die er in diesem Rahmen zu erfüllen hat, können auch für die Vorbereitung des Audits und die interne Betriebsprüfung genutzt werden.

## **7. Ausblick**

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 Konkurrenten 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 Rahmensezung schafft die Voraussetzungen für die Zielgerechtigkeit des Verfahrens und die Vergleichbarkeit der Kriterien und Ergebnisse. Das Datenschutz-Audit ist ein Instrument zur Erfüllung der Struktur-

---

<sup>34</sup> Ebenso der Arbeitskreis "Datenschutzbeauftragte" im Verband der Metallindustrie Baden-Württemberg (VMI), DuD 1999, 281 ff.

<sup>35</sup> S. hierzu ausführlich Roßnagel, DuD 1997, 513f.

<sup>36</sup> S. Engel-Flehsig, DuD 1997, 15; ders., RDV 1997, 67.

verantwortung des Staates.<sup>37</sup> Dieser könnte er gerecht werden, ohne öffentliche Haushalte zu belasten.<sup>38</sup>

---

<sup>37</sup> S. hierzu näher Roßnagel, ZRP 1997, 26 ff.

<sup>38</sup> 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.



**Prof. Dr. Hansjürgen Garstka**  
Berliner Datenschutzbeauftragter

## **Datenschutz und Informationsfreiheit – Zwei Bausteine für ein Informationsgesetzbuch**

### **Die Idee eines Informationsgesetzbuches**

Dass Datenschutz und Informationsfreiheit zueinander in einem Spannungsverhältnis stehen, bedarf keiner Erläuterung. Jeder Zugang zu Informationen birgt die Gefahr, dass die informationelle Selbstbestimmung der Betroffenen beeinträchtigt wird, jede vom Datenschutz aufgerichtete Schranke schränkt die Freiheit des Informationszugang ein, die möglicherweise für die Wahrnehmung politischer, aber auch individueller Interessen erforderlich ist. Ebenso unstrittig ist aber, dass beiden Prinzipien in der Rechtsordnung Geltung verschafft werden muss, wenn die Informationsgesellschaft informationelle Selbstbestimmung und Demokratie ermöglichende Transparenz gleichermaßen garantieren soll. Von daher liegt es nahe, die Konkordanz beider Prinzipien dadurch zu suchen, dass sie in einen übergeordneten Zusammenhang, und dies könnte heißen in eine übergeordnete Kodifikation eingebracht werden. Die zu erwartende Entwicklung des Internet, insbesondere in der Form des e-Commerce legt dies besonders nahe, denn gerade hier werden sich die Fragen des Informationszuganges und der Informationshemmung nicht trennen lassen.

Die Idee, beide Prinzipien zusammenzuführen, trifft sich mit darüber hinaus greifenden Vorschlägen, die bestehenden (BGB, SGB) bzw. geplanten (Arbeitsgesetzbuch, Umweltgesetzbuch) großen Kodifikationen um ein Informationsgesetzbuch zu ergänzen. So machte der Berliner Datenschutzbeauftragte in seinem Jahresbericht 1990 den Vorschlag, dem Herannahen der Informationsgesellschaft "mit klaren rechtlichen Vorgaben insbesondere für die staatliche Datenverarbeitung" zu begegnen. Diese könnten sich nicht auf die Datenschutzgesetze im engeren Sinne beschränken, sondern müssten die Informationsverarbeitung in allen Phasen abdecken. Wesentliche Elemente eines solchen Gesetzeswerkes wären neben einem am Ende zu

schaffenden Allgemeinen Teil, der die Grundstrukturen eines Informationsrechts vor die Klammer ziehen müsste, ein den Vorgaben des Bundesverfassungsgerichts entsprechendes Datenschutzgesetz, ein Gesetz, das die verschiedenen allgemeinen Anwendungsformen der Informationstechnik in der Verwaltung regeln muss, ein Gesetz, das gegenüber der informationstechnischen Infrastruktur die Transparenz für den Bürger sichern muss und schließlich Gesetze, die die Sekundärverwertung der erhobenen Daten für allgemeine staatliche oder gesellschaftliche Zwecke regeln (Statistikgesetz, Archivgesetz<sup>1</sup>). Dies fortführend, hat der Berliner Staatsrechtslehrer Michael Kloepfer in seinem Gutachten zum 62. Deutschen Juristentag 1998 für die Schaffung eines solchen Informationsgesetzbuches plädiert<sup>2</sup>. Der Juristentag hat aufgrund dieses Vorschlages beschlossen: "Die Reformschritte (zur Erneuerung des Informationsrechtes) sind zu einem umfassenden Informationsgesetzbuch zusammenzuführen". Entsprechende Vorarbeiten sind aufgenommen worden.

Interessant ist, dass die staatliche Duma der Russischen Föderation im Januar 1995 ein Gesetz über Information, Informatisierung und Informationsschutz verabschiedet hat, in dem programmatisch eine ähnliche Bündelung (hier allerdings auch Staatsschutzinteressen einbeziehend) vorgenommen wird<sup>3</sup>.

Das Projekt eines Informationsgesetzbuches hat auch eine wissenschaftstheoretische Entsprechung in den Bemühungen, als Leitkonzept für das Informationszeitalter neben Wirtschaft- und Rechtsordnung eine Wissensordnung zu setzen, die ihrerseits einen einheitlichen juristischen Zugang nahe legt. Spinner fordert ein "informationelles Gesamtkonzept" im Hinblick auf die rechtliche Bewältigung, das insbesondere eine Verbindung herstellen soll von freiem Informationszugang mit dem Schutz der Privatsphäre<sup>4</sup>.

---

<sup>1</sup> Berliner Datenschutzbeauftragter: Jahresbericht 1990, S. 8

<sup>2</sup> Kloepfer: Geben moderne Technologien und die europäische Integration Anlass, Notwendigkeiten und Grenzen des Schutzes personenbezogener Daten neu zu bestimmen? S. D 90ff

<sup>3</sup> Auszugsweise abgedruckt in Berliner Datenschutzbeauftragter: Internationaler und Europäischer Datenschutz. Materialien zum Datenschutz 24, S. 131 ff

<sup>4</sup> Spinner: Die Wissensordnung, Opladen 1994, S. 171

## Theoretische Grundlegung

Datenschutzrecht und Informationsfreiheitsrecht sind in den USA in den 60er Jahren aus unterschiedlichen Quellen entstanden. Das Datenschutzrecht (Right to Privacy) war eine freiheitsrechtliche Reaktion auf die Planung der Kennedy - bzw. Johnson-Administration, beim Statistischen Bundesamt unter Einsatz der gerade hinreichend mächtigen Computertechnologie eine Bundesdatenbank aufzubauen, in der Daten über sämtliche amerikanische Staatsbürger gespeichert werden sollten. Die öffentliche Diskussion dieser Planungen führte zu Nachforschungen über den damaligen Bestand großer Datensammlungen in den USA und zu entsprechenden Aufdeckungen (z.B. über den Umfang der Speicherungen über politische Meinungen bei der Armee<sup>5</sup>). Ergebnis war die Schaffung eines Gesetzes (Privacy Act) im Jahr 1974, mit dem die Befugnisse des Staates zur Verarbeitung personenbezogener Daten auf das erforderliche Maß begrenzt und dem Bürger Zugangsrechte zu seinen individuellen Daten eingeräumt werden sollten. Der Freedom of Information Act von 1967 wurzelt ebenfalls auf Ideen der Kennedy-Cam-pagne, hier jedoch auf dem Bedürfnis nach einer stärkeren Demokratisierung der Gesellschaft. Die so unterschiedlich, wenn auch in der gleichen politischen Philosophie wurzelnden Ideen führten zu einer Versäulung beider Gebiete, die heute noch die Wahrnehmung prägen.

Diese moderne Entwicklung verdeckelt, dass beide Paradigmen über eine lange Geschichte verfügen. Das im letzten Jahrhundert insbesondere in Großbritannien entwickelte "Right to be Alone" sowie das daraus entwickelte "Right to Privacy"<sup>6</sup> stehen in einem engen Zusammenhang mit hergebrachten Geheimhaltungsvorschriften. Die Öffentlichkeit von Gerichtsverhandlungen als Schritt hin zu mehr Transparenz staatlicher Entscheidungsfindung ist ebenso eine Quelle des Informationsfreiheitsrechtes, wie der Kampf der Presse um Zugang zu staatlichen Informationen, der bereits im 18. Jahrhundert in Schweden zu einer Informationsfreiheitsgesetzgebung geführt hat.

Dass diese traditionell getrennt wahrgenommenen Bereiche in einem engen Zusammenhang stehen, ergibt sich besonders deutlich aus

---

<sup>5</sup> vgl. Westin: Privacy and Freedom, New York 1967

<sup>6</sup> Warren/Brandeis: The Right to Privacy In: Harvard Law Review 1890, S. 3 ff

system-theoretischen Überlegungen zum Zusammenhang zwischen Realität und Recht, wie sie, aus biologischen Forschungen der 30er Jahre entstammend Bertalanffy<sup>7</sup>, in den 50er und 60er Jahren intensiv angestellt wurden (im Übrigen vor 1968 gerade in den sozialistischen Ländern<sup>8</sup>). Sie finden einen gewissen Höhepunkt in den Forschungen Wilhelm Steinmüllers, der das Recht selbst als Informationssystem betrachtet<sup>9</sup>.

Betrachtet man im Anschluss an die Überlegungen Spinners die Wissens- bzw. Informationsordnung als eine eigene Sphäre, die die Wirtschaftsordnung, aber auch die Ordnungen des privaten und öffentlichen Lebens überlagert, kommt dem Informationsrecht die Funktion zu, zwischen der realen Welt auf der einen Seite und dem Informationssystem auf der anderen Seite zu vermitteln, wobei das Recht als systemnormative Informationen selbst wiederum Bestandteil der Informationsordnung ist.

Die Informationsgesellschaft ist geprägt von der Rolle der Informationstechnik, die zunehmend die sozialen Beziehungen in der Gesellschaft dominiert. Die Informationstechnik greift in die Beziehungen zwischen Realität und Informationsschicht ein: Sie verändert Realität, indem sie durch Überwindung von Zeit, Orts- und Quantitätsgrenzen neue Handlungsformen ermöglicht. Bereiche werden eröffnet, die vorher nicht denkbar waren. Dies verändert auf gravierende Weise das Verhältnis von Wissen und Realität. Denkbar ist, dass nicht mehr das Wissen der Welt folgt, sondern umgekehrt die Welt sich nach den Möglichkeiten der Informationstechnik richtet. Aufgabe des Rechts in diesem Zusammenspiel ist, die Harmonie zwischen der Realität und der Informationssphäre aufrecht zu erhalten.

---

<sup>7</sup> Bertalanffy: Zu einer allgemeinen Systemlehre. In: Blätter für Deutsche Philosophie 1945, S 3 ff

<sup>8</sup> zusammenfassend Galperin; Lebedev: Die Leitung der gesellschaftlichen Prozesse und die Kybernetik. In: Staat und Recht 1965, S. 1622 ff

<sup>9</sup> Steinmüller: Informationstechnologie und Gesellschaft. Darmstadt 1993

## Konsequenzen

Diese zugegebenermaßen etwas abgehobenen Überlegungen führen sofort zu praktischen Konsequenzen, wenn bei der Frage nach den Inhalten eines Informationsgesetzbuches von diesem Denkmodell ausgeht.

Die Art und Weise, wie die Informationssphäre die Realität abbildet, und welche die Rolle die Technik dabei spielt, führt sofort zur Frage, welchen rechtlichen Restriktionen die Abbildung unterworfen werden soll. Dies heißt konkret, es stellt sich die Frage, in welchem Umfang Datenmengen und Dateninhalte einer Regulierung unterworfen werden sollen. Die in der modernen Datenschutzdiskussion erhobene Forderung nach "Datensparsamkeit" zielt genau in diese Richtung<sup>10</sup>. Damit in der Informationssphäre nicht so viele Spuren menschlichen Handelns hinterlassen werden, dass das Subjekt seine Unabhängigkeit verliert, ist vermittelnde Technik so zu gestalten, dass sie mit einem Minimum an (personenbezogenen) Daten auskommt. Anonymisierung oder Pseudonymisierung stellen sicher, dass autonomes Handeln nicht durch beliebige Nachvollziehbarkeit gefährdet wird.

Sind die Datenmengen und somit die Relation zwischen Informationssphäre und Realität bestimmt, stellt sich die wesentliche Frage: Wer hat Zugang zu den Informationen und kann damit auf die Beziehungen zwischen beiden Sphären einwirken, darüber hinaus, welche Verpflichtungen bestehen, diesen Zugang zu schaffen? Andererseits: Unter welchen Voraussetzungen soll der Datenzugang verweigert werden können bzw. besteht sogar eine Pflicht zur Offenbarung?

So betrachtet fügen sich Datenschutz und Informationsfreiheit in ein übergeordnetes System ein, das allerdings mehr umfasst, als die Gesetzgebung zu Datenschutz und Informationsfreiheit derzeit repräsentiert.

Informationsfreiheit als informationsrechtliches Prinzip kann bei so allgemeiner Betrachtung nicht nur den Zugang zu den Akten der

---

<sup>10</sup> zur politischen Forderung nach Datenvermeidung vgl. Rat für Forschung, Technologie und Innovation. Endbericht Informationsgesellschaft, Chancen, Innovationen und Herausforderungen Bonn 1995, S. 33

öffentlichen Verwaltung betreffen, sondern sie würde auch den Zugang zu den Informationen in privater Hand beinhalten. So überraschend diese Forderung auf den ersten Blick sein mag, so sehr leuchtet sie bei näherer Reflektion ein. Abgesehen davon, dass auch im Privatrechtsregime bisher an mancherlei Stellen Zugangsrechte verankert sind (Publizitätsvorschriften im Gesellschaftsrecht, Veröffentlichungspflichten der verschiedensten Art im Verwaltungsrecht, Impressumspflichten im Presserecht usw.), erscheint die Forderung nach mehr Transparenz in den privaten Herrschaftsbereichen als Konsequenz der zunehmenden Machtverschiebung des Staates gegenüber der Privatwirtschaft. In einem bisher für kaum möglich gehaltenen Umfang und Tempo häufen gerade in diesen Monaten große Privatunternehmen finanzielle Ressourcen und damit auch Macht an, die diejenige des Staates bei Weitem überflügelt. Hinzu kommt eine Übertragung bislang öffentlicher Aufgaben in den privaten Bereich, gerade im Bereich der Daseinsvorsorge; die wesentlichen Infrastrukturen der Informationsgesellschaft entstehen ohnehin im privaten oder privatisierten Raum. Entsprechend sind die Beherrschungsmöglichkeiten, die diese Unternehmen gegenüber den Einzelnen haben. Die alte vertikale Zweiteilung in Staat und Gesellschaft macht einer horizontalen Teilung in Staat und Business auf der einen Seite, Bürger und Verbraucher auf der anderen Seite Platz. Bürger und Verbraucher sind vom Zugang zu Informationen in Staat und Wirtschaft gleichermaßen Abhängig.

Das Datenschutzrecht als Ausprägung des informationellen Selbstbestimmungsrechtes des Individuums stellt ebenfalls nur einen Ausschnitt aus dem Recht der Informationsrestriktionen dar. Sollen diese Restriktionen übergreifend geregelt werden, geraten auch die Schutzrechte juristischer Personen (Geschäftsgeheimnisse) oder des Staates (Geheimschutzregelungen) ins Blickfeld - der Ansatz des Russischen Föderationsgesetzes ist daher so falsch nicht. Auch die Gründe für die Informationsverweigerung liegen nicht ausschließlich im Schutz der Privatsphäre begründet: Zeugnisverweigerungsrechte, Amts- und Berufsgeheimnisse zielen nicht oder jedenfalls nicht nur auf die Rechte des Individuums sondern auch auf die Aufrechterhaltung sozialer Systeme.

Besondere Probleme wirft das Verhältnis zwischen beiden Bereichen auf, wenn es zu Zweckänderungen ("Sekundärnutzungen") kommen

soll. Die großen datenschutzrechtlichen Konflikte in den vergangenen Jahren bewegen sich stets um die Frage, in welchen Fällen Restriktionsrechte zu Gunsten von Zugangsrechten (für Forschung, Statistik, Strafverfolgung, Archivierung) zurücktreten sollen.

Die Theorie der informationellen Selbstbestimmung geht allerdings von den Priorität der Informationsrestriktion aus

Ziel eines Informationsgesetzbuches müsste es sein, allgemeine Grundsätze zu formulieren, die in diesen Konfliktsituationen eine rationale Entscheidung erlauben.

