Alcatel SEL Stiftung
für Kommunikations-
forschung

DEUTSCHE GESELLSCHAFT FÜR
RECHT UND INFORMATIK E.V

Internationales Symposium
Informationsfreiheit und Datenschutz
in der erweiterten Europäischen Union

8./9. Oktober 2001 in Potsdam

Veranstaltung des
Landesbeauftragten für den Datenschutz
und für das Recht auf Akteneinsicht
in Zusammenarbeit mit der
Alcatel SEL Stiftung für Kommunikationsforschung
und der Deutschen Gesellschaft für
Recht und Informatik e.V.
mit Unterstützung der DaimlerChrysler AG

Dokumentation

In der Reihe „Potsdamer Materialien zu Akteneinsicht und Informationszugang“ sind bisher erschienen:

Band 1: Dokumentation Internationales Symposium Informationsfreiheit und Datenschutz 25./26. Oktober 1999

Band 2: Dokumentation Internationales Symposium Informationsfreiheit und Datenschutz in der erweiterten Europäischen Union 8./9. Oktober 2001

Impressum

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

Dezember 2001

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

E-Mail: Poststelle@LDA.Brandenburg.de
Internet: http://www.lda.brandenburg.de

Fingerprint: 0DD70C8A 65508B73 2A53EFEE AC857D66

Druck: Sonnendruck Druckerei und Verlag GmbH, Belzig

Inhalt

Vorwort

Informationsfreiheit und Datenschutz sind seit Verabschiedung der Europäischen Grundrechte-Charta wesentliche Bestandteile der entstehenden Europäischen Verfassung und gehören damit auch zu den rechtlichen Regelungen, die die beitrittswilligen Staaten Mittel- und Osteuropas als „acquis communautaire“ in ihre Rechtsordnungen aufzunehmen haben. Die regelmäßigen Berichte der Kommission über den Stand der Beitrittsvorbereitungen in den einzelnen Ländern geben hierüber Auskunft. Zugleich können sich aber auch die Länder Westeuropas die Erfahrungen zunutze machen, die etwa in Ungarn mit dem ersten in Europa verabschiedeten Informationszugangs- und Datenschutzgesetz gemacht worden sind. Die bevorstehende Erweiterung der Europäischen Union wird deshalb keine Einbahnstraße in west-östlicher Richtung sein.

Wir haben diesen Prozess zum Thema unseres diesjährigen Symposiums gemacht, das gemeinsam mit der Alcatel SEL Stiftung für Kommunikationsforschung und der Deutschen Gesellschaft für Recht und Informatik veranstaltet wurde und dessen Vorträge in diesem zweiten Band der „Potsdamer Materialien zu Akteneinsicht und Informationszugang“ dokumentiert werden. Ich danke auch an dieser Stelle den Referentinnen und Referenten aus dem In- und Ausland, den Mitveranstaltern und allen Mitarbeiterinnen und Mitarbeitern sehr herzlich dafür, dass sie diese Veranstaltung möglich gemacht haben.

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

Eröffnung des Internationalen Symposiums

Ich begrüße Sie herzlich zu unserem diesjährigen Internationalen Symposium in Potsdam. Ich tue dies zugleich im Namen der Alcatel SEL Stiftung für Kommunikationsforschung und der Deutschen Gesellschaft für Recht und Informatik, mit denen wir dieses Symposium gemeinsam veranstalten.

Es freut mich ganz besonders, den Ministerpräsidenten des Landes Brandenburg, den Präsidenten des Landtages Brandenburg und den Bürgermeister der Landeshauptstadt Potsdam bei uns begrüßen zu können.

Wir haben das Symposium, das wir nach 1999 zum zweiten Mal veranstalten, unter das Thema "Informationsfreiheit und Datenschutz in der erweiterten Europäischen Union" gestellt. Unserer Einladung sind zahlreiche Datenschutzbeauftragte aus mittel- und osteuropäischen Ländern gefolgt, die sich gegenwärtig auf den Beitritt zur Europäischen Union vorbereiten. Stellvertretend für sie möchte ich die Datenschutzbeauftragte unseres Nachbarlandes Polen, Frau Dr. Kulesza, herzlich begrüßen. Unter den Teilnehmenden sind auch Datenschutzexperten aus Neuseeland und Großbritannien, die ich ebenfalls herzlich begrüße.

Ich freue ich mich ebenso über die Teilnahme der Datenschutzbeauftragten aus Bund und Ländern sowie vieler behördlicher Datenschutzbeauftragter aus dem Land Brandenburg. Seien Sie alle herzlich willkommen!

Informationsfreiheit und Datenschutz stehen angesichts der Terroranschläge in den USA gegenwärtig vor einer besonderen Herausforderung. In den vergangenen Wochen sind Rufe nach einer pauschalen Einschränkung des Menschenrechts auf Datenschutz laut

geworden. Dies sei erforderlich, um die innere Sicherheit zu verbessern.

Dem habe ich gemeinsam mit den Datenschutzbeauftragten des Bundes und der übrigen Länder entgegengehalten, dass die Sicherheitsbehörden bereits heute über weitreichende Befugnisse zur Datenverarbeitung verfügen. Vollzugsdefizite können nicht dem Datenschutz angelastet werden. Vor übereilten Maßnahmen des Gesetzgebers ist zu warnen. Soweit im Detail eine Anpassung der Gesetzgebung an die neue Bedrohung tatsächlich notwendig ist, sind die Datenschutzbeauftragten zu einem konstruktiven Dialog bereit.

Jede künftige Gesetzgebung muss aber die grundlegenden Prinzipien des Rechtsstaats, zu denen auch das Grundrecht der freien Entfaltung der Persönlichkeit - und ich füge hinzu - die Transparenz staatlichen Handelns zählen, respektieren. Würden diese Grundregeln einer offenen Gesellschaft ohne erkennbaren Sicherheitsgewinn aufs Spiel gesetzt, so hätten die Feinde der offenen Gesellschaft eines ihrer Ziele bereits erreicht.

Notwendig ist stattdessen gerade in der gegenwärtigen Situation - wie der französische Premierminister dieser Tage zu Recht betont hat - eine Stärkung der unabhängigen Datenschutzbeauftragten, denen die Aufgabe zukommt, als vertrauenswürdige Instanz auf die Einhaltung der Balance zwischen den öffentlichen Sicherheitsinteressen und dem informationellen Selbstbestimmungsrecht der Einzelnen zu dringen.

Die Erweiterung der Europäischen Union rückt immer näher. Sie wird bisher überwiegend unter den - sicher wichtigen - Aspekten der wirtschaftlichen und arbeitsmarktpolitischen Auswirkungen sowohl in den Beitrittsländern als auch in den bisherigen Mitgliedstaaten der Union diskutiert. Ein weiterer, mindestens ebenso wichtiger Aspekt der Erweiterung ist bisher in der Öffentlichkeit zu wenig beachtet worden: Der Schutz der Grundrechte aller Bürgerinnen und Bürger in der Europäischen Union muss gestärkt werden. Zu diesem Zweck ist im vergangenen Jahr in Nizza die Charta der Grundrechte der Europäischen Union verkündet worden, zu denen auch der Informationszugang und der Datenschutz als Bestandteile eines Rechts auf gute Verwaltung gehören.

Die Länder Mittel- und Osteuropas, die den Beitritt zur Union anstreben, unternehmen gegenwärtig große Anstrengungen, um ihre Rechtssysteme dem Gemeinschaftsrecht entsprechend umzugestalten. Dies betrifft auch Regelungen zu Datenschutz und Informationsfreiheit. Brandenburg als Verbindungsland zwischen der gegenwärtigen Europäischen Union und den Beitrittskandidaten hat hier eine wichtige Brückenfunktion.

Als Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht will ich daher mit meinen Mitarbeiterinnen und Mitarbeitern den bereits begonnenen Aufbau unabhängiger Datenschutzbehörden in den mittel- und osteuropäischen Ländern unterstützen, wenn dies gewünscht wird. Es ist ein wichtiges Signal, dass der Landtag Brandenburg zu diesem Zweck die Durchführung unseres Symposiums ermöglicht hat; ich hoffe, dass die Politik uns auch weiterhin die nötige Rückendeckung hierfür geben wird.

Dabei geht es nicht um eine Einbahnstraße: Vielmehr können wir in Brandenburg auch von den Erfahrungen lernen, die in den beitrittswilligen Ländern (z.B. in Ungarn) gemacht worden sind und werden. Das wird - so hoffe ich - in diesen beiden Tagen deutlich werden.

Ich wünsche uns allen heute und morgen interessante Vorträge und anregende Gespräche.

Dr. Manfred Stolpe
Ministerpräsident des Landes Brandenburg

Grußwort zur Eröffnung

Im Namen der Landesregierung heiße ich Sie in Brandenburg sehr herzlich willkommen.

Begrüßen möchte ich insbesondere die Teilnehmer aus den mittelosteuropäischen Ländern, die schon bald die Europäische Union nicht nur erweitern, sondern vor allem bereichern werden. Ihre Anwesenheit macht diese Veranstaltung zu einem Dialog von europäischem Rang.

Ich freue mich, dass in diesem Jahr nach 1999 schon zum zweiten Mal ein hochrangiges Symposium zum Thema Datenschutz in Potsdam stattfindet. Dafür möchte ich dem Landesbeauftragten für Datenschutz und für das Recht auf Akteneinsicht Dank sagen.

Dank gilt auch der Alcatel-Stiftung für Kommunikationsforschung, die bei der Verwirklichung der Konferenz ganz wesentlich geholfen hat, ebenso wie der Deutschen Gesellschaft für Recht und Informatik und der DaimlerChrysler AG, die diese Tagung unterstützt haben.