## **Weiterungen**

Ein Informationsgesetzbuch wird sich nicht auf Gewährung und Beschränkung des Rechtes auf Information beschränken können. Neben den Rechten *auf* Information stehen die Rechte *an* Informationen: Einerseits die Rechte derjenigen, die die Informationen geschaffen und gestaltet haben (Urheberrecht), auf der anderen Seite derjenigen, die Gegenstand der Information sind, jetzt nicht betrachtet unter dem Aspekt der informationellen Betroffenheit, sondern vielmehr unter dem Aspekt des Eigentumsrechtes an Daten. Dies wird in Deutschland stets verworfen<sup>11</sup>, in den USA aber im Zusammenhang mit "property rights" intensiv diskutiert<sup>12</sup>. Diese Rechtspositionen stehen quer zu den bisher behandelten. Je nach dem, welche Bedeutung man dem Warenwert der Information beimisst, wird man beim Ausgleich zwischen Informationsfreiheit und Datenschutz auch diese Positionen berücksichtigen müssen. In welchem Umfang können Rechte an Informationen Informationsfreiheit beschränken oder umgekehrt, in welchem Umfang der wirtschaftliche Wert personenbezogener Daten ein Argument für den Datenschutz darstellen? So wird in den USA bereits diskutiert, ob die Befugnis, personenbezogene Daten zu verarbeiten, nicht an die Zahlung eines Entgelts geknüpft werden sollte, ähnlich der Nutzungsgebühr im Urheberrecht.

Es zeichnet sich ab, dass angesichts der Entwicklung im Internet der

---

<sup>11</sup> Meister: Datenschutz im Zivilrecht. Das Recht am eigenen Datum. Bergisch Gladbach 1981

<sup>12</sup> Branscomb: Who owns information? From Privacy to Public Access, New York 1994

Konflikt zwischen den Rechten an Informationen und den Informationszugangsrechten, die sich auf die Meinungsfreiheit stützen, zum dominierenden Problem wird. Auch zu diesem Grundkonflikt wird sich ein umfassendes Informationsgesetzbuch äußern müssen.

## **Informationstechnik**

Ausgehend von der theoretischen Vorstellung, dass die *Informationstechnik* die Relation zwischen Realität und Informationsordnung bestimmt, ergeben sich folgende Fragestellungen für ein Informationsgesetzbuch:

Führt Informationstechnik zu korrekten Abbildungen zwischen den Bereichen?

Welche Instrumente der Informationssicherheit im Allgemeinen, welche speziellen technischen Instrumente im Besonderen sind zur Verfügung zu stellen bzw. dürfen beschränkt werden (Kryptographie, digitale Signaturen, Auditierungs- und Zertifizierungsmechanismen)?

Welche Mittel der technischen Unterstützung von Informationszugangs- und Verweigerungsrechten sind bereitzuhalten, etwa um einen Online-Zugang zu Dokumenten zu ermöglichen (wie das im Electronic Freedom of Information Act der USA bereits vorgesehen ist)? Welche Anonymisierungs- und Pseudonymisierungsmechanismen müssen bereit stehen?

Im Internet stellen Suchmaschinen und Verweigerungsmechanismen (No-Robot-Funktionen, Filter und Firewalls, Techniken zur Unterstützung der informationellen Selbstbestimmung wie P3P) das technische Äquivalent zu Informationszugang und Datenschutz dar. Aufgabe eines Informationsgesetzbuches könnte es sein, Prinzipien für die Konstruktion von Informationssystemen vorzugeben, die diese Relation stabilisieren ("Systemdatenschutz").

Ich räume ein, dass diese Überlegungen zu theoretisch und zu abgehoben erscheinen. Gleichwohl: Wenn wir die Aufgabe ernst nehmen, dem Recht der Wirtschaftsordnungen ("lex mercatoria") sowie dem

Recht des Staates ("lex publica") eine "lex informatica"<sup>13</sup> zur Seite zu stellen, werden wir um derartig grundsätzliche Überlegungen nicht herumkommen.

---

<sup>13</sup> Reidenberg: Lex informatica: The Formulation of Information Policy Rules through Technology, In: Texas Law Review 1998, S. 533 ff



## **Dr. Thilo Weichert**

Stellvertretender Landesbeauftragter für den Datenschutz bei der Präsidentin des Schleswig-Holsteinischen Landtages

### **Für ein bürgerfreundliches Datenschutz- und Informationsfreiheitsrecht**

Auf dem 8. EDV-Gerichtstag Mitte September 1999 unter dem Motto "Freies Recht für freie Bürger" wurde öffentlich bekannt gegeben, daß demnächst die Entscheidungen des Bundesverfassungsgerichts im Internet jedermann unentgeltlich zum Abruf zur Verfügung gestellt würden. Eine kluge und nützliche Aktion, sollte man denken. Ganz andere Meinungen waren jedoch auf eben dieser Tagung zu hören. So trug ein Verlagsvertreter vor, die Gesetzessprache sei eine Fachsprache, die vom Normalbürger nicht verstanden werde. Manche meinten gar, die Veröffentlichung im Internet sei geradezu gefährlich, da die Bürger nur verwirrt würden. Die Bundesjustizministerin plädierte im Geleitwort zu dieser Tagung zwar für die Veröffentlichung juristischer Texte, doch kosten solle es schon etwas: "Bei Leistungen, die nur einem Teil aller Bürger, insbesondere professionellen Nutzern, zugute kommen, ist der Staat gehalten, zumindest kostendeckende Gebühren zu erheben". Offensichtlich kein Thema der Tagung war, weshalb die Gesetzessprache fast nur noch von kommerziell interessierten Experten verstanden werden kann. Und damit sind wir bei unserem Thema, der Frage nach "bürgerfreundlichem Recht". Diese Frage stellt sich in besonderem Maße bzgl. der Rechts der Informationstechnik, also eben der Technik, die in der Lage ist, juristische Texte billig und einfach jeder und jedem zugänglich zu machen.

Ich weiß nicht, weshalb gerade ich gebeten wurde, zu diesem Thema zu referieren. Vielleicht erwartet man von dem Vorsitzenden einer Bürgerrechtsorganisation wie der Deutschen Vereinigung für Datenschutz (DVD) und dem Mitarbeiter einer Datenschutzbehörde, die sich Serviceorientierung und Bürgernähe ins Pflichtenheft geschrieben hat, ein paar neue Anregungen. Vielleicht wird von mir auch Selbstkritik erwartet, da ich an einem Gesetzentwurf für ein neues Bundesdatenschutzgesetz (BDSG) nicht unmaßgeblich beteiligt war.

Wie dem auch sei. Ich hätte nicht gedacht, daß mir nach meiner Zusage zu diesem Vortrag noch derart abschreckendes und derart positives Material zum Thema über meinen Schreibtisch laufen würde. Beginnen wir mit dem Abschreckenden: Der der Öffentlichkeit vorgelegte Referentenentwurf für ein Bundesdatenschutzgesetz und der Regierungsentwurf für eine Reform der gesetzlichen Krankenversicherung mit dem Namen "Gesundheitsstrukturreform 2000" mögen hinsichtlich vieler Aspekte stark umstritten sein. Unbestreitbar dürfte aber sein, daß es sich bei beiden Gesetzentwürfen einer von der Mehrheit des Volkes gewählten Bundesregierung um Musterbeispiele bürgerunfreundlicher Gesetzgebung handelt. Als positives Beispiel möchte ich den Gesetzentwurf des SSW im Schleswig-holsteinischen Landtag über die Freiheit des Zugangs zu Informationen nennen. Die Gruppe des Süd-Schleswigschen Wählerverbandes im Landtag besteht aus einer Abgeordneten.

Solange wir in einer Industriegesellschaft gelebt haben, war die Bürgerfreundlichkeit von Informationsrecht nicht von zentraler Bedeutung. Beim Austausch von Waren ist ein leicht verständliches Bürgerliches Gesetzbuch wichtig. In dem Maße, in dem jedoch Informationen Relevanz im Alltag und im Wirtschaftsleben gewinnen, muß auch der Frage der Bürgerfreundlichkeit des Informationsrechts verstärkt nachgegangen werden.

Bei der ersten Generation der Datenschutzgesetze hat es sich zweifellos nicht um besonders abgehobenes Recht gehandelt. Darin enthaltene umständliche und unverständliche Regelungen, etwa die Sperrungsvorschrift des § 14 Abs. 2 BDSG '77, stießen auf keine ausdrückliche negative Resonanz. Diese Gesetze wandten sich vorrangig an die Verwaltung, in beschränktem Maße an die Wirtschaft und bestenfalls bzgl. der "Rechte der Betroffenen" (§ 4 BDSG '77) an die allgemeine Bevölkerung.

Die Zeiten haben sich insofern geändert. Der Bürger ist zum Datenverarbeiter geworden, der mit PC, ISDN-Anschluß, Chipkarten, Mobiltelefon, Telediensten und elektronischen Netzwerken im privaten wie im geschäftlichen Leben umgeht. Der Einzug der EDV in den Alltag führte zu einer Demokratisierung dieses Themas. Der Mensch, bisher nur Objekt der Informationsverarbeitung, wird plötzlich selbst zum Verarbeiter. Er nutzt seinen PC nicht nur als Schreibmaschine,

sondern als Bibliothek, als Zeitung, als Warenkorb oder gar als Spielzeug. Er ist durch die EDV nicht nur in seinen Grundrechten gefährdet, von ihm selbst kann eine Gefahr ausgehen. Er hat sich darum zu kümmern, daß seine Daten als Konsument und Arbeitnehmer von Großunternehmen oder unbekanntem Hackern nicht zu seinem Schaden genutzt werden. Er hat sich darum zu kümmern, daß er als Datenverarbeiter nicht durch fremde Netzaktivitäten beeinträchtigt wird. Es ist aber auch dafür verantwortlich, daß er selbst keinen Schaden bei Dritten verursacht. Als Nutzer des Internet kann er die informationelle Selbstbestimmung, die Meinungsfreiheit und geistige Eigentumsrechte anderer verletzen. Der Bürgerin bzw. dem Bürger bieten sich mit der Informationstechnik zudem ganz neue Möglichkeiten der Informationsbeschaffung und Meinungsbildung. Der elektronische Zugriff auf die im Internet abrufbaren gewaltigen Datenbestände, der Zugriff auf zig Fernseh- und Hörfunkkanäle, das uferlose On-Line- und Off-Line-Informationsangebot macht aus dem Recht des Art. 5 GG, sich frei informieren zu dürfen, eine reale Möglichkeit in ganz neuen quantitativen und qualitativen Dimensionen.

Diese Entwicklung der Informationstechnik läßt das bisherige Informationsrecht nicht so, wie es war. Nicht nur, daß sich Neuerungen der bisherigen, alten Regelungslogik, von der Struktur wie von der Begrifflichkeit, nicht mehr erfassen lassen. Viel problematischer ist es, daß durch die Globalisierung der Netzkommunikation und durch die zunehmende Flüchtigkeit der Datenverarbeitung - gekennzeichnet durch "schneller, mehr, billiger, intelligent und konvergent" - sich diese Verarbeitung der normativen Regulierung immer mehr entzieht. Die Antwort hierauf ist, daß die Verantwortung für die Wahrung der eigenen Rechte vom Staat und seinen Möglichkeiten der Rechtsdurchsetzung auf die Bevölkerung selbst übertragen werden muß. Dies kann aber nicht dazu führen, daß die Qualität des Informationsrechts von immer geringerer Wichtigkeit ist. Zwar verlieren klare materiell-rechtliche Ge- und Verbote an Bedeutung; doch sie werden ersetzt durch technisch-organisatorische Gewährleistungen, Dienstleistungsansprüche und verfahrensrechtliche Sicherungen. Nicht nur der weiterhin gültige Bestand an Ge- und Verboten, sondern das gesamte neue Normgefüge richtet sich an sämtliche Teile der Gesellschaft und eben auch an Otto Normalverbraucher. Sollte diese kurze Analyse korrekt sein, so ist Bürgerfreundlichkeit zu einer Gültigkeitsvoraussetzung des Informationsrechts geworden.

Nicht nur in seiner Subjektstellung, auch als Objekt der Datenverarbeitung hat sich für den Menschen in der Informationsgesellschaft viel verändert. Ihm stehen nicht mehr einzelne Datenverarbeiter mit klar definierter Datenverarbeitung zu ebenso klar definierten Zielen gegenüber, sondern Informationsverbünde, Data-Warehouses u.s.w. mit vielen Beteiligten, die kurzfristig ihre Organisation und ihre Rechtsform ändern können. Mit Hilfe von Datenabgleichen und sog. intelligenter Datenverknüpfung wird der Mensch tatsächlich zu dem gemacht, wovor Antikabelinitiativen vor mehr als einem Jahrzehnt gewarnt haben: zum auf Daten, Eigenschaften und Merkmale reduzierten Informationsmuster, das kontrolliert und manipuliert wird. Über Massenmedien - und auch das Internet ist ein Massenmedium geworden - kann der Mensch existentiell getroffen werden; er wird aus der Vertrautheit einerseits und der Anonymität andererseits seiner kleinen sozialen Gruppen herausgerissen und der massenmedialen Welt ausgesetzt, der Mensch wird zum potentiellen Prangeropfer im Internet bis hin zur Zielperson hochautomatisierter Direktvermarktung. Und nicht zuletzt macht die Informationsfreiheit den Menschen zum potentiellen Objekt fremder Ausleuchtung. Mit dieser verstärkten Objektstellung einher geht die Notwendigkeit der Stärkung der Betroffenenrechte in Form von Gestaltungs- und Abwehrmöglichkeiten. Auskunft, Benachrichtigung, Gegendarstellung, Widerspruch, Berichtigung, Löschung, Schadensersatz oder sonstige Folgenbeseitigung haben zwar schon eine rechtliche Vergangenheit. Das große Coming-Out steht den Betroffenenrechten in einer bürgerrechtlich orientierten Informationsgesellschaft aber erst noch bevor.

Dieser Bedarf steht in einem eklatanten Mißverhältnis zur Realität. Als beste Beispiele hierfür können das Sozialgesetzbuch (SGB) und das BDSG angeführt werden. Im Volkszählungsurteil hat das Bundesverfassungsgericht die Anforderungen an bürgerfreundliche (verfassungskonforme) Informationsgesetze festgehalten: Die Normen müssen im überwiegenden Allgemeininteresse stehen, sie bedürfen einer gesetzlichen Grundlage, müssen dem rechtsstaatlichen Gebot der Klarheit entsprechen. Zugleich müssen sie im Interesse des Grundrechtsschutzes organisatorische und verfahrensrechtliche Vorkehrungen treffen. Als Beispiel für Regelungen, die "in die verfassungsrechtlich gebotene Richtung weisen", nannte das Bundesverfassungsgericht damals - 1983 - ausgerechnet das Sozial-

recht, insbesondere die §§ 67 bis 86 SGB X. Betrachtet man sich heute die Datenverarbeitungsregelungen im SGB, so kann man über diese Aussage nur noch den Kopf schütteln. Zwischenzeitlich sind über dieses Gesetzeswerk einige Novellierungen hinweggegangen; zwei sind derzeit im Gange, die eine zur Reformierung der Gesundheitsstruktur, die andere zur Anpassung an die europäische Datenschutzrichtlinie. Verfahren wird immer nach dem selben Muster: Der politisch oder technisch bedingte Regelungsbedarf wird auf die alte Regelung aufgefropft. Dadurch werden die Regelungen immer länger, komplizierter und unübersichtlicher. Hatten von den Krankenkassen betriebene Arbeitsgemeinschaften zur Datenannahme bisher keine Gesetzesgrundlage, so erhalten sie nun eine, ebenso die Beratungs- oder die Werbeaktivitäten der Kassen; daß dadurch die gesamte Struktur der Datenverarbeitung der gesetzlichen Krankenversicherung auf den Kopf gestellt wird, kümmert den Gesetzgeber nicht. Nicht weniger perfide ist die Neigung des Gesetzgebers im SGB V, statt wesentliche Fragen selbst zu regeln, dies Vereinbarungen zwischen den Interessenverbänden der Kassen und den medizinischen Berufs- und Interessenverbänden zu überlassen. Bezeichnenderweise kommen die Bürger, die datenschutzrechtlich "Betroffenen", die Patienten, hierbei nicht mehr vor. Ebenso bezeichnend ist, daß kaum eine der ansonsten beteiligten Personen - auch nicht vom behördlichen Datenschutz - einen Überblick über diese Vereinbarungen hat.