Zur Sache: Informationsfreiheit und Datenschutz sind heiß diskutierte Fragen. Nicht erst seit den entsetzlichen Terrorattacken auf die USA machen wir uns Gedanken über das Verhältnis von informatorischer Selbstbestimmung und anderen öffentlichen Interessen. Mit der Osterweiterung der Europäischen Union tritt das Problem einheitlicher Standards im gesamteuropäischen Rechtsraum mit neuer Dringlichkeit auf die Tagungsordnung.

Der Zugang zu amtlichen Informationen und damit die Verbesserung der Transparenz behördlicher Arbeit ist innerhalb der Europäischen Union zunehmend ein Thema. Auch auf die Länder, die der Union beitreten wollen, kommen daher Reformaufgaben zu. Nachdem das Recht auf Informationszugang in der Grundrechte-Charta

der Europäischen Union verankert worden ist, haben jetzt das Europäische Parlament und der Rat eine Verordnung über den öffentlichen Zugang zu Dokumenten der europäischen Institutionen vorgelegt.

Damit soll eine verstärkte Beteiligung der Bürgerinnen und Bürger an den Entscheidungsprozessen der EU-Gremien ermöglicht werden. Die Verantwortlichkeit der Verwaltung gegenüber dem Bürger soll gestärkt werden. Brandenburg begrüßt und unterstützt diese Entwicklung. Als ostdeutsches Bundesland mit einer modernen Verfassung haben wir vor zehn Jahren bei der Neugründung des Landes neue Maßstäbe der Informationsfreiheit gesetzt. Das Recht auf Zugang zu behördlichen Informationen hat in Brandenburg Verfassungsrang.

In Ausgestaltung dieses Verfassungsauftrages wurde im März 1998 in Brandenburg als erstem Land in Deutschland ein Informationsfreiheitsgesetz in Kraft gesetzt. Diesem Beispiel folgten die Länder Berlin und Schleswig-Holstein mit eigenen Regelungen.

Auch im Hause des Bundesinnenministers wird derzeit an dem Entwurf eines für die Bundesbehörden geltenden Informationsfreiheitsgesetzes gearbeitet.

Dem öffentlichen Informationszugang auf der einen Seite steht auf der anderen Seite der Schutz des Rechts auf informationelle Selbstbestimmung gegenüber. Über die Möglichkeiten und Grenzen der Informationsfreiheit müssen wir uns also verständigen. Dieser immens wichtigen Aufgabe widmen Sie sich auf Ihrer Tagung. Dabei nehmen Sie zu Recht eine europäische Perspektive ein. Gemeinsam mit unseren Partnern in Mittel- und Osteuropa müssen wir die Reformen beraten und verwirklichen.

Dies gilt umso mehr, als die Europäische Union für den Datenschutz einheitliche rechtliche Standards gesetzt hat, die in den Mitgliedsstaaten umgesetzt werden mussten und mit denen sich auch die Beitrittskandidaten auseinandersetzen werden. Der Schutz personenbezogener Daten ist im Zeitalter der elektronischen Kommunikation eine große Herausforderung. Nicht zuletzt mit der EU-Erweiterung und der damit verbundenen Ausweitung und Vertiefung

der wirtschaftlichen Kontakte wird der Austausch von sensiblen personenbezogenen Daten weiter zunehmen. Die Behörden nutzen immer mehr die Möglichkeiten der elektronischen Kommunikation. Sie sind aus einer modernen Verwaltung nicht mehr wegzudenken.

Und auch hier steht der großen Chance der schnellen und leichten Kommunikation zwischen Bürgern und Behörden das Gebot des Schutzes der übermittelten Daten gegenüber. Auch darüber werden Sie während dieser Tagung sprechen. Dieses Symposium wird einen fundierten Überblick über die Vielfalt der rechtlich und wirtschaftlich relevanten Fragen der Informationsfreiheit und des Datenschutzes in der erweiterten Europäischen Union geben.

Damit schärfen Sie das Problembewusstsein der Politik und die Handlungskompetenz der Verwaltung. In diesem Sinne wünsche ich Ihnen einen ertragreichen und konstruktiven fachlichen Austausch! Danke für Ihr Kommen! Danke für die Bereitschaft der Mitarbeit!

Dr. Herbert Knoblich
Präsident des Landtages Brandenburg

Grußwort zur Eröffnung

Als ich im April Ihre Einladung erhielt, auf diesem Symposium ein Grußwort zu halten, war die Welt noch in Ordnung, hätte man mit dem Thema Ihrer Veranstaltung etwas lockerer umgehen können. Das hat sich mit den furchtbaren Terroranschlägen auf die USA verändert. Allerdings bin ich froh, dass sich nach ersten verständlichen Aufgeregtheiten inzwischen die Diskussion wieder versachlicht hat, die allzu simple Warnung, Datenschutz dürfe nicht zum Terroristenschutz werden, nicht mehr wiederholt wurde. Denn wer von den Datenschützern wollte sich schon zum Handlanger von Terroristen machen - eine abenteuerliche Vorstellung.

Dabei ist vieles, was jetzt so in der Veränderungsdiskussion ist - ich denke beispielsweise an das Ausländerzentralregister und den Zugriff darauf von Polizei und Verfassungsschutz -, heute schon möglich. Nur wurden diese Möglichkeiten anscheinend nicht ausreichend genutzt. Das lag aber wohl nicht an den Datenschutzbeauftragten. Sie werden auch die Letzten sein, die sich wirklich notwendigen Änderungen verschließen, wenn es dem Wohl und der Sicherheit der Allgemeinheit dient. Allerdings sollten wir nicht so tun, als ob es in diesem Bereich mit nationalen Alleingängen getan wäre. Hier bedarf es natürlich der Abstimmung zumindest mit unseren europäischen Partnern, wenn das Ganze einen Sinn machen soll.

Und da bleibt - aber wem sage ich das - noch viel zu tun. Dabei hat es in den vergangenen Jahren unbestritten Anstrengungen zur Harmonisierung gegeben. Denken Sie an die "Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr". Allerdings haperte es bei einigen Mitgliedsstaaten mit der rechtzeitigen Umsetzung.

Selbst die Bundesrepublik - so war dem Jahresbericht der von EU-Parlament und Rat eingesetzten Datenschutzgruppe für das Berichtsjahr 1999 zu entnehmen - wurde "wegen der nicht erfolgten Notifizierung aller zur Umsetzung der Richtlinie 95/46/EG erforderlichen Maßnahmen" beim Europäischen Gerichtshof verklagt. Da ist es dann auch wenig tröstlich, sich in ehrbarer Gesellschaft mit Frankreich, Luxemburg, Irland und den Niederlanden befunden zu haben.

Pfleglicher ging man deutscherseits mit der Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation vom Dezember 1997 um. Hier wurde alles rechtzeitig in nationales Recht umgesetzt. Aber wieder landeten vier Mitgliedsländer vor dem Kadi. Verwunderlich ist das natürlich nicht - denn selbst im eigenen Land gehen ja die Ansichten über den Sinn des Datenschutzes bisweilen weit auseinander. Aber die Europäische Gemeinschaft ist nun einmal - wenn sie denn funktionieren soll - auf Rechtsgleichheit angewiesen. Das erwarten zumindest die Menschen.

Gerade ich als gelernter DDR-Bürger habe die Informationsfreiheit und den Datenschutz als eine besondere Errungenschaft der Nach-Wendezeit empfunden. Und ich bin stolz darauf, dass wir dies so eindeutig in unserer Landesverfassung festgeschrieben haben.

Unter der Generalüberschrift "Freiheit, Gleichheit und Würde" steht in Artikel 11, Abs. 1: "Jeder hat das Recht, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen, auf Auskunft über die Speicherung seiner persönlichen Daten und auf Einsicht in Akten und sonstige amtliche Unterlagen, soweit sie ihn betreffen und Rechte Dritter nicht entgegenstehen. Personenbezogene Daten dürfen nur mit freiwilliger und ausdrücklicher Zustimmung des Berechtigten erhoben, gespeichert, verarbeitet, weitergegeben oder sonst verwendet werden." Einschränkungen sind nur auf gesetzlicher Grundlage und "im überwiegenden Allgemeininteresse" zulässig.

Über dieses Recht hinaus hat jeder Brandenburger Bürger ein von

dieser persönlichen Betroffenheit unabhängiges Informationsrecht, das in Artikel 21, Abs. 4 unserer Verfassung verankert ist: "Jeder hat nach Maßgabe des Gesetzes das Recht auf Einsicht in Akten und sonstige amtliche Unterlagen der Behörden und Verwaltungseinrichtungen des Landes und der Kommunen, soweit nicht überwiegende öffentliche oder private Interessen entgegenstehen." Ich gestehe freimütig, dass dies seit 1992 Verfassungsrecht ist, wir aber erst 1998 die gesetzliche Grundlage dafür geschaffen haben.

Es wird Sie nicht verwundern, dass es deshalb so lange gedauert hat, weil die unterschiedlichsten Bedenken und Befürchtungen gegen ein solches Akteneinsichts- und Informationszugangsgesetz vorgebracht wurden. Inzwischen hat aber wohl der letzte Bedenkenträger eingesehen, dass nichts so heiß gegessen wird, wie es gekocht wird. Es wurde keine Verwaltung durch übermäßige Anfragen lahmgelegt, noch haben außerbrandenburgische Institutionen den Schriftverkehr mit uns eingestellt.

Sie wollen sich heute und morgen mit dem Thema "Informationsfreiheit und Datenschutz in der erweiterten Europäischen Union" auseinandersetzen. Das dürfte auch angesichts der eingangs geschilderten neuen internationalen Situation eine interessante Diskussion werden. Zumindest was die Informationsfreiheit angeht, ist Europa jetzt auf Brandenburger Niveau. Der Amsterdamer-Vertrag hatte die Regierungen der Mitgliedsländer verpflichtet, bis zum 1. Mai dieses Jahres Regeln festzulegen, nach denen die europäischen Bürger Zugang zu den Dokumenten von EU-Kommission, Ministerrat und Europaparlament bekommen. Das ist per Verordnung vom 30. Mai 2001 geschehen. Wenn jetzt ein Bürger einen Antrag auf Einblick stellt, muss er innerhalb von 15 Arbeitstagen beantwortet werden. Wird die Anfrage abgelehnt, hat er die Möglichkeit, zunächst einen Zweitantrag zu stellen und bei Nichteinhaltung der Antwortfrist die Gerichte anzurufen.