Nicht weniger vernichtend fällt das Urteil über das BDSG aus. Seit dem Ursprungsgesetz aus dem Jahr 1977 hat es der Gesetzgeber nicht mehr geschafft, gestaltend tätig zu sein. Vielmehr sind sowohl die Novelle 1990 wie auch die derzeit diskutierte von Außen, vom Verfassungsgericht im Volkszählungsurteil und von der Europäischen Union in der Datenschutzrichtlinie, veranlaßt. Der Gesetzgeber tat und tut nun nichts anderes, als diesen rechtlichen Zwängen nachzugeben, ohne auch eine der lautstark vertretenen Verbandsinteressen beschädigen zu wollen. Heraus kommt ein sprachliches Ungetüm, das inhaltlich zwar niemandem weh tut, das aber dennoch allen schadet, weil es von niemandem verstanden und angewandt werden kann. Weiterhin schleppen wir Veraltetes von 1977 praktisch unverändert mit uns herum: vom Verarbeitungsbegriff bis hin zur "Datenverarbeitung zum Zweck der Übermittlung". Das Gewicht einer Regelung bemißt sich nach dem neuen Recht nicht mehr an der

faktischen Bedeutung, sondern vor allem an deren Länge, an der Zahl der Verweisungen auf andere Normen und der Anzahl von Schachtelsatzteilen, von denen jeder eine Regel zur Ausnahme oder umgekehrt macht. Geschadet wird damit dem Grundanliegen, dem Datenschutz selbst. Die Überregulierung produziert zwangsläufig Vollzugsdefizite und lähmt die Bereitschaft, sich mit dem Thema auseinanderzusetzen. Die dadurch verursachte Rechtsunsicherheit beeinträchtigt aber auch die Verwaltung und die Wirtschaft bei ihren informationstechnischen Innovationsbemühungen. Mangelnde Akzeptanz für solche Innovationen sind ein bei den Bürgerinnen und Bürgern ausgelöster Effekt; gravierender ist der damit einhergehende schleichende Prozeß der Bürgerrechtserrosion.

Gegenüber dem Datenschutz ist die Informationsfreiheit (noch) bürgerfreundlich normiert. Dies liegt vor allem daran, daß wir uns derzeit noch mit Ursprungsnormen der ersten Generation beschäftigen, und nicht, wie beim Datenschutz, mit der zweiten Generalrevision. Doch auch hier sei gewarnt. Das normative Chaos ist schon vorprogrammiert durch die Konkurrenz zwischen speziellen Normen etwa über Umweltinformationen und den allgemeinen zur Verwaltung generell sowie durch die Konkurrenz von Landes-, Bundes- und Europaregelungen. Künftig muß mehr bedacht werden, daß die Jedermannsregelungen zur Informationsfreiheit mit den Betroffenenrechten des Datenschutzes und den Beteiligtenrechten im Verwaltungsverfahren verzahnt werden.

Das normative Chaos hat zweifellos einen Grund in der technischen und gesellschaftlichen Komplexität der geregelten Themen. Doch hierin unterscheidet sich Informations(technik)recht nicht von anderen Rechtsgebieten, z.B. dem Wirtschafts- oder Steuerrecht. Gute Gesetzgebung zeichnet sich dadurch aus, daß Komplexität aufs Wesentliche reduziert wird. Daß dies insbesondere im Informationsrecht nicht mehr und vielleicht noch nicht wieder gelingt, liegt daran, daß es sich bei den Gesetzgebern um Personengruppen handelt, bei denen (noch) größte informationstechnische Defizite bestehen: bei der Ministerialverwaltung und der Politik. Solange auf diese beiden Gruppen kein politischer Druck, kein faktischer Zwang ausgeübt wird, sich Kompetenz anzueignen, bleiben mehr oder weniger bewußtlose Gesetzgebungsentscheidungen weiterhin vorprogrammiert.

Doch genug der Analyse und Kritik. Im folgenden möchte ich zunächst - zusätzlich zur erfolgten technologischen - eine verfassungsrechtliche Begründung für die Notwendigkeit eines bürgerfreundlichen Informationsrechts liefern, um dann in einigen Thesen dessen wesentlichste Wesensmerkmale herauszuarbeiten.

Informationsrecht hat in der Informationsgesellschaft allerhöchste Grundrechtsrelevanz. Die Grundrechte - nicht nur das Recht auf informationelle Selbstbestimmung und die Informationsfreiheit, sondern praktische sämtliche sonstigen Grundrechte auch - können nicht mehr allein aus sich heraus wirken, sondern bedürfen der gesetzlichen Konkretisierung. Erst die Inanspruchnahme dieser gesetzlich konkretisierten Rechte bringt die zugrundeliegenden Grundrechte zur Wirksamkeit und zum Leben. Bürgerfreundlichkeit ist also gleichbedeutend mit "Verständlichkeit und Praktikabilität für die Bürgerinnen und Bürger".

Der zweite Legitimationsstrang für ein bürgerfreundliches Informationsrecht ist ebenso klassisch: Informationsrechtliche Selbstbestimmung ist, so das Bundesverfassungsgericht, "eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens". Oder anders gesagt: Herr der Daten ist nicht die Regierung, sondern es sind die Bevölkerung und der einzelne. Die Regierung hat - bei der Gewährleistung der informationellen Selbstbestimmung der Bürger ebenso wie bei der Sicherstellung des Akten- und Informationszugangs - eine rein dienende Funktion. Damit der Service der Regierung durch die Bevölkerung angenommen werden kann, muß sich das Informationsrecht an den Grundbedürfnissen der Menschen orientieren, und nicht an den Wünschen einzelner Wirtschaftsgruppen oder der Verwaltung.

Wie kann und muß nun ein bürgerfreundliches Datenschutz- und Informationsfreiheitsrecht aussehen? Dazu zehn Thesen:

1. Das Gesetzgebungsverfahren muß (zumindest vorläufig) geändert werden. Solange die Ministerialverwaltungen nicht (mehr) in der Lage sind, sachgemäße bürgernahe Gesetze zu formulieren, sollte diese Aufgabe entweder externen Experten, z.B. Wissenschaftlern, Arbeitsgruppen oder "runden Tischen" übertragen werden. In diesen

Arbeitsgruppen müssen Interessenvertreter der Bürgerinnen und Bürger vertreten sein.

2. Informationsrechtliche Sachverhalte scheren sich nicht um Verwaltungsgrenzen und Gesetzgebungszuständigkeiten. Die Konvergenz in der Informationstechnik nimmt keine Rücksicht auf die föderalistische Struktur der Bundesrepublik. Im Interesse einer möglichst großen Einheitlichkeit unter Wahrung der demokratischen, föderalen Entscheidungsstrukturen sollte Informationsrecht im Rahmen des Erforderlichen in Staatsverträgen der Länder, evtl. unter Einbeziehung des Bundes, gemeinsam geregelt werden, wobei bei der Vorbereitung dieser Verträge Aushandlungsverfahren erprobt werden müssen, die mehrere Entscheidungsoptionen offen lassen. Auch Mustergesetzentwürfe können weitestgehende Einheitlichkeit bei gleichzeitiger Pluralität bewirken.

3. Informationsrechtliche Gesetze haben oft experimentellen Charakter. Im Interesse größerer Experimentierfreudigkeit wie auch im Interesse der Bereinigung von sich als unwirksam erweisenden Gesetze sollte verstärkt von der Möglichkeit Gebrauch gemacht werden, Normen zeitlich zu befristen.

4. Es kann nicht mehr genügen, daß Informationsgesetze irgendwo in einem Gesetzblatt veröffentlicht werden. Vielmehr müssen die informationsrechtlichen Normen für potentiell Interessierte allgemein verfügbar sein. Dies kann in Form von Online-Angeboten elektronisch ebenso erfolgen wie durch Hotlines oder besondere Publikationen auf konventionellem Wege.

5. Die Gesetzessprache muß geändert werden. Regelungen müssen verständlich sein. Dies bedeutet, daß Sätze aus nicht mehr als einem Haupt- und einem Nebensatz bestehen sollten. Die Länge eines Absatzes sollte 5 Zeilen nicht überschreiten. Zu verwenden ist eine normativ klare, zuvor evtl. definierte, mit dem landläufigen Gebrauch übereinstimmende Sprache. Verweisungen sollten sich auf Paragraphen im selben Gesetz beschränken. Weiterverweisungen haben zu unterbleiben. Jeder Paragraph erhält eine den Regelungsinhalt beschreibende Überschrift.

6. Redundante Regelungen, also Normtexte, die sich wiederholen oder gleiches beinhalten, sind im Interesse der Lesbarkeit zu vermeiden. Durch kluge systematische Einordnungen von Normen in allgemeine, speziellere und hochspezialisierte Normen lassen sich auch komplexe Sachverhalte einfach regeln. Statt sämtliche Datenschutzfragen in einem Gesetz regeln zu wollen (so z.B. SGB, StVollzG) ist es bürgerfreundlicher, in einem nachvollziehbaren Umfang auf allgemeinere und auf speziellere Gesetze zu verweisen.

7. Angesichts der sich rapide ändernden technischen Rahmenbedingungen sind feinzisierte, Perfektion anstrebende Normen schnell überholt und zumeist von Anfang an nicht ziseliert genug. Im Bereich des Informationsrechts drängen sich daher Regelungen auf, die die zu berücksichtigenden Interessen benennen, bestimmte Fallkonstellationen exemplarisch auführen, ansonsten aber eher ein Zielprogramm definieren, das durch untergesetzliche Normen, durch Verhaltensregelungen oder durch Rechtsprechung konkretisiert, präzisiert und weiterentwickelt werden kann.

8. Bürgerfreundlichkeit darf nicht mit Paternalismus verwechselt werden. Dies bedingt ein hohes Transparenzangebot, das aber den Bürgerinnen und Bürgern nicht aufgezwungen werden darf. Ein flexibles Regelungskonzept sollte die Betroffenen durch Einwilligungs- und Widerspruchsregeln, Informationsangebote und Informationspflichten in den Verarbeitungsprozeß mit einbeziehen, nicht aber überfordern. Technische Möglichkeiten bei der Informationsvermittlung oder im Rahmen der Willenserklärung sollten verstärkt genutzt werden.

9. Die gesetzlichen Regelungen sollten grds. zu den technischen auch konventionelle, nichttechnische Lösungen als Alternative anbieten. Die Informationsgesellschaft darf diejenigen nicht ausschließen, die aus finanziellen Gründen, aus Gründen der Ausbildung oder des sozialen Status zur Nutzung elektronischer Medien nicht in der Lage oder nicht Willens sind.

10. Sowohl im Bereich Datenschutz wie bei der Informationsfreiheit sind die Bürgerinnen und Bürger angesichts der zumeist komplizierten rechtlichen, technischen und organisatorischen Sachverhalte auf behördliche unabhängige Unterstützung angewiesen. Die Gesetze

sollten die hierfür erforderlichen Voraussetzungen schaffen. Im Interesse einheitlicher Ansprechmöglichkeiten sollten Zuständigkeiten (Datenschutz im öffentlichen und nichtöffentlichen Bereich, Informationsfreiheit) konzentriert werden. Insofern bieten sich die Landesbeauftragten für den Datenschutz an, denen aber die für die neuen Aufgaben notwendigen rechtlichen, materiellen und personellen Mittel zur Verfügung gestellt werden müssen.

Das bürgerfreundlichste Datenschutz- und Informationsfreiheitsrecht ist nichts wert, wenn es nicht in die Praxis umgesetzt werden kann. Der Politik muß daher vermittelt werden, daß der Weg in die Informationsgesellschaft auch Geld kostet. Bürgerfreundlicher Datenschutz und ebensolche Informationsfreiheit setzen ein Serviceangebot für die Menschen voraus, den elektronischen und konventionellen Zugang zu Informationen, die faktische Möglichkeit, Rechte geltend zu machen und durchzusetzen. Aber hier geht es nicht mehr ums Recht. Daher ist das eine andere Geschichte.

# *Forum Soziale Technikgestaltung*

Internationales Symposium „Informationsfreiheit und Datenschutz“  
25./26. Oktober 1999 in Potsdam

## **arbeit 21 – Der mobile Multimedia-Arbeitsplatz**

*Welf Schröter*

Leiter des Forum Soziale Technikgestaltung beim DGB Landesbezirk Baden-Württemberg, Mit-Initiator und Moderator der „Anwenderplattform Telearbeit Baden-Württemberg“, Mitglied des Beirates für Electronic Commerce des Bundesministeriums für Wirtschaft und Technologie, Mitglied im Delphi-Experten-Kreis des BMWi zum Thema

„Informationsgesellschaft im 21. Jahrhundert“

Stabsstelle „arbeit 21“ im Projekt „Multimedia-Arbeitsplatz der Zukunft“ ©

# *Forum Soziale Technikgestaltung*

Der Strukturwandel in der  
Wirtschaft ist auch ein  
Strukturwandel der Arbeit:  
Es entstehen nicht nur neue  
Wertschöpfungszusammenhänge  
sondern zugleich neue

„**Infrastrukturen der Arbeit**“ .

# *Forum Soziale Technikgestaltung*

Die beschleunigte Anwendung von neuen interaktiven Telekommunikations- und Mediatechniken in der Arbeitswelt führen zu drastischen Veränderungen unserer Vorstellungen von Arbeit:

- **tendenzielle Auflösung des Normalarbeitsverhältnisses**
- **Ausweitung neuer Selbständigkeiten**
- **Entbetrieblichung der Arbeit**
- **Virtualisierung der Arbeitswelten**
- **Entstehung flexibler Formen von virtuellen Wertschöpfungsketten in globalem Kontext**
- **Polarisierung und Spaltung des Arbeitsmarktes**

# *Forum Soziale Technikgestaltung*

Das Normalarbeitsverhältnis der Industriegesellschaft ist gekennzeichnet durch die Faktoren

- Ort
- Zeit
- soziale Organisation (Struktur)

*Die Informationsgesellschaft setzt an der **Flexibilisierung der Faktoren „Ort“ und „Zeit“** an.*

# ***Forum Soziale Technikgestaltung***

- In der Arbeitswelt der Informationsgesellschaft ist der betriebliche Dauernormalarbeitsplatz nicht mehr das dominierende Zentrum. Mehr und mehr wird Beschäftigung in befristeter selbständiger Form verbreitet sein.
- Die höhere persönliche Zeitflexibilität geht mit der **Gefahr geringerer sozialer Sicherheit** einher.
- Eine der großen Herausforderungen besteht darin, die errungenen sozialen Standards in die neuen **Infrastrukturen der Arbeit** zu transformieren bzw. hinüber zu retten.

# ***Forum Soziale Technikgestaltung***

## **Wandel der Arbeitskultur ....**

.... weg von der linearen, zeit- und prozeßbezogenen Organisation hin zu ergebnisorientierten, auftragsbezogenen Zielvereinbarungen für eigenständiges work-flow ....

.... management by objectives m.b.o.

# *Forum Soziale Technikgestaltung*

## Die neue **networking**-Kultur: Arbeiten in Netzwerken

- ◆ mehr Eigenständigkeit
- ◆ höhere Team- und Sozialkompetenz
- ◆ **Online-Kompetenz** in Virtualisierungsprozessen
- ◆ **management by objectives mbo**
- ◆ **mehr neue Selbständigkeiten**
- ◆ tasking statt jobbing
- ◆ Partizipationskulturen
- ◆ dynamische Eigenqualifizierung
- ◆ veränderte ‚Führungs‘-Kulturen
- ◆ Tendenz zu neuen Bezahlungsmodellen
- ◆ Transformation sozialer Standards

# *Forum Soziale Technikgestaltung*

- „**Online-Kompetenz**“ beschreibt die Fähigkeit, sich in virtuellen Netzwelten eigenständig orientieren und in virtuellen Netzzusammenhängen denken und handeln zu können.
- „**Online-Kompetenz**“ beschreibt die Fähigkeit, in virtuellen Netzen teamorientiert mit hoher Sozialkompetenz unter m.b.o. zu arbeiten.
- „**Online-Kompetenz**“ beschreibt die Fähigkeit, neue Infrastrukturen der Arbeit selbstständig auffinden und in virtuellen Arbeits- und Wertschöpfungszusammenhängen eigenes Einkommen erwirtschaften zu können.
- „**Online-Kompetenz**“ beschreibt die Fähigkeit, eigenständig neue Online-Lernformen zu nutzen.