Sie werden es mir nachsehen, dass ich mich angesichts des hier versammelten geballten in- und ausländischen Sachverstands nicht in weitere Details versteige und dadurch Gefahr laufe, aus dem Tritt zu kommen. Gerade weil diese Thematik eine so große Bedeutung

für jeden Einzelnen von uns hat, wünsche ich Ihnen fruchtbare Diskussionen, verwertbare Ergebnisse und Ihrer Veranstaltung insgesamt viel Erfolg. Mir bleibt nur noch, Sie im Land Brandenburg und seiner Landeshauptstadt Potsdam ganz herzlich willkommen zu heißen. Vielleicht haben Sie ja trotz Ihrer umfangreichen Agenda etwas Zeit, den Charme der Stadt auf sich wirken zu lassen.

Jann Jakobs
Bürgermeister der Landeshauptstadt Potsdam

Grußwort zur Eröffnung

Ich möchte Sie in Potsdam herzlich willkommen heißen.

Das Internationale Symposium zu Problemen der Informationsfreiheit und des Datenschutzes findet ja bereits zum 2. Mal in Potsdam statt. Seit Ihrer letzten Tagung 1999 hat sich in Potsdam viel getan.

Höhepunkt in diesem Jahr war natürlich die Bundesgartenschau.

Durch die BUGA haben die Innenstadt, die innerstädtischen Havelräume, die berühmte Potsdamer Feldflur, sowie die verwahrlosten ehemaligen Militärflächen hier im Potsdamer Norden einen enormen Entwicklungsschub erhalten.

Wenn Sie sich die Zeit nehmen unsere Stadt zu erkunden, werden Sie feststellen, dass sich in allen vier Kulissen das Gesicht der Stadt verschönert hat. Diese neue Lebensqualität wird Potsdam dauerhaft bereichern.

Informationsbedarf und Informationsmöglichkeiten in Staat und Wirtschaft sind enorm gestiegen.

Wegen der steigenden Bedeutung des internationalen Datenverkehrs, insbesondere vor dem Hintergrund der sprunghaft wachsenden Nutzung des Internet, kommt der Kooperation auf europäischer und internationaler Ebene immer mehr Bedeutung zu.

Auch die Stadtverwaltung Potsdam bietet Bürgern die Möglichkeit des elektronischen Zugriffs auf Angebote des "Virtuellen Rathauses".

Hier hat der Datenschutz eine wichtige Aufgabe. Er muss die Entscheidungsfreiheit der Bürger im Umgang staatlicher Stellen mit ihren persönlichen Daten gewährleisten.

Die Informationsfreiheit wird in allen Fällen an ihre Grenzen stoßen, in denen der Schutz personenbezogener Daten als höheres Rechtsgut einzustufen ist. Rechtsvorschriften, die diese Grenzen nicht klar definieren, verkomplizieren diese Sachverhalte.

Hier sehe ich die Möglichkeiten über diese Tagung neue Impulse zur Vereinheitlichung des Datenschutzes in der Europäischen Union zu geben. Angesichts der aktuell politischen Situation, wird auch der Datenschutz vor eine neue Herausforderung gestellt.

Bei der Fahndung nach den Hintergründen der Terroranschläge müssen Möglichkeiten gefunden werden, verschiedenste Daten für eine eventuelle Strafverfolgung auszuwerten und dennoch ist prinzipiell das Recht des Datenschutzes des Einzelnen zu gewährleisten.

Insbesondere in diesem Bereich ist ein internationaler Erfahrungsaustausch unumgänglich. Auch hier dürfte es einen immensen Diskussionsbedarf geben.

Für Ihr Symposium wünsche ich Ihnen konstruktive Beiträge und anregende Diskussionen.

Prof. Dr. Wolfgang Hoffmann-Riem
Richter des Bundesverfassungsgerichts

Voraussetzungen der Informationsfreiheit

I. Vorbemerkung

Das Thema der Informationsfreiheit darf sich nicht darin erschöpfen, nur nach einem subjektiven Recht auf Informationszugang zu suchen. Es geht vielmehr um die rechtlichen Voraussetzungen der Nutzung der Produktivkraft "Information" in Staat und Gesellschaft, und zwar nutzbar für die individuelle Entfaltung, aber auch für die Sicherung des Gemeinwohls. In den Blick gerät mehr als das seit langem entwickelte Grundrecht auf informationelle Selbstbestimmung. Die Herausarbeitung dieses Grundrechts in der Zeit der Volkszählung 1983 war überfällig, und zwar nicht nur aus Sorge um den Schutz vor dem Orwell'schen Überwachungsstaat. Die Zunahme der Datenverarbeitung durch den Staat forderte einen grundrechtlichen Schutz der informationellen Entfaltungsfreiheit der betroffenen Bürger.

Heute aber ist diese Sichtweise nicht mehr ausreichend. Wir wissen heute mehr als damals, dass der Zugang zu und die Verarbeitung von Daten nicht nur zu Gefährdungen führen kann. Informationen sind gewissermaßen das Blut einer jeden Gemeinschaft; der richtige Informationsfluss ist Voraussetzung einer lebensfähigen Gesellschaft. Dementsprechend dürfen wir nicht nur auf die Datenverarbeitung durch den und im Staat und nicht nur aus der Perspektive möglicher Gefährdungen sehen. Es geht vielmehr umfassender darum, die Funktionsfähigkeit von informationsgestützten Sozialbereichen zu schützen. Wichtig ist aber auch, die Funktionsfähigkeit der Informationsgesellschaft in einer bestimmten Qualität zu wahren, nämlich unter Erhalt ihrer Freiheitlichkeit. Es geht darum, Freiheitlichkeit für möglichst viele, also nicht nur für Macht- und Informationsstarke zu gewährleisten, und zwar im Sinne einer das reale Leben prägenden Freiheit.

Informationen beziehen sich auf Interaktionen. Kommunikation ist nur frei, wenn es eine Freiheit auf Gegenseitigkeit gibt. Kommunikationsgrundrechte ermöglichen die Freiheit der Entfaltung durch andere, aber auch die Freiheit der Entfaltung mit anderen. Angesichts gegenläufiger Entfaltungsinteressen geht es häufig um die Zuordnung verschiedener Freiheiten zueinander. Gelingende Kommunikation setzt Kommunikations-Chancengleichheit voraus, also im Rahmen des Möglichen das Fehlen von Machtasymmetrien.

Gelingende Kommunikation zu sichern ist schon schwer in der zwischenmenschlichen, von Person zu Person reichenden Kommunikation. Noch schwerer herzustellen ist sie im Bereich der Massenkommunikation; trotz vieler Versuche etwa in Presse- und Rundfunkgesetzen ist es nur teilweise geglückt, hier Kommunikations-Chancengleichheit abzusichern. Schwierigkeiten verursacht auch eine auf Chancengleichheit gerichtete und aufbauende Kommunikation im Bereich computergestützter Kommunikationssysteme, etwa der Individual- und Massenkommunikation im Internet.

Hier - aber auch darüber hinaus - stellt sich die Frage, ob und wie gelingende Kommunikation unter Berücksichtigung der Kommunikations-Chancengleichheit in den zunehmend vernetzten und auch vermachteten (Teil-)Welten der Informationsgesellschaft möglich ist. Insoweit geht es nicht nur um den angemessenen Umgang mit der unüberschaubar gewordenen Datenflut und dem Risiko der Informationsmanipulation. Zu fragen ist auch, wie das Gelingen von Kommunikation unter den Bedingungen der globalen Netzwerkökonomie mit ihren zum Teil neuartigen Vermachtungsrisiken möglich ist. Es gibt z. B. neue, auch virtuell konstruierte, Märkte und Handlungsarenen, die den Informationsfluss zu anderen gesellschaftlichen Bereichen mitsteuern können. Bisherige Selbstverständlichkeiten werden auf breiter Front in Frage gestellt. So erschweren die vielfach beobachtete Heterogenisierung und Pluralisierung von Werten – auch der situativ-opportunistische Umgang mit ihnen – die Orientierung. Auch sind wir noch nicht auf die verstärkt beobachtbaren Entgrenzungen früher klar geschiedener Bereiche eingestellt, etwa die zwischen Staat und Gesellschaft, zwischen Recht und Nichtrecht, zwischen informellem und formalen Handeln, und in räumlicher Hinsicht auf das Agieren in globalen Handlungsarenen.

Die bisherige Rechtsordnung war weitgehend auf der Vorstellung klarer Beziehungen, insbesondere von Zweierbeziehungen, aufgebaut. Auch beruht ein Großteil des öffentlichen Rechts weiterhin auf der Vorstellung, Staat und Gesellschaft seien getrennte und rechtlich trennbare Bereiche. Das private und das öffentliche Recht gehen zwar von Arbeitsteiligkeiten aus, haben aber beispielsweise noch nicht hinreichend die Entstehung hybrider privat-öffentlicher Entscheidungsverbände verarbeitet. Ein Beispiel sind die sog. Private-Public-Partnerships, die es in großer Zahl gibt, und für die ein angemessenes Recht erst entwickelt werden muss. Je komplexer und vernetzter die Wirklichkeit ist, desto wichtiger ist es, Recht auch als Mittel zum Management von Interdependenzen zu verstehen und einzurichten. Das gilt in besonderem Maße für das Informationsrecht.