# *Forum Soziale Technikgestaltung*

## **arbeit 21**

- deutliche Zunahme des electronic business  
und digitaler Wertschöpfungsprozesse
- deutliche Verstärkung der Virtualisierung von  
Geschäfts- und Arbeitswelten
- erhöhter Einsatz von „virtual agents“,  
„softbots“ und „virtual secretary“
- Anwachsen der dreifachen Mobilität
  - mobiler Mensch in mobilem Team
  - mobiler Auftrag
  - netz-mobile intelligente Werkzeuge
- Wandel des Arbeitsplatzes zum Arbeitsort

# *Forum Soziale Technikgestaltung*

Das Anwachsen virtueller Assistenzsysteme auf der Basis „intelligent“ kommunizierender softbots und virtual agents wird den Bedarf nach einer immens höheren Datenmenge über Kunden- und Auftraggeber nach sich ziehen, um überhaupt ein technikbasiertes Delegationswesen zu ermöglichen. **Die Bedeutung von Datensicherheit und Datenschutz wird qualifiziert steigen.**

Der Schutz sensibler Daten wird mehr und mehr technikimmanent durch integrierte Softwarewerkzeuge (Verschlüsselung) erfolgen müssen.

Die Mobilitätsanforderungen verlangen auch, daß das „mobile Büro“ in Gestalt des multimedialen Endgerätes komplexe Datensicherheitskomponenten aufweist.

# *Forum Soziale Technikgestaltung*

Die größte Herausforderung beim gestaltenden Übergang in neue Online-Arbeitswelten und virtuelle Wertschöpfungszusammenhänge bildet die Überwindung der „**nicht-technischen Innovationshemmnisse**“.

Das Augenmerk darf nicht allein auf Technik und Kosten gerichtet werden: Die Schlüssel sind die „**weichen Faktoren**“.

# *Forum Soziale Technikgestaltung*

## Neue Wege der Gewerkschaftsarbeit

- ◆ **Denken in virtuellen digitalen Arbeits- und Wertschöpfungszusammenhängen**
- ◆ Experimentieren mit virtueller Betriebsrats- und Gewerkschaftstätigkeit: Online-Beratung TELEWISA
- ◆ Projekt „Virtuelles Gewerkschaftshaus“
- ◆ COALA Gewerkschaftliches Competence-Center für neue Online-Arbeitswelten
- ◆ Moderation der „Anwenderplattform Telearbeit“
- ◆ **Regionale Innovationspartnerschaften / RISE**
- ◆ Mitwirkung im CyberOne-Wettbewerb von „Baden-württemberg: connected“

COALA online - Netscape

Datei Bearbeiten Ansicht Gehe Communicator Hilfe **PM LIVE**

Zurück Vor Neuladen Anfang Suchen Suchen Guide Drucken Sicherheit Stop Netscape

Lesenzeichen Adresse: <http://www.gewerkschaftshaus.de/coala.html>



**COALA**  
virtuelles  
**C**ompetence - Center  
für neue  
**O**nline -  
**A**rbeitswelten  
für interaktive  
**L**ernumgebungen  
in der Zukunfts@rbeit  
und innovative  
**A**nwendungen im  
Electronic Commerce

[\[Projektskizze\]](#)  
[\[virtuelles Gewerkschaftshaus\]](#)

Dokument: Übermittelt

Start | Internet Explorer | Microsoft Word ... | Microsoft Power... | T-Online | COALA online... | 14:26

# *Forum Soziale Technikgestaltung*

Die Sicherung von Arbeit und Wertschöpfung in der Region stellt das Ziel des neuen gewerkschaftlichen Vorhabens **“RISE”** auf den Gebieten Telekommunikation und Multimedia dar.

Das Forum Soziale Technikgestaltung des DGB Baden-Württemberg will dabei mit dem Konzept **“Regionale Innovationspartnerschaften”** die Entwicklung des elektronischen Geschäftsverkehrs und die Ausbreitung neuer Tele-Arbeitsformen beschäftigungswirksam mitgestalten.

“RISE” befaßt sich mit den Voraussetzungen und Rahmenbedingungen für regionale Multimedia-Aktivitäten.

# *Forum Soziale Technikgestaltung*

“**RISE**” steht für “**R**egionale **I**nnovationspartnerschaften zur **S**tandortsicherung von elektronischen und virtuellen Wertschöpfungsketten, von **E**lectronic Business, **E**lectronic Commerce und Teleworking”.

# Forum Soziale Technikgestaltung

**About the Competence Network Electronic Commerce**

The Competence Network Electronic Commerce (IW1) is a project of the [Institute of Information Systems \(IWI\)](#) in cooperation with the [DG Bank AG](#)

- [Concept and Design of the Competence Network Electronic Commerce](#)

supported by

Navigation: Home, Advanced Search, Experts, Partners, Glossary, Kontakt, XML, Help

zum nächsten vorausgegriffene Kameraterminal unter der Kongreß-Ausstellung am 27.10.98.

## ERSTER GEMEINSAMER "ANWENDERTAG TELEARBEIT", Stuttgart

Hilfe zur Selbsthilfe für Betriebe und Beschäftigte bietet der erste baden-württembergische "Anwendertag Telearbeit" am 8. November 1999 in Stuttgart an. Die "Anwenderplattform Telearbeit Baden-Württemberg", eine gemeinsame Initiative von Forum Soziale Technikgestaltung des DGB und der DTAG Deutschen Telekom AG Direktion Stuttgart - unterstützt von IHK, Handwerkskammer, Forschung und zahlreichen Partnern aus Wirtschaft und Arbeitswelt - will den praktischen Erfahrungsaustausch zwischen betrieblichen Anwendern fördern und erleichtern.

### The Measurement of Electronic Commerce, Singapore

It is difficult to obtain reliable statistical data on the extent of electronic commerce, because of the absence of international standards. The conference will provide a forum for discussing possible new standards for measuring activities in electronic commerce. It is organized by the [Singapore Department of Statistics](#) and the Centre for Management of Technology at the [National University of Singapore](#).

Navigation: Home, Guide, Suchen, Sicherheit, Stop, Netscape

**Concept and Design of the Competence Network Electronic Commerce**

Address: Commission on Electronic Commerce (CEC2001)  
AD Business - Internet Advertising and Promotion Management  
Dobler Advertising Discussion List  
Aufbauende Netzwerke und Services unter der Leitung von Incentivize (ISCL)  
Videotalk - The Key For Social Advertising Network  
CustomerCare - Research, Evaluation and Analysis Service (Evaluationscenter der IT-Industrie)  
Tollfree  
TELENETSA  
Forum Soziale Technikgestaltung  
Strahlen, Gerate und Werkzeuge  
Anwenderplattform Telearbeit  
Global Forum Dialogue on Electronic Commerce  
Practical Internet Telearbeit Countries  
National Industrial Information Infrastructure (NII)2001 Committee  
Dial-Up Marketplace

Navigation: Home, Advanced Search, Experts, Partners, Glossary, Kontakt, XML, Help

supported by

# *Forum Soziale Technikgestaltung*

## **Anwenderplattform Telearbeit Baden-Württemberg**

**Anwendertag Telearbeit 8. Nov. 99**

*Praxis – Informationen – Gespräche – Kontakte*

“Regionale Innovationspartnerschaft” von Wirtschaft, Handwerk, Verbänden, Gewerkschaften, Forschung und Politik zur Unterstützung und Verbreitung qualifizierter Telearbeit im Rahmen von Telekooperation, Electronic Commerce und Electronic Business

auf Initiative des Forum Soziale Technikgestaltung und der DTAG Deutsche Telekom AG Direktion Stuttgart

# *Forum Soziale Technikgestaltung*

**“Innovation und Arbeitsplätze in der Informationsgesellschaft des 21. Jahrhunderts - Aktionsprogramm der Bundesregierung” vom 22. Sept. 1999 (Auszug):**

“Telearbeit setzt sich in Deutschland vergleichsweise langsam durch..... Auch auf regionaler Ebene haben sich hierzu bereits Initiativen gebildet, die auf eine stärkere Ausschöpfung der Potentiale der Telearbeit zielen. So hat die **”Anwenderplattform Telearbeit Baden-Württemberg”**, die von DGB Baden-Württemberg und der Deutschen Telekom initiiert wurde und von rd. 20 weiteren Partnerorganisationen getragen wird, das Ziel, die Ausbreitung der Telearbeit durch lösungsorientierten Erfahrungsaustausch von Betrieb zu Betrieb, durch Beratung und Demonstration zu befördern. Der Bund kann derartige Initiativen durch seine eigenen Aktivitäten wirksam unterstützen.”

# *Forum Soziale Technikgestaltung*

## **These**

Die sozialisierende Wirkung von stabilen, kollegial erlebten Arbeitsumgebungen lässt nach zugunsten einer stärkeren Autonomie des Individuums. Diese Autonomie trägt die beiden Gesichter „Emanzipation“ und „Atomisierung“.

Es wird für die Gesellschaft in Zukunft in höherem Maße darauf ankommen, soziale Bindekräfte außerhalb der Berufswelt zu stärken und auszuweiten. Dabei könnte die Förderung von Bildungswelten und Bildungsergebnissen vermehrt diese sozialisierende Funktion übernehmen.

# ***Forum Soziale Technikgestaltung***

[www.anwenderplattform-telearbeit.de](http://www.anwenderplattform-telearbeit.de)

[www.gewerkschaftshaus.de](http://www.gewerkschaftshaus.de)

[www.gewerkschaftshaus.de/coala.html](http://www.gewerkschaftshaus.de/coala.html)

[www.forsoztec.dgb-bw.de](http://www.forsoztec.dgb-bw.de)

[www.telewisa.de](http://www.telewisa.de)

[www.aifu.de](http://www.aifu.de)

[www.onforte.de](http://www.onforte.de)

[www.bloch-akademie.de](http://www.bloch-akademie.de)

[www.telebus.de](http://www.telebus.de)

mail [schroeter@talheimer.de](mailto:schroeter@talheimer.de)

## **Arend Steenken**

Direktor des Landesamtes für Datenverarbeitung und Statistik Brandenburg

### **Das Landesverwaltungsnetz - Chancen für die bürgernahe Verwaltung**

Erkennen Sie, meine Damen und Herren, immer Ihre Chancen? Genau am heutigen Tag (26. Oktober), im Jahre 1861 stellte der Physiklehrer Philipp Reis in Frankfurt ein Gerät vor, das er „Telephon“ nannte. Immer sind es Pioniere ihrer Zeit, die die Skepsis gegenüber Neuem und Unbekanntem überwinden helfen. Je größer die Veränderung, um so größer der Widerstand.

Schauen wir uns heute um, das Telefon von damals hat nicht nur sein „ph“ sondern auch seine Schnur verloren.

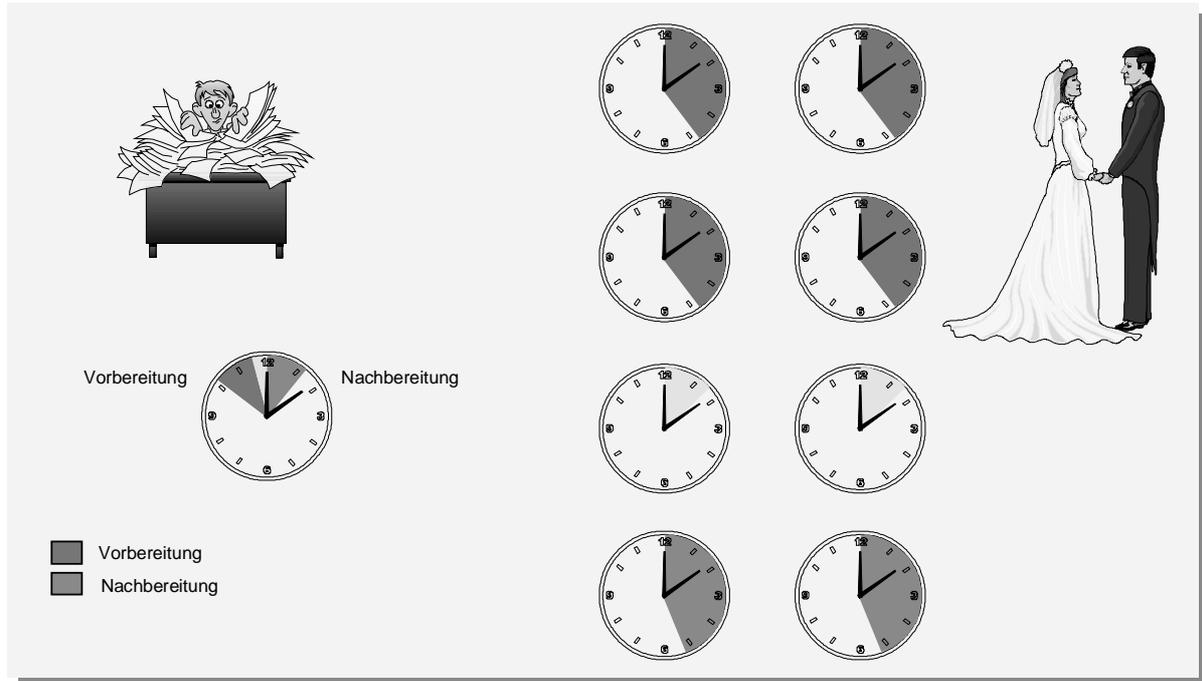
Ich verdeutliche Ihnen heute die **Chancen für eine bürgernahe Verwaltung**, die uns das Landesverwaltungsnetz eröffnet. Als Direktor des Landesamtes für Datenverarbeitung und Statistik bin ich sozusagen von Amtes wegen Pionier in dieser Sache. Nein, mir ist es ein echtes Bedürfnis, Sie für die Nutzung des Landesverwaltungsnetzes zu gewinnen. Dabei spielt weniger der Stolz auf die technische Innovation eine Rolle als vielmehr der Nutzen für den Bürger. Das LDS BB steht außer für das Landesverwaltungsnetz auch für Verwaltungsmodernisierung. Wir sind Pilotbehörde für die Einführung neuer Steuerungsmodelle. Die Frage, die ich in einigen Gesichtern lese - Was hat das miteinander zu tun? - werde ich mit meinen Ausführungen beantworten.

Ein aus dem Leben gegriffenes Beispiel verdeutlicht uns, wo wir heute stehen.  
Eine Eheschließung.

Wieviel Zeit wendet die Verwaltung für eine Hochzeit auf?	Wieviel Zeit benötigt das Ehepaar für Behördengänge?
---	--



## Eheschließung 1998 in Brandenburg



LDS Brandenburg 2322/1

Arend Steenken - LDS BB - Das Landesverwaltungsnetz - Chancen für die bürgernahe Verwaltung

### Vorbereitung

Rede vorbereiten, Musik bereitstellen, Raum ausgestalten,	Wo kann ich wann die Behörde erreichen und welche Unterlagen brauche ich? Urkunden zusammensuchen, Fahr- und Wartezeiten, Vorgespräch, Terminvereinbarung Vorgespräch, Terminvereinbarung, Urkunden überprüfen, Formulare ausfüllen,
---	---

### Trauung

Rede, Beglaubigung	JA , Kuss, Unterschrift
--------------------	-------------------------

### Nachbereitung

Urkunde und neue Papiere ausstellen	Ummeldung im öffentlichen und nicht-öffentlichen Bereich
-------------------------------------	--

## Fazit

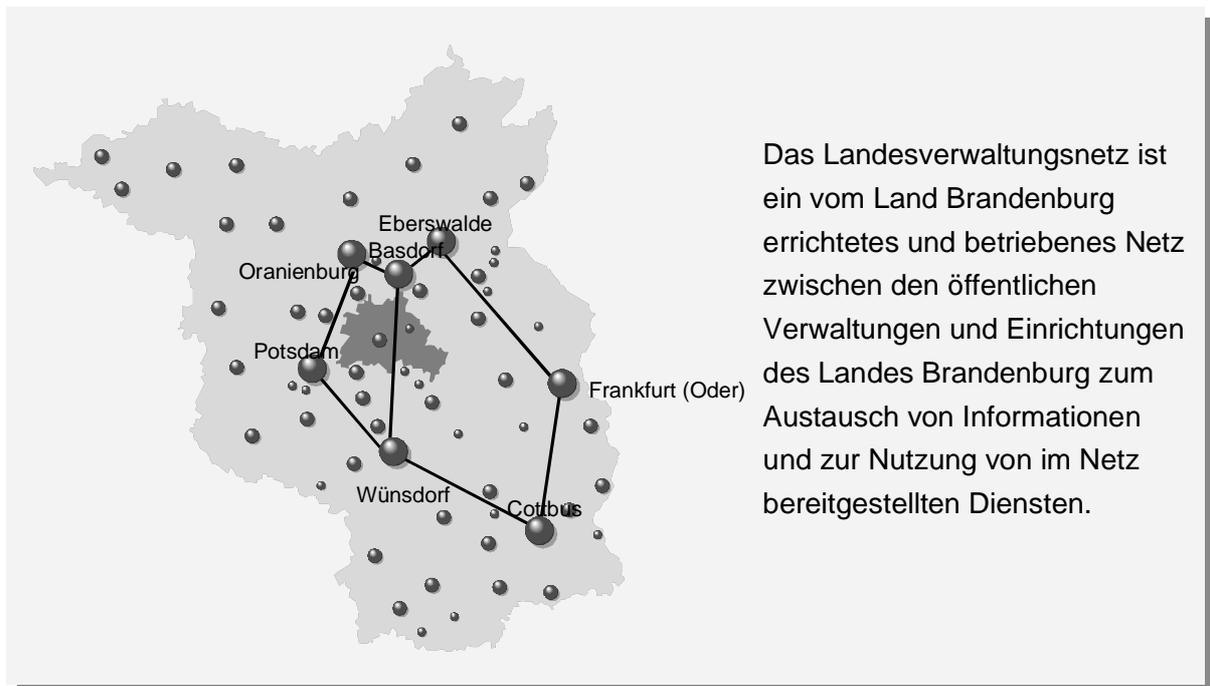
Tragen Mann und Frau im gleichen Maße zur Bewältigung der Formalitäten bei, dann sind sie beide drei Tage mit Behördengängen beschäftigt. Die Verwaltung investiert in jede Eheschließung einen Arbeitstag.

Meine Damen und Herren, lassen Sie mich den Einzelfall auf die Gesamtheit hoch rechnen. 1998 gab es 9266 Eheschließungen im Land Brandenburg. Somit verbrachten 18 532 verliebte Menschen 305 778 Stunden mit Behördengängen. Würde diese Aufgabe ein Paar allein wahrgenommen haben, dann wären sie 52 Jahre (365 Tage/Jahr zu je 8 Stunden) mit Behördengängen befasst. Bei den Behörden summieren sich 33 358 Stunden. Ein fleißiger Beamter hätte somit 16 Jahre sein Auskommen.

Muss es so sein? Das Landesverwaltungsnetz bietet die technische Unterstützung, um Veränderungen herbeizuführen.



## Landesverwaltungsnetz



Das Land Brandenburg errichtete und betreibt das Landesverwaltungsnetz zwischen den öffentlichen Verwaltungen und Einrichtungen,

- um den Informationsaustausch zu ermöglichen,
- um im Netz verfügbare Dienste zugänglich zu machen und
- zentrale Übergänge bereitzustellen.

Die heutigen und zukünftigen Nutzer sind Ministerien, obere und untere Landesbehörden, Verwaltungen der Landkreise, Kommunalverwaltungen und private Nutzer, die über das LDS BB einen zentralen Zugang erhalten.

Zur Zeit befindet sich das Netz in der letzten Ausbaustufe, 300 Landesbehörden, alle Landkreise und kreisfreien Städte sowie einige Kommunen sind angeschlossen.

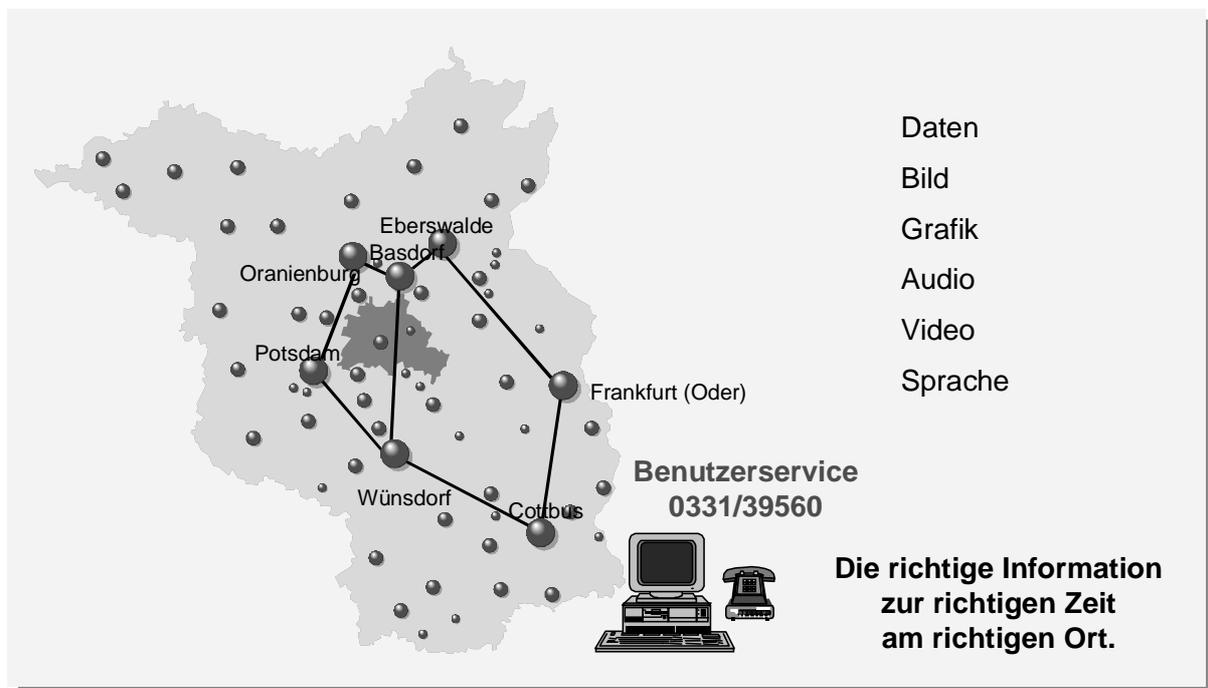
Die angebotenen Dienste und Anwendungen sind:

- Bürokommunikation (GroupWise, Elektronische Mail, Kommunikationsmittel FAX),
- Internet und Intranet (World Wide Web, Brandenburg online, Brandenburg intern)
- Datensicherung und Archivierung
- Konvertierung elektronischer Dokumente
- Telefonieren über das LVN
- Wohngeld

Das Netz dient dem Austausch von Daten, Bildern, Grafiken, Tönen, Filmen und Sprache. Das strategische Ziel ist es: Die richtige Information zur richtigen Zeit am richtigen Ort verfügbar zu haben.



## Strategisches Ziel



Hier ist die kabelgebundene Vernetzung schon eine Einengung und die beim Telefonieren gewonnene Freiheit wird auch hier erwartet ... und es ist möglich. Mit Handy, Laptop, der entsprechenden Software und einem speziell eingerichteten Zugang zum Landesverwaltungsnetz können Sie unterwegs arbeiten, als wären Sie an ihrem Schreibtisch. Diesen kurzen Ausflug möchte ich damit aber schon abbrechen. Ich verweise auf die Telefonnummer oder Internetadresse vom Benutzerservice meines Hauses, der sie gern ausführlich berät.

Die Bereitstellung und Nutzung der technischen Möglichkeiten macht nur Sinn, wenn die Effizienz der Verwaltung erhöht wird. Somit ist diese moderne Informationstechnologie eine Chance, um die Verwaltung zu modernisieren.



## Verwaltungsmodernisierung braucht moderne Informationstechnologie

- **Arbeitsplätze modernisieren**
  - Prozesse rationalisieren
  - Aufgaben ganzheitlich bearbeiten
  - Bearbeitung und Verantwortung verbinden
  - Hierarchieebenen entlasten
- **Verteilte Standorte verbinden**
  - Behörden mit Behörden
  - Behörden mit Außenstellen
  - Landesweite Kommunikation
  - Länderübergreifender Informationsaustausch
- **Verteilte Informationen erschließen**
  - Datenbanken
  - Internet-/Intranet-Dienste



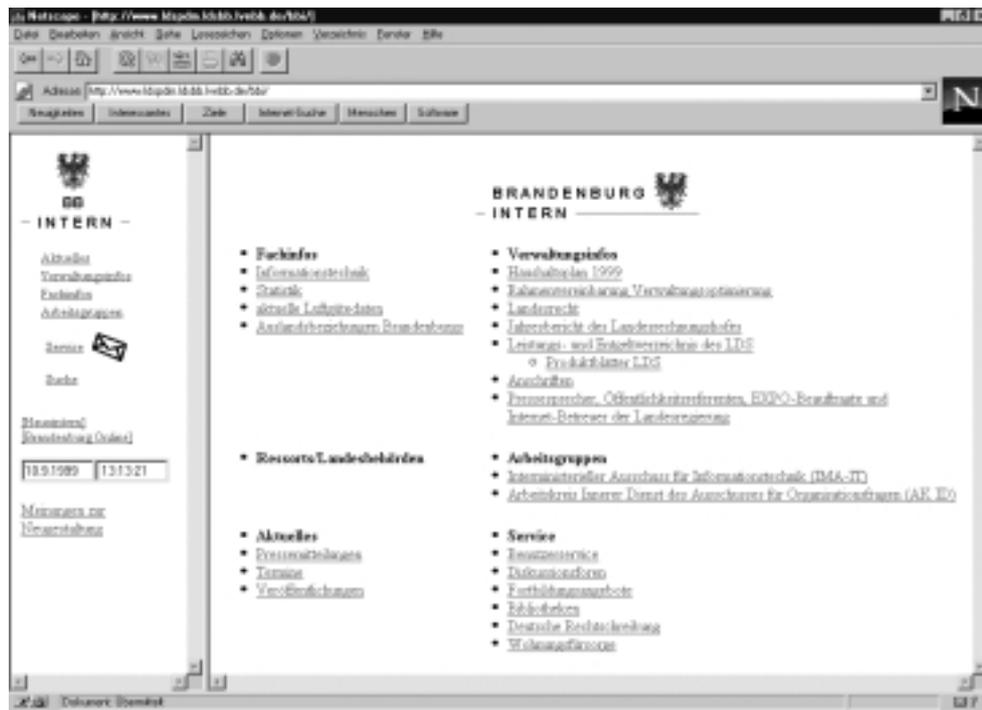
Wir können Arbeitsplätze modernisieren, Prozesse rationalisieren, Aufgaben ganzheitlich bearbeiten und somit die Arbeitsaufgabe mit der erforderlichen Verantwortung verbinden. Diese Bündelung von Aufgabe und Verantwortung ist eine wichtige Forderung bei neuen Steuerungsmodellen und ergibt sich bei der Einführung dieser Technologien nahezu zwangsweise. Organisatorische Veränderungen müssen die technischen Möglichkeiten flankieren, weil sonst Effizienz wieder verspielt wird.

Meine Damen und Herren, diese Sätze sind so schnell gesagt, klingen logisch, modern und so gesprochen oder auf dem Papier regt sich kein Widerstand. In der Praxis sieht es anders aus. Für altgediente Verwaltungsmenschen stürzen Welten zusammen. Die geliebten Vorgänge existieren nicht mehr auf dem Papier sondern elektronisch.

Die Mitarbeiter tauschen per Mail Informationen aus, die der Vorgesetzte eventuell nicht kennt. Das Verhältnis Vorgesetzter zu Mitarbeiter bekommt eine viel stärkere Ausrichtung auf Teamarbeit. Das geliebte Informationsprivileg wird durch das Intranet, wie beispielsweise Brandenburg intern torpediert.



## Brandenburg intern



LDS Brandenburg 2320/1

Arend Steenken - LDS BB - Das Landesverwaltungsnetz - Chancen für die bürgernahe Verwaltung

Auch wenn es hier überspitzt dargestellt ist, der Glaubenskrieg auf diesem Feld der Veränderungen tobt. Die ärgsten Feinde dieser Prozesse sind mittlere Leitungsebenen, die ihre Daseinsberechtigung aus den alten Organisationsabläufen beziehen. So ergibt sich vollkommen logisch eine weitere Forderung der Neuen Steuerungsmodelle, der Abbau von Hierarchieebenen.

Dabei möchte ich es belassen, um die Auswirkungen und den Zusammenhang von Verwaltungsmodernisierung und Informationstechnologie für die internen Abläufe zu verdeutlichen und zu den externen kommen.

Verschiedene Standorte der Behörden behindern die Kommunikation weniger, wenn die Kommunikationsverbindungen optimal sind. Den persönlichen Kontakt können sie jedoch nicht ersetzen. Bei der ganzen Begeisterung für Technik dürfen wir den menschlichen Aspekt nicht aus dem Auge verlieren. Für viele reine Behördenvorgänge ist die Vernetzung jedoch ein Segen. Per E-Mail werden Informationen im Bruchteil einer Sekunde übermittelt, die sonst den Postweg nahmen.

Die Nutzung von Informationen aus dem Internet oder nehmen wir es eine Nummer kleiner, aus dem Intranet. Brandenburg intern bietet schon heute viele wichtige Verwaltungsinformationen die sonst mühsam recherchiert werden mussten. Hier liegt auch ein großer Nutzen des Landesverwaltungsnetzes für die Kommunen.

Bei allen Veränderungen steht die Frage: Was bringt es? Und dabei in erster Linie: Was bringt es dem Bürger? Hier sind uns die Kommunen ein ganzes Stück voraus und umso hilfreicher wird es sei, mit den Kommunen näher zusammen zu rücken. Dabei geht es nicht um eine Verwischung der Zuständigkeiten, sondern um die Nutzung gemeinsamer Ressourcen. Das Streben nach Bürgernähe und die Rationalisierung der Verwaltungstätigkeit bilden eine Einheit.  
Wo liegt nun der Nutzen für den Bürger?



## Nutzen für den Bürger

### Die Informationen sollen laufen, nicht der Bürger

- offene Verwaltung
  - einfacherer Informationszugriff
  - transparente Prozesse
  - Informationszugewinne
- effizienterer Behördengang
  - gezielte Vorbereitung
  - elektronische Kommunikation
  - Zeitersparnis - Kostenersparnis
- Arbeits- und Qualifikations-Service
  - elektronische Stellenvermittlung
  - gezielte Qualifikationsvermittlung
  - Wahrung der Anonymität



**Ohne Datennetz ist in einem großen Flächenland eine bürgerfreundliche Verwaltung nicht möglich.**



Auf einen kurzen Nenner gebracht:  
„Die Informationen sollen laufen, nicht der Bürger!“

- Die Verwaltung bleibt für den Bürger nicht der Moloch hinter verschlossenen Türen. Die Verwaltung wird transparent in ihrem Handeln. Der Beginn ist sicher die Information über Öffnungszeiten, Ansprechpartner, notwendige Unterlagen und die zu verwendenden Formulare. Das für mich derzeitig sichtbare Ziel könnten die Beobachtung von Vorgangsbearbeitungen -wie bei UPS- und die elektronische Akteneinsicht, zu der wir nachher noch etwas hören, sein.

- Ein effizienter Behördengang ist nur möglich, wenn alle erforderlichen Unterlagen mitgebracht werden. Diese Informationen können über das Internet abgerufen werden. Das ist keine Zukunftsmusik sondern in vielen Städten und Ämtern bereits Realität. Zum Teil werden auch die auszufüllenden Formulare mit angeboten. Fragen können per E-Mail gestellt werden und so sind beim direkten Behördengang die meisten Formalitäten bereits erledigt.

- Bereits heute können im Arbeitsamt und über Internet freie Stellen, Qualifikationsmöglichkeiten und -anbieter abgefragt werden. Dabei muss bei der Abfrage kein Grund für das Interesse angegeben werden und es ist keine dritte Person dazwischengeschaltet, der man sich offenbaren muss.