Auch in der modernen Gesellschaft stellt sich die alte Frage, was darf, vor allem aber: was kann der Staat? Hinzu kommt die Frage, was kann, was darf der Einzelne? Verstärkt wird heute die Frage wichtig, was können, was dürfen Staat und Einzelne im kooperativen Zusammenwirken?

II. Zum Konzept der Grundrechte

Recht gestaltet das Dürfen aus. Dementsprechend ist Freiheit unter dem Grundgesetz nicht anarchische, sondern rechtlich abgesicherte und ggf. in Einzelheiten näher ausgestaltete Freiheit. Durch Recht zu bewältigen sind insbesondere Kollisionen, die bei der Ausübung der Freiheit mit anderen durch den Freiheitsgebrauch gefährdeten Rechtsgütern entstehen können. Ferner sorgt Recht für Rahmenbedingen der Funktionsfähigkeit einer Ordnung, hier der Informationsordnung.

Die Informations- und Kommunikationsfreiheiten beruhen auf der gleichen Idee wie die anderen liberal-rechtsstaatlichen Freiheiten. Es ist die Idee der Freiheit für alle. Die Freiheit wird also kombiniert mit Gleichheit. Freiheit soll das Leben aller prägen, nicht etwa – wie früher – nur das eines bevorrechtigten Adelsstands oder sonstiger Stände oder – auf die Gegenwart bezogen – nur die Entfaltung einzelner Bevölkerungsgruppen und einflussreicher Unternehmen. Er-

kämpft wurde die rechtsstaatliche Freiheit im 18. und 19. Jahrhundert im Zuge der sog. Aufklärung, einem Zeitalter des Umbruchs, das auch an dem historischen Ort dieser Tagung – Potsdam – nachhaltig geprägt wurde. Für dessen intellektuelle Aufbereitung steht Sanssouci im wahrsten Sinne des Wortes. Letztlich verwirklicht wurde die Freiheit der Aufklärung erst im 20. Jahrhundert. In Frage gestellt wird sie jetzt im 21. Jahrhundert. Der Terroranschlag in New York und Washington vom 11. September 2001 ist ein Ausdruck neuer Gefährdungen. Vieles spricht dafür, dass bisherige Selbstverständlichkeiten nicht länger selbstverständlich bleiben und dass das Geschehen am 11. September und vor allem die weltweite Reaktion darauf dieser Beobachtung einen schrecklich sinnfälligen Ausdruck verliehen haben.

Im 18. und 19. Jahrhundert war die Umsetzung der neuen Idee der Freiheit für alle mit dem Kampf um eine radikale Veränderung der gesellschaftlichen Verhältnisse verbunden. Zum Aufbau der neuen Ordnung mussten die überkommenen Machtstellungen, insbesondere die der Fürsten, der Kirchen und der Zünfte, gebrochen werden, die Schichtung der Bevölkerung in verschiedene Stände und Klassen musste aufgehoben werden und dies alles musste parallel zu erheblichen sozialen und technologischen sowie wirtschaftlichen Umbrüchen geschehen. Das ist durchaus gelungen. Heute aber stehen neue Aufgaben der Veränderung vor uns. Gerade dann, wenn wir – um mit Lampedusa zu sprechen – die Dinge erhalten wollen, müssen wir bereit sein, sie zu ändern, also ihre Verwirklichungsbedingungen der jeweiligen Lage anzupassen.

Die Freiheitsrechte waren historisch betrachtet ein wichtiges Mittel zur Veränderung der Gesellschaft. Die revolutionären Bemühungen zielten auf eine neue Struktur der Gesellschaft sowie eine Neuordnung des Verhältnisses zwischen dem Bereich des Staates einerseits und dem der gesellschaftlichen Freiheit andererseits. Gegenwärtig entwickelt sich eine neue Struktur, und zwar weltweit. Dies geschieht nicht als Produkt revolutionärer Bewegungen, sondern evolutionärer Technologieentwicklung und deren ökonomischer Nutzung und durch eine begleitende Veränderung unserer Kulturen. Zu den Wegbegleitern dieses Änderungsprozesses gehören aber auch Ängste.

Die im Zeitalter der Aufklärung entwickelte Freiheitsidee ging davon aus, dass die Freiheit mit Hilfe des Rechts zu verwirklichen sei. An der Wiege der modernen Freiheit stand deshalb auch die Rechtsstaatsidee. Freiheit sollte mit Hilfe des Gesetzes gesichert werden. Das Gesetz hatte insofern zwei Aufgaben. Zum einen ging es darum, die Macht des Monarchen und seiner Regierung und Verwaltung zu begrenzen. Hinzu trat die Aufgabe, die Freiheit vieler miteinander vereinbar zu machen. Auch in diesem Sinne waren Freiheitsrechte ein Programm einer neuen gesellschaftlichen Ordnung, die noch verwirklicht werden musste. Herzustellen war eine Balance zwischen der Macht des Staates als Ordnungskraft einerseits und der Freiheit der Gesellschaft als Lebensfeld andererseits, aber auch eine Balance zwischen den Freiheitsausübungen der verschiedenen Mitglieder der Gesellschaft.

In diesem Sinne waren die Freiheitsrechte von Anfang an ein Auftrag an den Gesetzgeber, eine freiheitliche Ordnung mit Hilfe des Rechts zu schaffen. In moderner Terminologie heißt dies, dass die Freiheitsrechte nicht nur subjektive Rechte der Träger von Freiheit vermitteln sollten, sondern zugleich einen objektivrechtlichen Auftrag zur Gestaltung der Lebensverhältnisse durch Recht enthielten. Historisch war dieser objektivrechtliche Auftrag zunächst sogar wichtiger als die erst allmählich erfolgende Anerkennung subjektiver Rechte.

Die heute übliche Konzentration des Blicks auf subjektive Rechte darf nicht die zweite Dimension der Freiheitsrechte vergessen lassen, also die Aufgabe einer Zuordnung von Staat und Gesellschaft und der Ordnung der Verhältnisse innerhalb der Gesellschaft nach dem Prinzip größtmöglicher gesellschaftlicher und individueller Freiheit. Dass wir heute die objektivrechtliche Dimension der Grundrechte weitgehend aus dem Blick verloren haben und uns auf das subjektive Recht konzentrieren können, ist Beleg dafür, wie weitgehend das objektivrechtliche Programm erfüllt worden ist, der Gesetzgeber also seinen Auftrag zur Schaffung einer freiheitlichen Ordnung umgesetzt hat. Im Kontext dieser Ordnung gibt es viele subjektive Rechte. Ihre Durchsetzung, ggf. mit Hilfe der Gerichte, sichert den Erhalt dieser Ordnung. Sollten die veränderten ökonomischen, politischen, kulturellen oder sozialen Verhältnisse aber

Anlass geben, die bisherige Ordnung zu modifizieren, reichen die bisherigen Normen allein nicht. Subjektive Rechte sichern den Status quo. Der objektivrechtliche Auftrag geht über ihn hinaus.

III. Rechtsdogmatik der Informationsfreiheit

Das Wechselspiel von subjektiv- und objektivrechtlichen Grundrechtselementen ist auch bei der Deutung der Informationsfreiheit des Artikel 5 Abs. 1 Satz 1 GG bedeutsam. Das Grundgesetz kennt die Informationsfreiheit als subjektives Recht nur in einem kleinen Ausschnitt. Es begrenzt dieses Recht in Artikel 5 Abs. 1 GG auf den Zugang zu allgemein zugänglichen Quellen: diejenigen Informationsquellen, die der Allgemeinheit zugänglich sind, dürfen auch vom Staat nicht verstopft oder versperrt werden. Insofern ist die Informationsfreiheit ein Abwehrrecht gegen den Staat.

Dies aber kann nicht ausreichen, wenn Information als Lebensnerv der Gesellschaft verstanden wird, die in allen Lebensbereichen wichtig ist, so dass informationelle Energie überall fließen muss. Wenn Informationen die Grundlage der interaktiven Freiheit aller sind, zugleich für die staatliche Funktionserfüllung unentbehrlich (etwa für die Regulierung, die Aufsicht u. ä.) und ferner zur dynamischen Produktivkraft einer global vernetzten Welt geworden sind, dann wird es zu einer Lebensfrage einer rechtsstaatlichen Demokratie, wie sie mit Informationen umgeht, vor allem, wer an ihnen teil hat. Insofern kann die grundrechtliche Absicherung des Artikel 5 Abs. 1 Satz 1 GG, dass allgemein zugängliche Quellen auch allgemein zugänglich bleiben, nicht ausreichen.

Auf die Frage, welche und wie viele Informationen allgemein zugänglich sind, gibt Artikel 5 Abs. 1 Satz 1 GG nämlich keine Antwort. Das Grundrecht verbürgt nicht ein Recht auf Eröffnung der Zugänglichkeit. Insofern reagiert diese Grundrechtsnorm noch nicht hinreichend darauf, dass – jedenfalls allem Anschein nach – die Sicherung des Zugangs zu den Voraussetzungen freier Entfaltung das Grundrechtsproblem der Gegenwart und Zukunft ist. Im Informationsbereich geht es insbesondere um die Sicherung des Zugangs zu kommunikationsbezogenen Infrastrukturen, Diensten und Inhalten. Zugang zu sichern, ist eine alle Bereiche der Gesellschaft

betreffende Aufgabe. Die folgenden Ausführungen sind allerdings auf einen Ausschnitt beschränkt, nämlich auf den Zugang zu Informationen aus dem staatlichen Bereich.