Und genauso im Überblick - der Nutzen für die Verwaltung



## Nutzen für die Verwaltung

- interne Kommunikation verbessern
  - schnellere Verbindung
  - niedrigere Kosten
  - höhere Qualität
- Verfahren beschleunigen
  - schnellere Datensammlung
  - effizientere Datenverteilung
  - produktiverer Datentransport
- Produktivität in der Verwaltung
  - technische Prozessunterstützung
  - zentrale Massenaufgaben
  - dezentrale Dispositionsunterstützung
- Zusammenarbeit Landesverwaltung, Kommunalverwaltung
  - technischer I+K Verbund
  - Nutzung gemeinsamer Ressourcen
  - Entbürokratisierung



**Ohne Datennetz ist in einem großen Flächenland eine bürgerfreundliche Verwaltung nicht möglich.**



- Die interne Kommunikation wird verbessert, weil die Informationen schneller und gezielter vom Sender zum Empfänger gelangen. Die Kosten werden geringer, weil die Post mit ihren Portogebühren inzwischen die teuerste Transportvariante ist und Zeit ist schließlich auch Geld. Mehr und gezieltere Information führt auch zu besseren Ergebnissen. Allein schon die Beteiligung von mehreren Personen an einem Vorgang erforderte in der herkömmlichen Weise viel Zeit und schreckte ab. Heute können per Knopfdruck viele Beteiligte werden, wobei die Einarbeitung der vielen Meinungen bleibt. Es ist aber auch Fakt, wer beteiligt wurde trägt das Ergebnis dieses Prozesses viel eher mit,

als jemand, der vor vollendete Tatsachen gestellt wird. Aber auch Kommunikationsverluste, die bei der mündlichen Weitergabe von Informationen unvermeidlich sind, werden ausgeschlossen. Nahezu trivial klingt es, wenn ich hier mit anführe, dass Dokumente nicht mehrfach geschrieben werden müssen. Vor zehn, fünfzehn Jahren war der Anteil der Schreibarbeiten doch sehr hoch und deshalb gab es spezielle Schreibkräfte. Heute sind solche Stellen in Reinkultur kaum noch anzutreffen. Im LDS BB sind all diese Stellen schon seit Jahren Mischarbeitsplätze.

- Die Beschleunigung der Verfahren ist insbesondere für die Statistik von Bedeutung. Optimal wäre folgende Vorstellung: Ein Auskunftspflichtiger zieht die Zahlen, die er an die Statistik melden muss aus seinen sowieso vorhandenen Datenbestand (Buchhaltung, Lagerhaltung) und schickt sie per Datenleitung an das LDS BB. Bei uns werden die Daten aller Auskunftspflichtigen zu Aggregaten zusammengefasst und in Zusammenhänge gestellt. Die Datenwünsche der Kunden sind in Prozeduren abgelegt und nach Freigabe des Datenbestandes erhalten unsere Kunden ihre Daten per Datenleitung. Erste Schritte auf diesem Weg sind wir bereits gegangen, aber das ist nicht unser heutiges Thema.

- Verfahrensbeschleunigung und Produktivität hängen natürlich eng zusammen. Lassen Sie mich aber hierfür das Beispiel Wohngeld anführen. Das Wohngeldverfahren läuft als zentrales Verfahren im LDS BB und wir nehmen für alle Wohngeldstellen die Zahlbarmachung gegenüber der Landeshauptkasse vor. Alle Wohngeldstellen erhalten Programmänderungen aufgrund von geänderten gesetzlichen Grundlagen vom LDS BB. Soweit die Zentralisierung. Die Wohngeldstellen sind die Ansprechpartner für die Bürger/innen und können vor Ort Auskunft über das zu erwartende Wohngeld und den Stand der Bearbeitung geben.

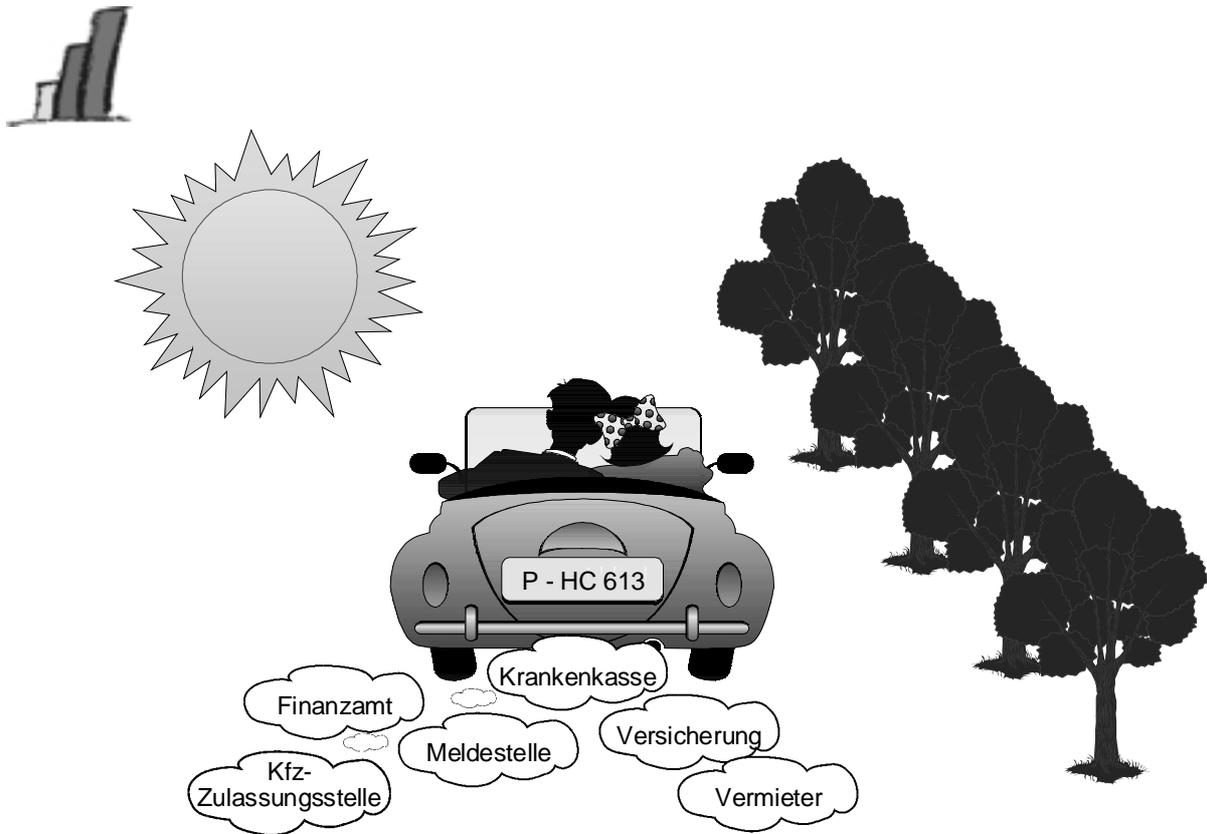
- Die Zusammenarbeit von Landes- und Kommunalverwaltung wird durch den Informations- und Kommunikationsverbund gestärkt. Wir sind in der Lage Ressourcen besser zu nutzen. Das Beispiel Wohngeld steht auch für diese Zusammenarbeit. Im Sinne des Bürgers müssen die Prozesse so gestaltet sein, dass die Bürokratie auf das notwendige Maß zurückgefahren wird.

Meine Damen und Herren, wie würden die Hochzeitsvor- und nachbereitungen unseres Brautpaares aussehen, wenn sie alle technischen Möglichkeiten nutzen könnten und die organisatorischen Rahmenbedingungen vorhanden wären?

Sie buchen den Trauungstermin im Internet und entscheiden welche Formalitäten gleich im Anschluss an die Trauung erledigt werden sollen. Mit der Unterschrift bei der Eheschließung ist gleichzeitig der Auftrag für alle gewünschten Änderungen gegeben. Dabei kann diese Unterschrift auch eine elektronische sein.

Unser Ehepaar fährt in die Flitterwochen und die Verwaltung wird für das glückliche Paar aktiv.

Lassen Sie uns einen Moment bei diesem Paar bleiben. Sie sind im siebten Himmel und keine Bürokratie trübt das Glück.



Sie sparen Nerven und 33 Stunden Behördengänge und als Statistiker darf ich hoffen, sie nutzen die Zeit, um die Bevölkerungsstatistik zu verbessern.

Bei den tangierenden organisatorischen Rahmenbedingungen ist der Gesetzgeber gefragt. Die modernen Technologien müssen Einzug halten in die Einzelgesetze und den Datenschutz. Oft gelten die Behörden und der Datenschutz als hinderlich und Verhinderer von Fortschritt. Aber in vielen Fällen schafft erst die gesetzliche Grundlage den erforderlichen Spielraum. Der Anstoß für die Veränderungen muss von uns kommen. Wir müssen sagen, welche Rahmenbedingungen wir für fortschrittliche Verfahren benötigen. Doch! Auch wenn es unbequem ist, wir müssen, sonst wartet noch in Jahrzehnten Einer auf den Anderen.

Meine Damen und Herren, wenn wir jetzt in uns gehen und ganz ehrlich fragen, lassen uns die bestehenden Gesetze keinen Spielraum? - dann sind es eventuell gar nicht die Gesetze, sondern unsere selbst erlassenen Verwaltungsrichtlinien. Eine kritische Analyse muss erfolgen, um die Hürden zu erkennen.

Die Frage heißt also nicht Behördenarbeit und Datenschutz oder Fortschritt, sondern es geht meiner Meinung nach darum, die Arbeit mit fortschrittlichen Mitteln zu praktizieren. Bereits heute kann ich empfehlen, den Datenschutz von vornherein in die Überlegungen zu integrieren und bei der Realisierung zu berücksichtigen. Unsere Erfahrungen mit dieser Vorgehensweise sind hervorragend und deshalb nutze ich die Gelegenheit, um mich bei Herrn Dr. Dix und seinen Mitarbeiterinnen und Mitarbeitern für die gute Zusammenarbeit zu bedanken.

Wir, das LDS, stehen Ihnen mit technischen Lösungen zur Seite. Bündeln wir unsere Kräfte, unser Wissen und unsere Erfahrungen im Interesse unseres gemeinsamen Ziels, der bürgernahen Verwaltung



**Dr. Hans-Jürgen Lemle**

Projektleiter der NetCity-Initiative Rathenow

## **Elektronische Akteneinsicht in einer brandenburgischen Stadtverwaltung**

Sehr geehrte Damen und Herren,

das Thema meines Vortrages lautet:

„Die elektronische Akteneinsicht in einer brandenburgischen Stadtverwaltung“

Nun ist Rathenow nicht irgendeine märkische Stadt, sondern in der Fachwelt seit vielen Jahrzehnten als "Stadt der Optik" bekannt.

Bereits Ende des 18. Jahrhunderts wurden hier einfache Linsensysteme zusammengesetzt und erste Mikroskope und Ferngläser hergestellt. Die industrielle Fertigung von optischen Erzeugnissen begann mit der Verleihung des königlich-preußischen Privilegs zum Führen einer Optischen Industrie-Anstalt an den Rathenower Pfarrer Johann Heinrich August Duncker sowie mit der Patentierung seiner Vielschleifmaschine am 10. März 1801.

So wurde Rathenow zur Wiege der optischen Industrie in Deutschland und erlangte im Verlaufe der letzten 200 Jahre mit seinen Erzeugnissen Weltruf.

Gestatten Sie mir, dass ich Sie mit einem Zitat von Tony Blair aus „Our information age– the government´s vision“ (Juni 1998) nach den wenigen Worten in eigener Sache auf das eigentliche Thema, die elektronische Akteneinsicht, einstimme.

*„Von der Informationsgesellschaft müssen viele profitieren, nicht wenige. Der Ausschluss von Bevölkerungsgruppen vom Informationszugang würde nicht nur unfair, sondern auch kontraproduktiv sein.“*

Dieses Zitat ist das Leitmotiv unseres Handelns.

Im Folgenden werde ich mich bei meinen Ausführungen auf vier Themenschwerpunkte konzentrieren.

1. Rathenows Weg in die Informationsgesellschaft - Meilensteine
2. NetCity-Projekt
3. Media@Komm
4. Elektronische Akteneinsicht
5. Ausblicke

## **1. Rathenows Weg in die Informationsgesellschaft – Meilensteine**

- 2/1997 Umzug der Stadtverwaltung in ein zentrales Verwaltungsgebäude
- 6/1997 Einrichtung des Bürgerbüros – Anschluß an das LVN
- 7/1997 Erste Internetpräsentation der Stadt
- 8/1997 Bewerbung bei der EU mit dem Projekt NetCity
- 3/1998 Gründung des BWN-RN
- 5/1998 Beteiligung beim Städtewettbewerb Media@Komm und Auszeichnung als eine der 10 besten von insgesamt 136 Kommunen (1.Phase)
- 3/1999 Projektpreis im Media@Komm-Wettbewerb
- 4/1999 Kooperationsvertrag mit IBM/DISOS
- 8/1999 Beteiligung am InnoRegio-Wettbewerb

Das Erscheinungsbild einer Verwaltung wird heute in der Öffentlichkeit nicht gerade positiv bewertet. Die Gründe sind bekannt:

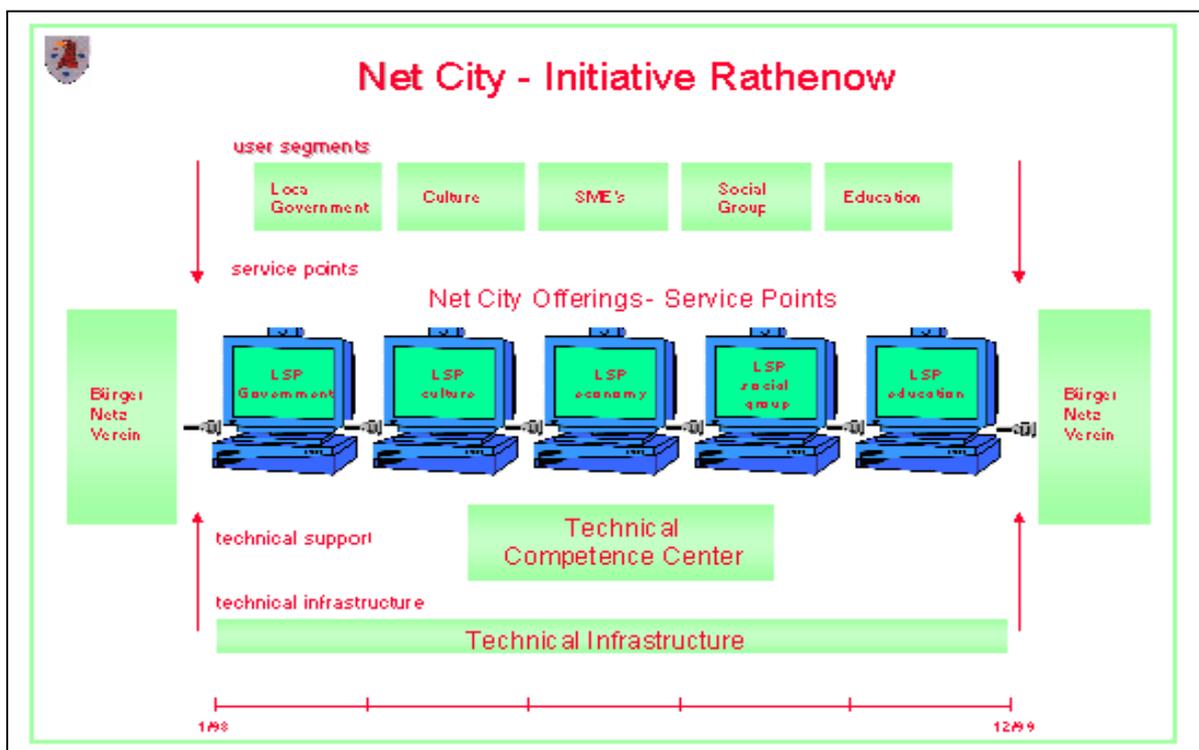
- der Service stimmt nicht
- unverständliche Ausdrucksweise in Wort und Schrift („Bürodeutsch“)
- lange Formulare und
- lange Bearbeitungszeiten

Die Strukturen einer Verwaltung sind zwar verwaltungsfreundlich, aber nicht immer bürgerfreundlich ausgerichtet.

Will man den Anforderungen der Informationsgesellschaft/ Wissensgesellschaft gewachsen sein, geht kein Weg am komplexen Einsatz von Informationstechnik und einer damit verbundenen Strukturreform der Kommunalverwaltungen vorbei. In dem Umfang, wie in den letzten Wochen und Monaten die Modernisierung der öffentlichen Verwaltung diskutiert wird, steigen auch der Zwang und die Einsicht an der elektronischen Informationsbereitstellung sowie an einem strukturierten Informationsaustausch im Rahmen des Verwaltungshandelns.

Möglichkeiten, den Service für den Bürger zu erhöhen, sind die Einrichtung von Bürgerbüros und Bürgerämtern unter Berücksichtigung moderner Informations- und Kommunikationsmitteln (Landesverwaltungsnetz –LVN) und nicht zuletzt das Angebot neuer Dienstleistungen wie z.B. die elektronische Akteneinsicht.