Mit einer Teilfrage hierzu hatte sich das Bundesverfassungsgericht in seiner jüngsten grundlegenden Entscheidung zur Informationsfreiheit zu befassen[1]. Auf Verfassungsbeschwerde des Fernsehveranstalters n-tv hin war darüber zu entscheiden, ob Rundfunkveranstalter nicht nur einen Zugang zu Gerichtsverhandlungen als solchen haben, sondern ob sie auch mit Hilfe audiovisueller Übertragungstechniken aus Gerichtssälen berichten dürfen. Die Beschwerdeführerin berief sich darauf, dass die Rundfunkfreiheit ihr ein Recht auf Zugang zu staatlich organisierten Ereignissen eröffnet und dass hiervon auch das Recht erfasst ist, die ihr geeignet erscheinenden Aufnahme- und Übertragungsmöglichkeiten zu nutzen. Dass öffentliche Gerichtsverhandlungen allgemein zugängliche Informationsquellen sind, stand nicht zur Debatte, wohl aber die Frage, ob die Zugänglichkeit durch den Gesetzgeber unbegrenzt eröffnet sein muss. Dies ist in § 169 Satz 2 GVG nicht, nämlich nur unter Ausschluss audiovisueller Aufnahme- und Verbreitungsmöglichkeiten, geschehen. Die Beschwerdeführerin berief sich auf eine frühere Aussage des Bundesverfassungsgerichts, wonach der Schutz der Medienfreiheit von der Beschaffung der Information bis zu ihrer Verbreitung reiche[2]. Diese Argumentation der Beschwerdeführerin hat das Bundesverfassungsgericht für den vorliegenden Fall nicht akzeptiert. Das steht nicht im Widerspruch zu der früheren Rechtsprechung, weil der zitierte Satz nicht im Sinne eines Rechtsanspruches auf Beschaffung von Informationen zu verstehen ist, sondern ausschließlich in dem Kontext der Funktion von Grundrechten als Abwehrrechten gegen den Staat steht: der Staat darf die Medien nicht bei der Beschaffung von Informationen behindern. Ob er auch verpflichtet ist, ihnen Informationen bereitzustellen, ist eine andere Frage.

Das Bundesverfassungsgericht verweigerte sich auch der Argumentation der Beschwerdeführerin, ihr Informationszugangsrecht aus der Medienfreiheit abzuleiten, und das, obwohl das Gericht mehrfach festgestellt hat, dass Medien wichtige Akteure bei der Informa-

---

1 BVerfGE 103, 44 ff.

2 Vgl. BVerfGE 10, 118, 121; 91, 125,134.

tionsversorgung und der Verschaffung von kommunikativer Orientierung für die Bürgerinnen und Bürger sind: Medien, insbesondere der Rundfunk, sind nach Auffassung des Bundesverfassungsgerichts Medium und Faktor der Meinungsbildung und als solche grundrechtlich privilegiert. Würde allerdings das Recht auf Informationszugang aus der Medienfreiheit, und zwar nur aus der Medienfreiheit, abgeleitet, hieße dies, dass die Medien auch insoweit eine notwendig privilegierte Stellung einnähmen. Privilegien sind rechtlich zulässig, wenn auch rechtfertigungsbedürftig. Soll es allerdings sogar eine rechtliche Pflicht zur Schaffung von Privilegien geben, bedarf diese einer besonderen Begründung, die im vorliegenden Zusammenhang auch ergeben muss, dass ein besonderes Recht auf Informationszugang gerade aus der Medienfreiheit abzuleiten wäre.

Insofern stellt sich insbesondere die Frage, ob der Informationszugang in der Informationsgesellschaft nicht auf breiterer Basis begründet ist und sein muss. Zum besseren Verständnis der Dimension des Problems mag eine medien- und rechtspolitische Zwischenüberlegung hilfreich sein. Wer die Entwicklung der Medien beobachtet, stellt fest, dass sie bei der Aufnahme und Verarbeitung von Informationen nach spezifischen “Gesetzlichkeiten” der Publizistik und Medienwirtschaft vorgehen. Sie können ja nicht alles Mögliche bringen, sondern müssen selegieren. Dabei haben sie auch, jedenfalls die privatwirtschaftlichen Medien, den kommerziellen Imperativ des Erfolgs am Markt zu befolgen. Dementsprechend orientieren sie sich häufig nur an einem spezifischen – aus gesamtgesellschaftlicher Sicht einseitigen – Interesse. Nicht zufällig suchen die meisten Massenmedien z. B. nicht in erster Linie nach dem “Normalen”, sondern sie wollen vorrangig über das Besondere, Abartige u. ä. berichten, das am ehesten Aufmerksamkeit verspricht. Häufig greifen sie zu Mitteln wie der Skandalisierung und Personalisierung; die verknüpfen Fiktion mit Nonfiktion und verzahnen Information und Unterhaltung; sie nutzen besondere Techniken der Aufmerksamkeitsbindung und der Vorsteuerung, ja auch Manipulation von Kommunikationsinteressen. Dass Medien am ökonomischen Markt Erfolg haben wollen, darf ihnen nicht vorgeworfen werden. Es ist notwendiges Korrelat einer privatwirtschaftlichen Medienordnung. Dass die Verfassung diese Struktur ermöglicht, muss aber bei der Klärung berücksichtigt werden, wie weit die Privilegien der Medien

reichen, hier also, ob es verfassungsrechtlich angezeigt ist, dass sie eine privilegierte Stellung auch beim Zugang zu Informationen erhalten, der anderen nicht eröffnet ist. Immerhin verfügen Presse und Rundfunk schon über Privilegien bei der Aufbereitung und Verbreitung von Kommunikation in und durch Massenmedien.

Es wäre aber eine Selbsttäuschung zu glauben, dass alle für die Informationsversorgung aller Teile der Bevölkerung wichtigen Informationen auch über Medien vermittelt würden. Auch wäre es verfehlt, auf Medien und deren Wirken nur mit der Brille des Modells der Aufklärung zu sehen oder z. B. zu glauben, dass sich Wahrheiten regelhaft in einem herrschaftsfreien Diskurs ermitteln lassen. Medien beteiligen sich an dem gesellschaftlichen Prozess der Wirklichkeits- und Sinnkonstruktion nach ihren Bedingungen. Dementsprechend prägt die Kommerzialisierung der meisten Kommunikationsorganisationen den Beitrag von Medien für die öffentliche Meinungsbildung. Derartige – hier nur beispielhaft genannte – Faktoren sind regelhaft mit erheblichen Selektivitäten, etwa thematischen Einseitigkeiten, gekoppelt. Ungeachtet der großen Bedeutung der Medien für die öffentliche Meinungsbildung ist nicht gesichert, dass die Bürgerinnen und Bürger – auch etwa wirtschaftliche Unternehmen – alle für sie relevanten Informationen aus den Medien entnehmen können. Deshalb bleiben medienunabhängige Möglichkeiten der Interaktion und des Zugangs zu Informationen wichtig.

Soll das Informationsrecht Entfaltungsfreiheit für alle sichern, muss es als ein grundsätzlich an den Interessen aller orientiertes Recht verstanden werden. Die Gleichbehandlung aller bei der Ausgestaltung des Informationszugangs betont dementsprechend das Bundesverfassungsgericht: “Soweit die Medien an der Zugänglichkeit einer für jedermann geöffneten Informationsquelle teilhaben, wird der Zugang durch die Informationsfreiheit des Artikel 5 Abs. 1 Satz 1 GG geschützt, d. h. für Medien nicht grundsätzlich anders als für die Bürger allgemein .... Zum Schutzbereich (scil. der Rundfunkfreiheit des Artikel 5 Abs. 1 Satz 2 GG) gehört aber ebenso wenig wie zu dem der Informationsfreiheit ein Recht auf Eröffnung einer Informationsquelle. Insofern reicht die Rundfunkfreiheit nicht weiter als die Informationsfreiheit des Artikel 5 Abs. 1 Satz 1 GG, die als Abwehrrecht nur den Zugang zu allgemein zugänglichen Informations-

quellen gegen staatliche Beschränkung sichert. Erst nach Herstellung der allgemeinen Zugänglichkeit (scil. einer Informationsquelle) und nur in ihrem Umfang kann der grundrechtliche Schutzbereich des Artikel 5 Abs. 1 Satz 1 GG betroffen sein. Hoheitliche Beeinträchtigungen dieses Zugangs sind Grundrechtseingriffe." "Über die Zugänglichkeit und die Art der Zugangseröffnung entscheidet, wer nach der Rechtsordnung über ein entsprechendes Bestimmungsrecht verfügt. Die Ausübung dieses Rechts ist für Dritte keine Beschränkung im Sinne des Artikel 5 Abs. 2 GG. Das Bestimmungsrecht richtet sich nach dem allgemeinen Vorschriften, für Privatpersonen insbesondere nach denen des bürgerlichen Rechts, für den Staat vornehmlich nach denen des öffentlichen Rechts[3]."

IV. Das Recht als Auftrag und Mittel zur Ausgestaltung

Bei dieser abstrakten Feststellung ist das Gericht aber nicht stehen geblieben. Es ordnet das Informationszugangsrecht in einen größeren normativen Kontext. Zu dem eben in dem Zitat erwähnten öffentlichen Recht gehört nämlich auch das Grundgesetz. Dieses enthält in seiner rechtlichen Verankerung der Demokratie, des Rechtsstaates, der Sozialstaatlichkeit und auch der internationalen Offenheit einschließlich der Europäischen Integration objektivrechtliche Aufträge zur Ausgestaltung der (Informations-)Ordnung. Sämtliche dieser Prinzipien sind für ihre Funktionsweise nämlich auf Informationsprozesse angewiesen. Soweit der Zugang zur Information für die Bürgerinnen und Bürger wesentlicher Bestandteil der Funktionsfähigkeit der gesellschaftlichen Ordnung und persönlicher sowie öffentlicher Meinungsbildung ist, muss der Staat ihn ermöglichen, es sei denn, dass gewichtige Gegengründe bestehen. Das Mittel einer solchen Zugangssicherung ist die darauf gerichtete Ausgestaltung der Rechtsordnung, und zwar im Privatrecht wie im öffentlichen Recht.