## 2. NetCity-Projekt



Ausgehend von der spezifischen Situation Rathenows (hohe Arbeitslosigkeit, ländlicher Raum) repräsentiert NetCity den Versuch, Innovation und Bedarf in einen ausgewogenen Zusammenhang zu bringen. Das NetCity-Konzept stellt eine Plattform für die Beteiligung aller gesellschaftlichen Bereiche dar. Daher musste zunächst eine technische Infrastruktur entworfen werden, die den Anschluss aller ermöglicht, auch der Bürgerinnen und Bürger im ländlichen Umfeld. Dabei muss der Ansatz für Rathenow finanzierbar und für Brandenburg multiplizierbar sein.

## **Bürger- und Wirtschaftsnetzverein**

Der Bürger- und Wirtschaftsnetzverein Rathenow ist eine Initiative der Stadt Rathenow im Rahmen der Brandenburger Informations-Strategie BIS 2006 mit der Absicht, das NetCity-Konzept umzusetzen und die Anwendung der Neuen Medien zu fördern.

Am 23.03.1998 wurde der Verein unter Vorsitz des Rathenower Bürgermeisters mit 55 Mitgliedern gegründet. Heute zählt der Verein ca. 200 Mitglieder.

Der Bürger- und Wirtschaftsnetzverein macht das Medium Internet für kleine und mittlere Unternehmen, Vereine, Behörden und Verwaltungen sowie Privatpersonen zu günstigen Preisen verfügbar. Der Rathenower Bürger- und Wirtschaftsnetzverein spielte von Anfang an eine strategische Rolle. Er ist: Keimzelle für lokale Initiativen bei der Nutzung des NetCity-Konzeptes, eine gemeinsame Institution für Bürger und Vertreter aus Wirtschaft und Verwaltung, kein „Freak-Club“, sondern ein sich selbst tragender Fachverein, eine geschlossene Benutzergruppe für Pilotprojekte und Experimentierfelder, und er hat vier synergetische Arbeitsgruppen für die thematischen Schwerpunkte :

- Wirtschaft
- Bildung
- Vereine, Verbände & Senioren
- Technik & Informationssystem

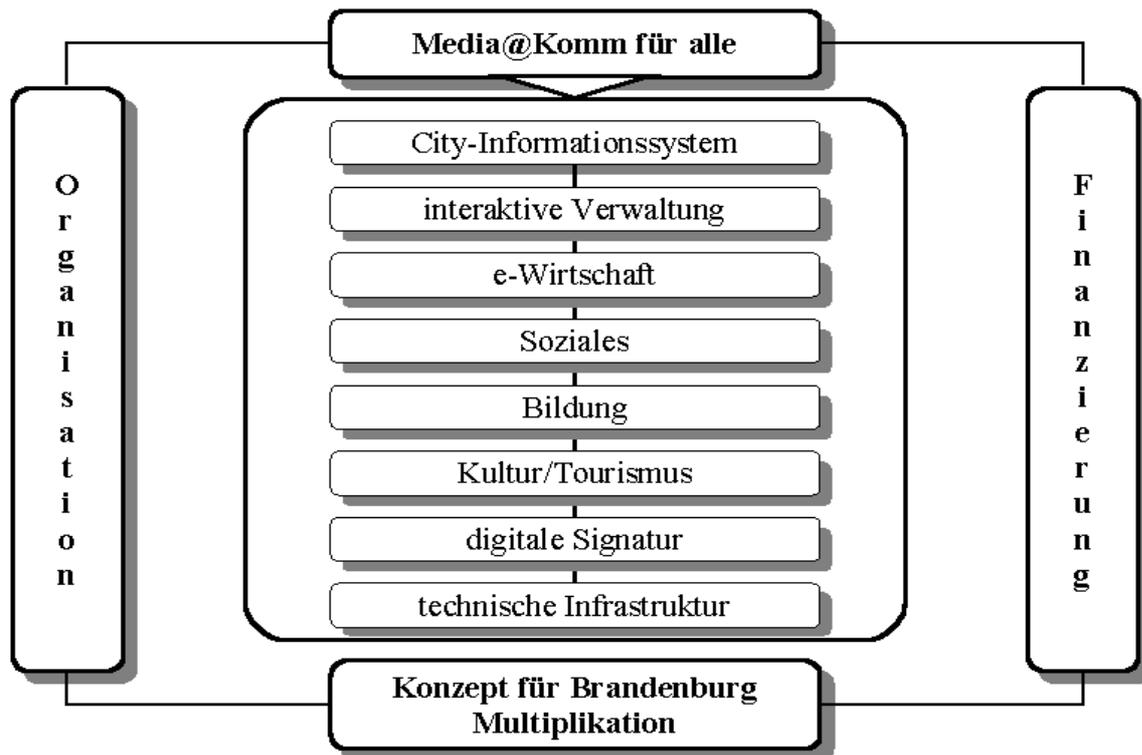
### **3. Media@Komm - Städtewettbewerb**

MEDIA@Komm ist eine Initiative des ehemaligen Bundesministers für Bildung, Wissenschaft, Forschung und Technologie (BMBF), um die Entwicklung von Multimedia in Städten und Gemeinden gezielt zu unterstützen und die Anwendung zu beschleunigen.

MEDIA@Komm ist Teil des Förderprogramms Informationstechnik "Innovationen für die Wissensgesellschaft" und der "Initiative Informationsgesellschaft Deutschland (IID)". In einem integrativen Ansatz sollen im städtischen Raum innovative multimediale Dienste und Anwendungen - möglichst unter Nutzung der digitalen Signatur - entwickelt und Möglichkeiten sowie wirtschaftliche Potentiale demonstriert werden.

An diesem Wettbewerb haben sich bundesweit 136 Städte und Gemeinden mit Ideenskizzen beteiligt. Von den eingereichten Unterlagen wurden von einer internationalen Jury 10 für eine Förderung der Konzepterarbeitung vorgeschlagen (Berlin, Bremen, Dortmund, Esslingen, Karlsruhe, Köln, Leipzig, Nürnberg, Rathenow und Kreis Landkreiis Kitzingen).

Die Stadt Rathenow, die mit Abstand kleinste Stadt in der 2.Phase des Wettbewerbs, wurde für das am 15.01.99 eingereichte Konzept mit einem Projektpreis ausgezeichnet. Die Realisierung des Konzeptteils „Elektronische Akteneinsicht „ist ab Januar 2000 vorgesehen.



## Ziele

Das Projektteam formulierte nach Durchführung von Experten-Workshops folgende Ziele:

- Innovationsimpulse
- Integration des ländlichen Raumes
- Basis für neue Arbeitsplätze
- Interaktive Verwaltungs- u. Geschäftsprozesse – z.B. elektronische Akteneinsicht
- Pilotierung der digitalen Signatur
- Modell für Brandenburg

## CityInformationssystem: CIS-RN

Das CIS-RN ist das Fenster des NetCity-Konzeptes zum Anwender. Es soll vor allem auch ungeübten Nutzern eine leicht verständliche Bedienung der neuen Medien ermöglichen, die die analoge Gedankenwelt der Anwender in eine digitale Systemnavigation überführt.

Dafür wurden thematische Kontext-Menues konzipiert und partiell bereits entwickelt, welche komplizierte und zeitaufwendige Systemiterationen automatisch ablaufen lassen.

## **Interaktive Verwaltung**

Das Thema interaktive Verwaltung stellt für NetCity ein Kernmodul dar. Den Anfang machte das 1997 installierte Bürgerbüro als einen zentralen physischen Bürgerservicepunkt.

Ihm liegen eine Workflowanalyse von Verwaltungsprozessen zugrunde und eine technische Grundkonzeption, die eine kontrollierte und abgesicherte Nutzung des Landesverwaltungsnetzes ebenso einschließt wie den eigens entwickelten Prototyp für die digitale Signatur.

Diese Technik wird über CIS-RN auf eine bedienerfreundliche Systemplattform gehoben. Ein virtuelles Bürgeramt ist das technische Kernstück. Die Realisierung ist in drei Stufen geplant. Einige Anwendungen wie z.B. Teilbereiche im Meldewesen und die elektronische Akteneinsicht sind bereits vorbereitet bzw. umgesetzt worden. Das Modul „elektronische Akteneinsicht“ im Projekt „interaktive Verwaltung“ berücksichtigt das spezifisch brandenburgische Akteneinsichts- und Informationszugangsgesetz (AIG).

Auf der Basis der NetCity-Infrastruktur soll Akteneinsicht auch elektronisch zur Verfügung gestellt werden. Das Projektteam hat das gesamte Aktenmaterial der Stadtverwaltung Rathenow analysiert und typologisiert, um einsichtsrelevante Akten von anderen zu unterscheiden, die Volumen zu bestimmen und daraus einen Kostenrahmen zu entwickeln.

## **4. Elektronische Akteneinsicht**

Brandenburg hat als erstes und bislang einziges Bundesland ein umfassendes Akteneinsichts- und Informationszugangsgesetz. Mit dem Akteneinsichts- und Informationszugangsgesetz (AIG) hat das in Artikel 21 der Brandenburgischen Verfassung festgeschriebene Zugangsrecht der Bürger zu Verwaltungsunterlagen eine gesetzli-

che Grundlage erhalten. Damit wird ein Informationsbereich erschlossen, der dem Bürger in dieser Weise bisher nicht für seine Meinungs- und Willensbildung zur Verfügung stand.

Im Mittelpunkt des Projektes „elektronische Akteneinsicht“ stehen Bürger, Interessengruppen und Verbände, denen auf diesem Wege die Ausübung ihrer Rechte aus dem AIG und dem BbgDSG vereinfacht und transparenter gemacht werden soll. Ziel ist es, den Bürger über seine Einsichtsrechte in Kenntnis zu setzen, die Wahrnehmung auf einfachem Wege zu ermöglichen und damit das AIG mit Leben zu erfüllen. Denn derzeit muß man zur Einsichtnahme zu den Öffnungszeiten der Verwaltung bei der zuständigen Stelle erscheinen. Diese Zeit- und Ortsbindung aufzuheben und die damit verbundenen Aufwände und Beschwerden zu vermeiden, ist Aufgabe dieses Projektes.

Auf diese Weise werden die Bürger unterstützt, aktiv am kommunalen Geschehen teilzuhaben. Durch die zügige Information über Beschlussvorlagen in der Stadtverordnetenversammlung, über Planungsverfahren und weitere Aspekte des kommunalen Lebens wird die politische Partizipation der Bürger unterstützt, d.h. sie werden in die Lage versetzt, sich qualifiziert in die Prozesse einzubringen.

Ein weiterer sehr wichtiger Grund für die Digitalisierung und Elektronifizierung der Aktenablage und –einsichtnahme sind Einsparungspotentiale in nicht unbeachtlichem Maße. So plant das Bundesministerium der Justiz zur Zeit eine Änderung des BGB hinsichtlich der Gleichstellung der Digitalen Signatur gem. SigG mit der Schriftform. Dabei wird das Einsparungspotential allein im Bereich des Rechnungswesens der Sozialversicherungen auf eine Milliarde DM pro Jahr geschätzt.

## **Inhalt des Verfahrens**

Gem. § 3 des Akteneinsichts- und Informationszugangsgesetzes (AIG) sind Akten „alle schriftlich, elektronisch, optisch, akustisch oder auf andere Weise aufgezeichnete Unterlagen, soweit diese ausschließlich amtlichen oder dienstlichen Zwecken dienen. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil des

Vorganges sind und spätestens nach dessen Abschluß vernichtet werden.“

Nach Maßgabe des AIG hat jeder das Recht auf Akteneinsicht, wenn dem nicht überwiegende öffentliche oder private Interessen widersprechen oder bereichsspezifische Regelungen greifen (§ 1 AIG).

Unter Einsicht ist in diesem Fall der Einblick in die Originaldokumente sowie mit Einverständnis des Antragstellers auch die Zurverfügungstellung von

1. Vervielfältigungen,
2. Dokumentationen,
3. elektronischer Post,
4. Broschüren und
5. sonstigen Informationsträgern

zu verstehen (§ 7 AIG).

Innerhalb des Projektes „elektronische Akteneinsicht“ sollen jedoch nicht nur die Sachverhalte des AIG behandelt werden, sondern die Akteneinsicht wird weitergefasst, als jedwede Einsichtnahme in Verwaltungsdokumente, auf welcher gesetzlichen Grundlage sie auch erfolgt.

Bei der Akteneinsicht gibt es zwei verschiedene Einsichtnahmen:

1. Die Kenntnisnahme der eigenen Akte bzw. Daten.
2. Die Einsicht in beliebige Akten.

Die Einsicht in eigene Akten und Daten wird durch das Verwaltungsverfahrensgesetz (VwVfG) und das Datenschutzgesetz (BbgDSG) abgedeckt. Dieses gibt jedem das Recht, über sich selbst zu wissen, was andere über ihn wissen.

Eine uneingeschränkte Akteneinsicht würde jedoch nicht nur störend auf den Verwaltungsbetrieb wirken, sondern auch staatliche oder private Geheimhaltungsinteressen beeinträchtigen. Aus diesem Grunde sieht § 29 II VwVfG einige Einschränkungen vor.

Beim Problem der Einsicht in beliebige Akten greift das AIG. Es stellt den Bürger in die Situation, dass er ein Recht auf Akteneinsicht hat und die Verwaltung ihm ein Verwehren stichhaltig begründen muß. Bereits in Art. 21 Abs. 3,4 der Brandenburgischen Verfassung wurde das Informationsrecht verankert.

Voraussetzungen einer elektronischen Durchführung der Akteneinsicht sind:

- Vorliegen der Akten in elektronischer Form
- Zugang des Einsichtnehmenden zu elektronischen Medien
- Gewährleistung der Identifizierung des Antragstellers
- Sicherstellung der Authentizität der Akten.

Da in der Stadtverwaltung Rathenow nur wenige der Akten komplett elektronisch geführt werden, ist die Digitalisierung Voraussetzung für die elektronische Akteneinsicht. Dies kann auf verschiedenen Wegen erfolgen:

1. Ad-hoc-Digitalisierung der gewünschten Akten zum Zwecke der Einsichtnahme. Danach würden die elektronischen Abbilder der Akten vernichtet werden, da sie bei Weiterbearbeitung der Originalakten veralten würden.
2. Digitalisierung der Akten zur Archivierung. Hierbei würden die Originaldokumente weiterhin im Papierarchiv verbleiben.
3. Digitalisierung der Akten zum Zwecke der weiteren digitalen Bearbeitung, d.h. die Akte wird nur noch in der elektronischen Form weiter bearbeitet. Dies wäre der Übergang zur elektronischen Aktenführung.

Eine fallbezogene Aktendigitalisierung kann zwar für eine kurze Übergangsphase durchgeführt werden, bringt aber gegenüber dem Kopieren nur einen geringen Effektivitätsgewinn im Bereich des Versands. Aus diesem Grunde werden die elektronische Aktenarchivierung bzw. im weiteren die elektronische Aktenführung mittelfristig anzustrebendes Ziel sein.

Der Zugang der Einsichtnehmenden wird über das CityInformationssystem (CIS-RN) der Stadt Rathenow erfolgen. Bei größeren Datenmengen kann dann auch die Bereitstellung von CDs oder anderen Massenspeichermedien erfolgen. Die Einsichtnahme kann durch Übersenden von Mails und Dateien bzw. durch legitimierten (Nutzername/Password) Zugriff auf einen Datenserver erfolgen.

Ein direkter Durchgriff auf die elektronische Akte durch den Einsichtnehmenden soll vermieden werden. Vielmehr soll die endgültige Entscheidung über die Einsicht und die Bereitstellung der Daten durch den zuständigen Sachbearbeiter erfolgen.

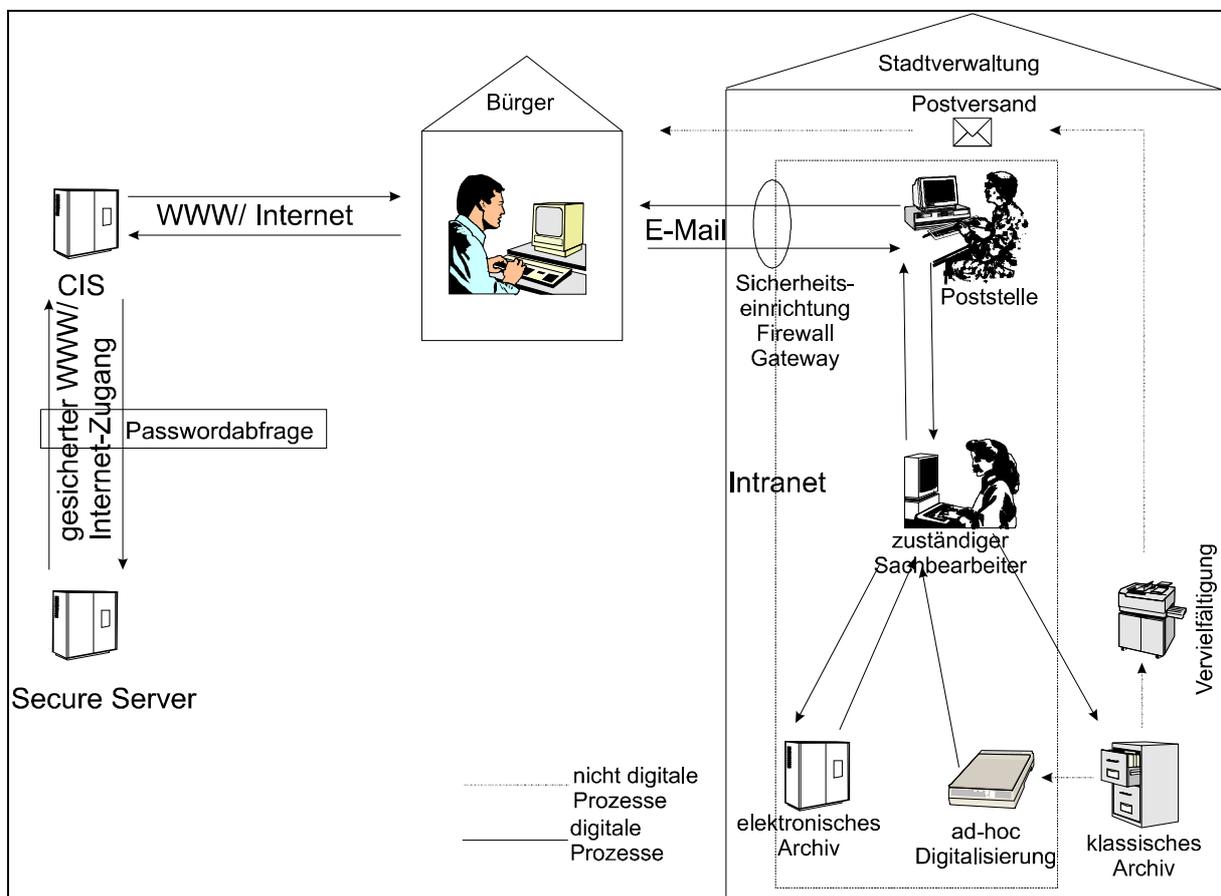
Die Identifizierung des Online-Antragstellers erfolgt mittels Digitaler Signatur. Hierdurch ist eine hinreichende Sicherheit der Identifizierung gegeben. Eine genauere Ausführung zur Problematik „Identifizierung“ findet sich unter dem Teilprojekt „Digitale Signatur“ und wird an dieser Stelle nicht weiter ausgeführt. Mit dem OSGV gibt es dazu eine Arbeitsgruppe, die die Realisierung vorbereitet.

Die Authentizität der bereitgestellten Informationen wird ebenfalls durch den Einsatz der Digitalen Signatur sichergestellt.

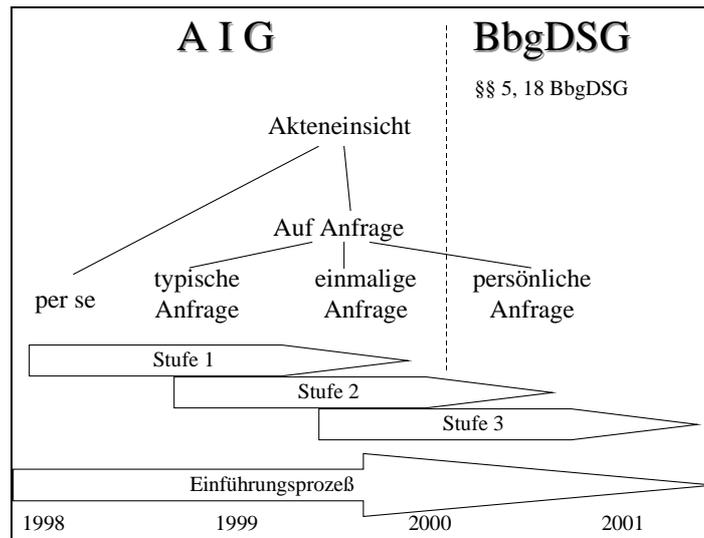
Im folgenden Schaubild wird die technische Ausgestaltung der elektronischen Akteneinsicht verdeutlicht. Der Bürger kann über das Internet auf die ständig verfügbaren Informationen zugreifen. Zu den Akten, die auf diesem Wege einzusehen sind, gehören unter anderem: Gesetze, Verordnungen, Satzungen, Protokolle und Vorlagen der öffentlichen Stadtverordnetenversammlungen. Die Einsicht in den B-Plan ist jedoch kostenpflichtig, und würde über den gesicherten Server erfolgen. Bei Daten, deren Einsicht gebührenpflichtig ist, erfolgt der Zugriff nach vorheriger Anmeldung und der Übergabe eines Accounts mit Passwort. Anhand dieses Accounts erfolgt dann die Gebührenzahlung mittels e-cash, Bankeinzug oder Rechnung.

Über E-Mail kann der Bürger die Einsicht in Akten beantragen, die nicht generell zur Einsicht zur Verfügung stehen dürfen. Dazu gehören unter anderem auch seine persönlichen Akten. Er stellt den Antrag mittels einer digital signierten und verschlüsselten E-Mail bzw. Formulare, der an die Poststelle der Verwaltung gesendet wird. Hier

wird er entschlüsselt und anhand des öffentlichen Schlüssels des Senders überprüft. Ist die Prüfung erfolgreich, stellt der Eingangsbearbeiter die Anfrage dem zuständigen Sachbearbeiter im lokalen Bürokommunikationssystem zu. Wenn der Antrag unberechtigt ist oder aus anderen rechtlichen Gründen versagt werden muß, erhält der Bürger eine digital signierte und verschlüsselte E-Mail mit dem abschlägigen Bescheid. Im Bewilligungsfalle entscheidet sich das weitere Vorgehen nach der Aktenablage. Ist die Akte im digitalen Archiv, wird sie aus diesem heraus weiter bearbeitet. Liegt die Akte noch nicht elektronisch vor, wird sie dem Bürger entweder als Kopie auf dem Postweg zugesendet oder digitalisiert. Die digital vorliegende Akte geht an die Poststelle, die diese dem Bürger digital signiert und verschlüsselt zusendet.



Das Vorgehen bei der Realisierung der Akteneinsicht richtet sich nach den Spezifika der Aktenbestände und der daraus resultierenden Einsichtnahme. Allgemein lässt sich die Akteneinsicht in folgende Typologien einteilen.



- per se

Zu diesem Aktenbereich mit einem generellen Einsichtsrecht gehören die Dokumente, deren Inhalt auf den Lebensbereich möglichst vieler einwirkt, aber keine persönlichen Bezüge enthält sowie keinen besonderen Geheimhaltungspflichten unterliegt. Hierunter fallen z.B. Protokolle der öffentlichen Sitzungen der Stadtverordneten, Verwaltungsvorschriften und Satzungen.

- typische Anfrage

Hierunter fallen Akten mit aktuellem Bezug bzw. häufiger Nachfrage. Diese Akten werden außer im Archivsystem der Verwaltung zusätzlich auf einem öffentlich zugänglichen Server vorgehalten. Auf diesen können Interessenten entweder pauschal kostenfrei, bzw. wenn in der Gebührensatzung entsprechende Regelungen vorgesehen sind, auch nach Anmeldung innerhalb eines geschlossenen Benutzerkreises kostenpflichtig zugreifen.

Beispiele für diesen Aktentyp sind: B-Pläne, Flurkarten, FNP. Diese Informationen sind in der einfachen Form für Bauherren zur Vorbereitung des Planungsprozesses von Interesse. Architekten, Baufirmen und Investoren benötigen darüber hinaus Daten, die sie medienbruchfrei in ihre Planungsverfahren integrieren können.

Ein besonderer Fall der typischen Anfrage ist die Melderegisterauskunft. Dieser unterliegt zwar nicht originär dem AIG sondern den spezifischen Regelungen des Pass- und Meldewesens, stellt aber einen nicht unerheblichen Anteil am Anfrageaufkommen dar. Bei der einfachen Melderegisterauskunft, die jedem Bürger zur Verfügung steht, wird die Anfrage durch den zuständigen Mitarbeiter bearbeitet und das Ergebnis dem Anfragenden elektronisch (verschlüsselt und signiert) zugeleitet. Die erweiterte Melderegisterauskunft steht dagegen nur einer geschlossenen Benutzergruppe kostenpflichtig zur Verfügung.

- einmalige Anfrage

Diesem Bereich werden alte Akten zugeordnet, deren ständige Bereithaltung nicht effektiv ist. Diese Akten weisen ein geringes Nachfrageaufkommen auf. Eine entsprechende Einspeisung, d.h. die elektronische Zurverfügungstellung der gewünschten Informationen, wird dann auf Antrag vorgenommen. Auf diese Weise wird vermieden, dass neben dem notwendigen elektronischen Archiv übermäßig Speicherressourcen benötigt werden.

- persönliche Anfrage

Über eine persönliche Anfrage kann auf der Basis des BbgDSG bzw. bei laufenden Verfahren auf der Grundlage der entsprechenden Verfahrensgesetze Einsicht in die eigenen Daten genommen werden. Hierzu ist eine sichere Identifizierung des Antragstellers notwendig sowie zur Gewährleistung des Datenschutzes eine Verschlüsselung der Daten. Die herauszugebenden Daten werden nach Prüfung durch den Bearbeiter für jeden Antrag extrahiert und dem Antragsteller zur Verfügung gestellt. Ein direktes Zugreifen des Antragstellers auf das Archiv sowie eine weitere Speicherung des Auskunftsdatensatzes erfolgt nicht. Diese Regelung entspricht den datenschutzrechtlichen Anforderungen.

### **Vorgehensweise NetCity**

In der ersten Stufe werden Akten allgemeiner Zugänglichkeit zur Einsicht freigegeben. Dies betrifft u.a. Ratsdokumente aus der Stadtverwaltung, soweit sie öffentliche Sitzungen betreffen, Proto-

kolle der öffentlichen Sitzungen der Stadtverordnetenversammlung und Verwaltungsvorschriften. Da diese in der Regel elektronisch erfaßt werden, steht einer öffentlichen Einsichtnahme nichts im Wege. Dies ist bereits in der Realisierung und wird bis voraussichtlich Ende 1999 abgeschlossen sein. Eine entsprechende Information der Bürger erfolgte über die Stadtverordnetenversammlung, der das Projekt am 25.11.1998 öffentlich vorgestellt wurde.

Die folgenden Stufen beinhalten die Einbeziehung der eigentlichen Verwaltungsakten. In der zweiten Stufe wird zunächst einmal aus dem Bestand von rund 7 Mio. Blatt Akten im Archiv der Stadtverwaltung ein besonders interessanter Teilbereich herausgesucht, dessen Akten digitalisiert werden; wie z.B. die Bereiche Bau, Liegenschaften, Straßenverkehr, Ordnung und Sicherheit. Diese sind dem Typus der typischen Anfrage zuzuordnen.

Hierbei wird zudem eine Akten-Check-Liste entwickelt, nach der überprüft werden kann, ob eine Einsicht gewährt werden kann. Hierfür müssen der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht mit hinzugezogen werden.

In der dritten Stufe werden dann die Einzelfallanfragen realisiert.

### **Partner bei der Umsetzung**

Als Partner sind in diesem Projekt neben der Firma UDM und der Projektgruppe Media@Komm noch der Landesbeauftragte für den Datenschutz und das Recht auf Akteneinsicht, das Landesamt für Datenverarbeitung und Statistik und die DISOS GmbH involviert.

- Digitalisierungsvolumen

Die Kosten für die Digitalisierung gliedern sich in volumenabhängige und volumenunabhängige Aufwendungen. Im Falle Rathenows wurden bereits ca. 40% des Aktenarchivs elektronisch erstellt und liegen demzufolge bereits in digitaler Form vor. Daraus ergibt sich, dass von den vorhandenen 1014 laufenden Metern Akten noch knapp 608 laufende Meter in nicht digitaler Form vorliegen.

Anhand der Erfahrungen eines Wirtschaftsunternehmens bei der Digitalisierung vorhandener Akten werden im Folgenden die notwendigen Aufwendungen für Rathenow abgeschätzt, wobei sich Änderungen aufgrund der technischen Entwicklung ergeben können. Die volumenunabhängigen Kosten fallen bereits in der ersten Phase an, da hier die notwendigen Hardwarebeschaffungen erfolgen müssen. In den folgenden Phasen werden dann die Akten schrittweise digitalisiert.

- Volumenunabhängige Kosten

Zu dieser Kostenart zählen die Aufwände, die generell notwendig sind, unbeschrieben der anfallenden Datenmenge und Vorgangszahlen. Die Erfahrungen aus vergleichbaren Projekten im privatwirtschaftlichen Sektor lassen für den technischen Bereich einen Ansatz von ca. 210 TDM erwarten. Darin sind die Kosten für Soft- und Hardware des Digitalisierens und Speicherns enthalten. Eine genaue Spezifikation der Hard- und Softwareplattform erfolgt basierend auf den Ergebnissen der Projektgruppe „Interaktive Verwaltung“.

- Volumenabhängige Kosten

Hierzu zählen die Aufwendungen, die sich in Abhängigkeit von der Datenmenge und Vorgangszahl ergeben. So betragen die Arbeitskosten pro gescanntem Blatt 0,15 DM. Dazu kommen noch die Vorbereitungsarbeiten von ca. 50,00 DM/h und die zu erstellenden CDs.

Für Rathenow wurde im Rahmen des Teilprojektes „elektronische Akteneinsicht“ eine detaillierte Aktenanalyse durch die Archivarin vorgenommen. Dabei ergab sich folgende Archivstruktur:

<i>Bereich</i>	<i>Kürzel</i>	<i>lfd. Meter</i>
Ordnungsamt	OA	86
Kämmerei	KÄ	198
Archiv	AR	312
Sozialamt	SO	167
Lohnbüro	LB	15
Personal	PA	12
Rechnungsprüfung	RP	10
Rechtsamt	RA	19
Hauptamt	HA	45
Wirtschaftsamt	WA	93
Bildung, Kultur, Sport	BKS	27
Bürgermeister	BM	30
<b>Gesamt</b>		<b>1014</b>

Auf dieser Basis ergibt sich für Rathenow ein Digitalisierungsumfang von rund 610 lfd. Meter Akten, die gemäß obiger Aufstellung zu einem Datenvolumen von ca. 4,2 bis 4,9 Mio. A4-Seiten führen würden.

Die gesamte Stadtverwaltung umfasst demnach eine Archivmenge von 1014 Metern; dies entspricht 3,5 cm pro Bürger. Bezogen auf die 2.600.000 Bürger Brandenburgs kann ein zu digitalisierendes Aktenvolumen im Kommunalbereich von 90,9 km unterstellt werden.

Diese Zahl unterstreicht, dass eine Gesamtdigitalisierung von Akten fachlich und finanziell wenig sinnvoll wäre. Daher muss eine Gewichtung der Akten nach Digitalisierungsrelevanz vorgenommen werden. Nach der erfolgten Zuordnung des Aktenbestandes zu den Kriterien Schutzwürdigkeit und Zugriffsfrequenz wurden u.a. folgende Aktenbereiche zur Digitalisierung in der Pilotphase ausgewählt:

Ausschreibungsunterlagen, Projekte, Konzepte, Satzungen, Beschlüsse, Schulentwicklungsplanung, Turnhallenbelegung, Bewirtschaftungsunterlagen Kita, Bebauungspläne, Vorhaben- und Erschließungspläne, Flächennutzungspläne, Straßenverzeichnis/ Aufbruchverzeichnis.

## **5. Ausblicke**

- Weiterer Ausbau des NetCity-Projektes
- Fertigstellung des CIS-RN
- Weiterführung des Media@Komm-Projektes (elektronische Akteneinsicht)
- Aufbau eines virtuellen Bürgeramtes