So können im Privatrecht – man denke etwa an das Aktienrecht – Transparenzpflichten eingerichtet werden; das für Massenkommunikation vorgesehene Recht der Kurzberichterstattung über besonders wichtige Ereignisse (§ 5 RStV) ist ebenfalls eine Beschränkung privat-autonomer Ausschlussmöglichkeit durch Sicherung eines Zu-

[3] BVerfGE 103, 44 ff.

gangsrechts für andere (hier bestimmte Medien). Auch das öffentliche Recht kennt Vorkehrungen des Informationszugangs.

Vorreiter einer neuen Entwicklungsstufe war in Deutschland das Land Brandenburg mit seinem Informationszugangsgesetz. Dieses steht konzeptionell in dem hier geschilderten Zusammenhang. Es versteht sich als Mittel zur Sicherung der Funktionsfähigkeit von Staat und Gesellschaft, nicht etwa als Erfüllung vorgegebener subjektiver Rechte der Bürgerinnen und Bürger. Die Gesellschaft ist auf Informationen aus dem staatlichen Bereich angewiesen. Das brandenburgische Gesetz löst einen objektivrechtlichen Auftrag zur Herstellung größtmöglicher Transparenz staatlicher Vorgänge, auch im Interesse ihrer Kontrollierbarkeit, ein. Die Schaffung dieses Gesetzes war ein demokratischer und rechtsstaatlicher Fortschritt und hat dementsprechend Nachahmer in Deutschland gefunden, so in Schleswig-Holstein und in Berlin, demnächst auch im Bund.

Aber es war nur ein erster Schritt beim Fort-Schreiten in die Informationsgesellschaft. In der sich jetzt entfaltenden Entwicklungsstufe dürfte dieses Konzept für sich allein zu kurz greifen, so deshalb, weil es letztlich auf dem Modell des Gegenüber von Staat und Gesellschaft aufbaut, das den Staat als vorrangigen Gefährder von Freiheit versteht. Es wendet – der Tradition der Rechtsordnung entsprechend – seinen Blick dabei auf rechtlich voneinander abgegrenzte Bereiche. Dies blendet angesichts der schon erwähnten Entgrenzungen – auch und insbesondere im Verhältnis von Staat und Gesellschaft – Wesentliches aus. Die beschränkte Sichtweise kann insbesondere den vielen Vernetzungen des Öffentlichen und des Privaten in der Informationsgesellschaft nicht gerecht werden. Diese finden weltweit und damit auch außerhalb der Einwirkungsmöglichkeit des Nationalstaates statt und bewirken, dass ein Großteil wichtiger Informationen gar nicht dem Bereich des Staates zuzuordnen ist. Ein auf den Staat begrenztes Konzept der Zugangssicherung greift insbesondere zu kurz, weil der Staat als Machtträger neben den anderen, also gesellschaftlichen Machtträgern, steht, die für die Informationsversorgung immer wichtiger werden. Die verschiedenen Machtträger betätigen sich in real beobachtbaren, aber auch in virtuellen Entscheidungszusammenhängen. Der Blick auf die internationalen Finanzmärkte zeigt beispielhaft, dass hier eine eigene Welt, insbesondere eine Informationswelt virtueller Vernet-

zungen, entstanden ist, deren Wirkungen weit gehend sind, auf deren Abläufe der Staat aber kaum noch Einfluss hat. Dennoch werden von ihnen auch staatliche Handlungsmöglichkeiten massiv beeinflusst. Der durch private Akteure ausgelöste Zusammenbruch der Aktienmärkte nach dem Terroranschlag vom September deutet beispielhaft auf Funktionszusammenhänge, in denen der Staat fast keine Rolle mehr spielt, von deren Folgen aber auch seine Möglichkeiten der Aufgabenwahrnehmung – etwa bei der Bekämpfung der Arbeitslosigkeit –abhängen.

Die Verfügungsmacht über Informationen vermittelt generell vielfältige Möglichkeiten des Machteinsatzes und dabei auch der direkten und indirekten, insbesondere subtilen, ja subliminalen, Manipulation. Deshalb ist das Denken in Rechten des Informationszugangs (nur) zum Staat viel zu eng. Das Grundgesetz ist allerdings hinreichend weit konzipiert, um auch andere Relevanzen im Recht einkalkulieren zu können.

So sind die Kommunikationsfreiheiten in der Ordnung des Grundgesetzes in ein System von verschiedenen verfassungsrechtlichen Zielwerten und Verbürgerungen eingeordnet, die der Staat in ihrer Funktionsweise gewährleisten muss. Die erwähnten Staatsziel-Bestimmungen Rechtsstaat, Demokratie und Sozialstaat, aber auch europäische Integration, wirken auf die Ordnung der Gesellschaft zurück. Soweit die Funktionsfähigkeit einer Demokratie auf die Leistungsfähigkeit von Informationsprozessen und die eines Rechtsstaates auf die rechtlich angemessene Ordnung von Lebensverhältnissen angewiesen ist, fordert auch der programmatische Gehalt des Grundgesetzes entsprechende Vorgaben zu Sicherung der Idee der Freiheit als einer real wirksamen Freiheit unter den Bedingungen der Gegenwart. Das beschränkt sich nicht auf Vorgaben rechtlicher Ansprüche und es erfasst alle Lebensbereiche, die auf Interaktion angewiesen sind, sei es in der Berufswelt, der Freizeit oder der Privatsphäre. Die normativen Vorgaben der Verfassung enthalten programmatische Aufträge an den Staat, durch seine Rechtsordnung auf die verschiedenen Lebensbereiche Einfluss zu nehmen, um das für die Funktionsfähigkeit nötige Mindestmaß an Informationszugang zu sichern. Ist der Zugang zu Informationen eröffnet, dann sichert Artikel 5 Abs. 1 Satz 1 GG dessen Erhalt in der rechtlichen Konstruktion subjektiver Abwehrrechte.

Schwierigkeiten entstehen aber, wenn der Staat seinem objektivrechtlichen Auftrag nicht gerecht wird. Dies behauptete die Beschwerdeführerin in dem n-tv-Verfahren. Das Bundesverfassungsgericht ist ihr nicht gefolgt. Es hat allerdings festgestellt, dass der Gesetzgeber grundsätzlich berechtigt ist, die Zugänglichkeit zu Gerichtsverhandlungen in größerem Rahmen herzustellen als § 169 Satz 2 GVG vorsieht. Das Gericht hat dabei auf das Rechtsstaatsprinzip und den in ihm enthaltenen Grundsatz der Öffentlichkeit mündlicher Verhandlungen verwiesen und zusätzlich auf das allgemeine Öffentlichkeitsprinzip der Demokratie abgestellt. Dabei hat es aber auch ausgeführt, dass die Funktionsfähigkeit der Rechtspflege ein wichtiges Gut ist. Verfahrensgerechtigkeit kann – wie es ebenfalls den Ideen der Aufklärung entspricht – auch durch Öffentlichkeit abgesichert werden; sie kann aber auch dadurch gefährdet werden, etwa wegen möglicher Rückwirkungen der Öffentlichkeit auf den Inhalt von Zeugenaussagen oder wegen unzuträglicher Beeinträchtigung der Persönlichkeitsrechte von Prozessbeteiligten. Wenn das Bundesverfassungsgericht den Gesetzgeber grundsätzlich als berechtigt ansieht, die Gerichtsöffentlichkeit in weiterem Umfang als bisher herzustellen, soweit er gegenläufige Rechtsgüter angemessen berücksichtigt, steht es in der Reihe der neueren Rechtsprechung anderer Gerichte in ausländischen Staaten. Auch der amerikanische Supreme Court ist nicht weitergegangen, hat also nicht etwa eine Rechtspflicht zur Öffnung von Gerichtsverhandlungen für Fernsehaufnahmen formuliert.

In dem erwähnten Urteil des Bundesverfassungsgerichts ist die Minderheit allerdings über diese Sichtweise hinausgegangen. Sie leitet aus objektivrechtlichen Vorgaben der Verfassung eine Verpflichtung des Gesetzgebers her, eine über die bloße Saalöffentlichkeit hinausgehende Medienöffentlichkeit herzustellen, soweit keine gegenläufigen rechtlich geschützten Interessen entgegenstehen. Dies hat die Minderheit zwar nicht näher ausdifferenziert, aber beispielsweise für den Verwaltungsprozess grundsätzlich eine Pflicht bejaht und eine Öffnung für einzelne Verfahrensschritte angemahnt.

Insofern geht die Minderheit von einer grundsätzlichen Handlungspflicht des Gesetzgebers aus und konkretisiert diese insbesondere

auch als Pflicht zur Auswertung und Gewinnung von Erfahrungen als Grundlage der zukünftigen Umsetzung der programmatischen Handlungsaufträge. Allerdings gibt es regelhaft bei der Verletzung objektiven Rechts keine subjektiven öffentlichen Rechte der Bürger, sich dagegen wehren zu können. An dieser Stelle wird Leitsatz 2 des Urteils wichtig, den Mehrheit und Minderheit tragen: “Das Grundrecht des Artikel 5 Abs. 1 Satz 1 GG umfasst ein gegen den Staat gerichtetes Recht auf Zugang, wenn eine im staatlichen Verantwortungsbereich liegende Informationsquelle auf Grund rechtlicher Vorgaben zur öffentlichen Zugänglichkeit bestimmt ist, der Staat den Zugang aber verweigert.” Entscheidend wird also, ob die Rechtsordnung den Staat zur Zugangseröffnung verpflichtet. Solche Pflichten des Staates können grundsätzlich aus den schon erwähnten Staatsziel-Bestimmungen abgeleitet werden, also etwa der auf größtmögliche Transparenz und Kontrollierbarkeit gerichteten Demokratie, aber auch aus spezifischen europarechtlichen Vorgaben. Im Europarecht gibt es – wenn auch nur mit begrenzter Wirkung – zunehmend Transparenz sichernde Vorkehrungen. Ich nenne nur die Artikel 255 EG-Vertrag und Artikel 1 Abs. 2 des EU-Vertrages. Auch hat die Europäische Gemeinschaft ergänzende Transparenz sichernde Vorkehrungen geschaffen, beispielhaft mit Hilfe der Richtlinie über Umweltinformationen. Transparenz fördernd wirkt sich auch Artikel 8 der Europäischen Menschenrechtskonvention aus, gewissermaßen im Sinne eines Menschenrechts auf Umweltinformation. Selbst soweit derartige europarechtlichen Vorgaben innerstaatlich nicht verbindlich sein sollten, können sie auch auf die deutsche Rechtskultur einwirken und möglicherweise Interpretationshilfen bei der Konkretisierung von Verfassungsprinzipien sein.

Soweit den auf den Staat bezogenen Normen eine Pflicht zur Öffnung einer Informationsquelle zu entnehmen ist, können die Bürger dies im Rahmen ihrer Informationsfreiheit aus Artikel 5 Abs. 1 Satz 1 GG subjektivrechtlich durchsetzen. Allerdings hat die in Leitsatz 2 der erwähnten Entscheidung des Bundesverfassungsgerichts formulierte Einsicht in der Literatur auch Kritik gefunden. Diese lautet, dass der Umschlag von objektivem Recht zu subjektiven Rechten grundrechtsdogmatisch nicht begründet und auch nicht begründbar sei. Stattdessen verweist die Literatur auf die schon oben als defizitär kritisierte Möglichkeit, über Artikel 5 Abs. 1 Satz 2 GG, also die Rundfunkfreiheit, ein subjektives Zugangsrecht zu eröffnen.

Das Bundesverfassungsgericht versteht es nicht als seine Aufgabe, zu grundrechtsdogmatischen Fragen Stellung zu nehmen oder bestimmte rechtsdogmatische Konstruktionen zu entwickeln. Dies überlässt es der literarischen Auseinandersetzung. Insofern ist es wünschenswert, dass es in der Zukunft weitere wissenschaftliche Arbeiten zu dem skizzierten Problem gibt. Ich nenne aber schon jetzt eine von einem jüngeren Wissenschaftler, Tobias Gostomzyk, in einer juristischen Fachzeitschrift vorgeschlagene Konstruktion: Wenn die Öffnung des Zugangs zu einer Informationsquelle entgegen rechtlichen Vorgaben unterbleibt, sei – so führt er aus – dies funktional der Verhinderung des schon eröffneten Zugangs vergleichbar. Das aber wäre ein Eingriff in die Informationsfreiheit. Die Blickweise auf funktionale Äquivalente von Eingriffen ist der Rechtsordnung in der Tat nicht völlig fremd. So ist beispielsweise die im Laufe der Zeit erfolgte Einordnung faktischer und mittelbarer Grundrechtseingriffe in den Schutzbereich von Grundrechten am ehesten dadurch erklärbar, dass solche Beeinträchtigungen als funktionale Äquivalente traditioneller Grundrechtseingriffe verstanden wurden und nicht nachvollziehbar war, warum sie trotz gleicher Wirkungen rechtlich anders als jene behandelt werden sollten.

Jedenfalls wird es zu den grundrechtsdogmatischen Aufgaben der näheren Zukunft gehören, das Zusammenspiel zwischen objektivrechtlichen und subjektivrechtlichen Verbürgungen weiter aufzuklären und dabei auch das für die Gegenwart und Zukunft besonders wichtige Grundrechtsproblem zu lösen, nämlich die Sicherung von Zugang – dies unter den je aktuellen Bedingungen der Informationsgesellschaft.

Dafür scheint die vom Bundesverfassungsgericht angebotene Lösung umgreifender zu sein als es solche in der Literatur formulierten Vorschläge sind, die das Informationszugangsrecht als Ausfluss (nur) auffindbarer subjektiver Rechte wie insbesondere der Medienfreiheit verstehen. Der umfassendere Ansatz des Bundesverfassungsgericht ist auf die Bedingungen der Informationsgesellschaft ausgerichtet, in der nicht nur die Medien ein existenzielles Interesse an Informationen aus dem Bereich des Staates haben. Der Ansatz sieht keine Verengung auf ohnehin Privilegierte vor und wird auch nicht aus dem – insoweit ebenfalls zu engem – Recht auf informati-

onelle Selbstbestimmung entwickelt. Das Bundesverfassungsgericht nimmt vielmehr den objektivrechtlichen Auftrag des Staates zur Sicherung der Funktionsfähigkeit von informationsgestützten Sozialbereichen als Ausgangspunkt seiner Überlegungen und konzentriert den Blick auf das Zugangsproblem als ein Freiheitsproblem. Zugleich weist das Gericht einen Weg zu Rechtsbehelfen, die es erlauben, sich gegen eine staatliche Nichterfüllung von Zugangsöffnungspflichten zu wehren. Auch wenn dieses Konzept den Ausgangspunkt nicht bei den subjektiven Rechten wählt, ermöglicht es bei der Sicherung des Informationszugangs vermutlich mehr Freiheit für alle als eine auf schon anerkannte subjektive Rechte, insbesondere die Medienfreiheit, beschränkte Position.

V. Sicherung der Funktionsfähigkeit informationsgestützter Sozialbereiche

Das Ausgehen vom objektivrechtlichen Ausgestaltungsauftrag zur Sicherung der Funktionsfähigkeit informationsgestützter Sozialbereiche erlaubt es im Übrigen, nicht nur auf das Verhältnis zum Staat zu sehen. Die Gestaltung des Rechts der Informationsgesellschaft nach dem Grundsatz der Freiheit für alle erfordert es, mehrdimensionale Problemverschachtelungen wahrzunehmen, multifunktionale Aufgabenfelder zu regeln, multipolaren Interessenkonstellationen gerecht zu werden, die Dynamiken der Entwicklung der Informationsgesellschaft zu respektieren und darauf aufbauend Lernfähigkeit für Staat und Gesellschaft zu organisieren. Eine derartig komplexe Aufgabe lässt sich nicht lösen, wenn ausschließlich in bipolaren Rechtsverhältnissen gedacht wird. Erforderlich ist vielmehr eine neue Kultur der Regulierung komplexer Sozialbereiche. Die Regelungsaufgabe ist immens und der Erfolg ihrer Erfüllung keineswegs absehbar.

Dabei muss die dem früheren Grundrechtsdenken eigene Sichtweise korrigiert werden, nach der der Staat ein Gegner von Freiheit ist. Das kann er sein. Der Staat ist heute aber auch Schützer von Freiheit, gewissermaßen ihr Garant.

Der Staat als Garant von Freiheit

Diese Garanten-Stellung ist nicht nur eine Antwort auf die immer komplexer gewordene Lebensverhältnisse, die der Einzelne allein gar nicht durchschauen kann. Sie stützt sich auch auf die Einsicht, dass es neben dem Staat andere Machtträger gibt, von denen Risiken für den Freiheitsgebrauch ausgehen. Gerade in den aktuellen Zeiten der Privatisierung und Deregulierung stellt sich das Problem der Freiheitssicherung neu. Gibt der Staat eine Aufgabe ab und handeln stattdessen Private, so fällt der Staat als Verpflichteter der Bindung an Grundrechte fort. Private sind nicht, jedenfalls nicht in der gleichen Weise wie der Staat, an Grundrechte gebunden. Ihre Grundrechtsbindung kann nur hergestellt werden, wenn in der für sie geltenden (Privat-) Rechtsordnung Vorsorge getroffen wird, dass sie die Möglichkeiten freier Entfaltung anderer nicht übermäßig beengen. Anders formuliert: Soll der Grundrechtsschutz infolge der Verlagerung von Aufgaben auf Private in seinem bisherigen Niveau erhalten bleiben oder gar ausgebaut werden, bedarf es neuer rechtlicher Strukturen der Grundrechtsverwirklichung. Dies gilt auch für das Recht auf chancengleichen Zugang zu Informationen und damit auf chancengleiche Mitwirkung an Informationsprozessen. Aber auch das Recht auf Schutz vor Informationsmissbrauch, etwa Datenmissbrauch, bedarf entsprechender Absicherung gegenüber Privaten. Die in den neueren Datenschutzgesetzen enthaltene Erstreckung des Datenschutzrechts auch auf die private Datenverarbeitung greift das Problem auf, obwohl die Normen – wie auch Datenschützer immer wieder kritisieren – dieses Problem noch nicht angemessen lösen.

Wird das Datenschutzrecht traditioneller Art durch ein Recht zur Sicherung der Funktionsfähigkeit von informationsgestützten Sozialbereichen abgelöst und werden in diesem Kontext auch persönlichkeitsschützende Vorkehrungen der Datenverarbeitung geregelt, dann geht das Datenschutzrecht in einer umfassenderen Ausgestaltung der positiven Ordnung der Informationsbeziehungen auf. Informationsrecht als Management von Interdependenzen ist dabei notwendig auch Datenschutzrecht. Datenschutz bedeutet aus dieser Perspektive nicht nur, jedenfalls nicht in erster Linie, das Setzen von Schranken gegenüber der Ausübung von Kompetenzen des Staates oder von Freiheiten anderer Bürger, sondern wird zum un-

abdingbaren Teil der Sicherung der Funktionsfähigkeit der Informationsordnung: Datenschutz wird zu einem konstitutiven Element des Rechts der Informationsgesellschaft. Zu diesem Recht gehört auch die Sicherung des Zugangs zu Daten, die für das eigene Informationsverhalten wichtig sind, also eine Zugangsvorsorge.

Es reicht jedoch nicht, Zugang in einem rechtlichen Sinne abzusichern, wenn nicht auch die Interaktionsfähigkeit geschützt wird oder besser, faire Interaktionschancen für jedermann bestehen. Kommunikationsberatung, Informationsaufbereitung und Informationshilfe können in einer solchen Informationsordnung ihren Platz finden. Selbstverständlich gehören dazu auch Vorkehrungen zur Abwehr von Gefahren für persönliche Entfaltungsrechte, also etwa von Manipulation. Derartige Gefahren können – um das Beispiel des Internet aufzugreifen – mit privat gestalteten Navigatoren und Hyperlinks verbunden sein. Das Recht dieser neuen Informationsordnung kann und sollte auch Schutz vor Informationsausbeutung gewähren, etwa vor den gegenwärtig mit Hilfe der sog. Cookies in die Software eingebauten Möglichkeiten zur (unerkannten) Erfassung von Nutzerdaten und darauf aufbauend der Erstellung und Vermarktung von Nutzerprofilen. In den Kontext eines solchen Rechts gehört selbstverständlich auch die Anerkennung subjektiver Rechte, etwa neben dem Grundrecht auf informationelle Selbstbestimmung auch ein Grundrecht auf multimediale Selbstbestimmung und –entfaltung, und zwar als Teil einer rechtlich geprägten Informationsordnung.

Zu einem solchen Rechtsbereich gehört aber auch der Schutz vor der Informationsfilterung durch Private. Die Filterung des Zugangs von Informationen für die Öffentlichkeit ist begrifflich als Zensur bekannt. Der historische Kampf um die Informationsfreiheit war in erster Linie ein Kampf gegen die Zensur von Staat und Kirche. Heute gibt es andere mächtige Filterinstanzen als Staat und Kirche, also gate keeper der Information etwa in Form der Provider im Internet. Angesichts der Schwierigkeiten des Staates, die Geltung des Rechts im Internet durchzusetzen, vertraut der Staat zunehmend auf private Akteure wie die Provider. So erwartet der Staat in den von ihm geschaffenen Haftungsregeln (vgl. §§ 5 MDStV, TDG), dass Provider unter bestimmten Voraussetzungen gewisse Inhalte – etwa pornographische oder sonstwie strafbare – aus dem Internet herausfiltern. Das Haftungsrecht ermuntert gewissermaßen zum

Aufbau privater “Zensur”macht. Diese unterliegt aber nicht den gleichen rechtsstaatlichen Vorkehrungen vor Missbrauch, etwa für Transparenz, wie die Kontrollmacht des Staates. Insofern ist die Vorsorge wichtig, dass hier nicht neue Machtprobleme entstehen, Manipulation geübt wird oder sich gar eine Art Geistespolizei entwickelt und danach eine Zeit kommt, in der das Bemühen aussichtslos erscheint, den privaten Filter-Zauberlehrling auch wieder los zu werden.

Zur Ausgestaltung einer Informationsordnung neuen Zuschnitts gehört auch die Vorsorge dafür, dass die durch einen erweiterten Informationszugang mögliche professionell-kommerzielle Aufbereitung von so erlangten Informationen und ihre Verwertung – und damit die Vermarktung des Mehr-Werts der Informationsaufbereitung – auf eine Weise geschieht, die Informationschancengleichheit bewahren hilft.

Der Staat als Gefährder der Freiheit

Kam bisher der das Recht der Informationsgesellschaft ausgestaltende Staat als schützender Staat in den Blick, so soll dies nicht heißen, dass der Staat nicht weiterhin auch potentieller Gefährder von Freiheit ist. Auch das lässt sich an aktuellen Ereignissen der Gegenwart illustrieren. So zeigt die durch den Anschlag am 11. September 2001 ausgelöste Reaktion auf Terrorismus, dass vom Staat einerseits Schutz erwartet wird, dass aber andererseits Anlass für die Sorge besteht, von ihm könnten neue Gefahren ausgehen. Eine Lage, wie die durch die Terrorismusbedrohung ausgelöste, führt zu der Versuchung für den Staat, jetzt das zu tun, was er schon immer tun wollte, aber bisher aus rechtsstaatlichen Gründen nicht tun durfte. So gibt es immer neue gesetzliche Ideen und Instrumente für einen erweiterten Informationszugriff auf die Bürger, die noch vor Kurzem in der Öffentlichkeit einen Sturm der Entrüstung ausgelöst hätten – gegenwärtig aber nicht auslösen.

Der Rechtsstaat gilt auch in Krisenzeiten, ja er bewährt sich erst wirklich in der Krise. Natürlich muss der Rechtsstaat Antworten auf neue Gefährdungen ermöglichen, also auch auf die Gefahren des Terrorismus. Er muss aber auch dann seinen Prämissen der Frei-

heitssicherung treu bleiben. Sie stehen nicht zur Disposition. Meint der Staat Anlass zu haben, seinen Bürgern oder bestimmten Teilen der Bürgerschaft zu misstrauen, dann besteht das Risiko, dass die Bürger auch Anlass nehmen, dem Staat zu misstrauen.

Das Risiko einer Spirale wechselseitigen Misstrauens ist in Zeiten der Bedrohung besonders groß. Fatal ist es, wenn darüber nicht auch in Zeiten gesprochen werden kann, in denen weltweit Solidarität im Kampf gegen den Terrorismus erwartet wird. Solidarität ist eine wichtige Waffe im Kampf gegen Bedrohungen. Solidarität muss aber konstruktiv bleiben: Sie darf nicht blind machen und erst recht nicht bedingungs- und damit auch kritiklos sein. Erwartet wird zurzeit Solidarität nicht nur in politischer und militärischer Hinsicht, sondern auch in symbolischer, bis hin zur sprachlichen Disziplinierung des Redens über die Art der terroristischen Bedrohung und über die Antwort auf diese Bedrohung. Beobachtbar ist gegenwärtig ein Wächtertum über political correctness, das ein Klima der sprachlichen Vorsicht geschaffen hat. Dies macht es fast unmöglich, auch über das Risiko zu sprechen, dem Menschenleben verachtenden Terrorismus dadurch in die Falle zu gehen, dass wir gebannt durch die Angst vor terroristischer Bedrohung gar nicht mehr fragen, ob wir die freiheitliche Ordnung des Miteinander durch unsere Reaktion vielleicht noch stärker bedrohen.

Natürlich erwarten die Menschen Antworten auf Bedrohungen und sie wollen zu Recht, dass der Staat sein allgemeines Schutzversprechen auch konkret einlöst. Wir sollten von einem verantwortungsbewussten Staat aber auch erwarten, dass er erstens nicht mehr verspricht als einlösbar ist und dass er zweitens prüft, welche weiteren Folgen mit möglichen Maßnahmen verbunden sind. Zum Ersten gehört auch das Eingeständnis, dass real viel weniger Schutz eingelöst werden kann als gegenwärtig versprochen wird. Zum Zweiten gehört die Bereitschaft zur gründlichen Analyse von Möglichkeiten und Folgen, vor allem auch von Folgesfolgen neuer Instrumente. Der Erlass von Gesetzen reicht für sich allein zur Gefahrenabwehr niemals. Das gilt ganz besonders für Gesetze, die (nur) auf Informationen – also Datenerhebung – zielen. Es muss ebenfalls vorgesorgt sein, dass die erhobenen Daten auch “bewältigt”, also sinnvoll ausgewertet und in rechtsstaatlicher Weise für die Gefahrenabwehr verwendet werden können. In einem Rechtsstaat

muss ferner vorgesorgt sein, dass die Erhebung von Daten auf das Erforderliche begrenzt bleibt und angemessen auch insoweit ist, als die Informationen unbeteiligte Dritte betreffen. Maßnahmen der Gefahrenvorsorge und -abwehr müssen ferner zielgerecht und vollziehbar sein. Wenn gesagt wird, die vorhandenen – in reichhaltiger Weise zur Informationserhebung ermächtigenden – Gesetze reichen nicht, muss auch gefragt werden: warum denn nicht? Denn ihr Erlass war meist mit dem Versprechen erfolgreicher Gefahrenvorsorge und -abwehr verbunden. Die Gefahr terroristischer Anschläge ist als solche ja nicht neu, auch wenn seine gegenwärtigen Erscheinungsformen und die globale Intensität zum Teil neu sind. Wo aber ist eine nachvollziehbare Auswertung des Erfolgs oder Misserfolgs bisheriger Informationserhebungsinstrumente? Warum ist sie nicht öffentlich diskutierbar?

Sollte es aber unabweisbar sein, vermehrt auf die Daten der Bürger zuzugreifen, wird umso wichtiger, dass die Datenverarbeitung kontrollierbar bleibt. Selbstverständlich müssen Daten geheim sein, sofern der Erfolg einer Maßnahme auf der Geheimhaltung beruht, und selbstverständlich muss der Staat Strategien der Gefahrenbekämpfung wählen dürfen, die den Verursachern der Gefahren verborgen bleiben. Das aber schließt öffentliche Kontrolle der Art der Datenverarbeitung durch den Staat ebenso wenig aus wie eine informierte öffentliche Diskussion darüber, welche Risiken in der freien Kommunikation miteinander die Gesellschaft tragen will, um Risiken anderer Art abzuwehren. Ohne informierte Auseinandersetzung über den zukünftigen Weg könnten wir die Chance verspielen, Misstrauen durch Vertrauen abzulösen.

Letztlich kann ein Rechtsstaat nur funktionieren, wenn seine Rechtsordnung Ansporn ist, vom Grundsatz des Vertrauens auszugehen, und zwar mit dem Blick auf die Bürger einerseits und auf den Staat andererseits. Vertrauen gibt es nicht ohne Risiken, aber auch Misstrauen birgt Risiken. Eine Gesellschaft ohne Risiken gibt es in der Moderne nicht. Dies schließt aber den Willen nicht aus, Risiken abzuwägen und dann zu entscheiden, welche Risiken wir zu tragen bereit sind. Auf dieser Maxime sollte auch die Zukunft der Informationsgesellschaft gegründet werden. Sonst könnten wir wahrlich nicht sagen, wir seien “sans souci”.

Prof. Dr. Bogusław Banaszak
Professor für Verfassungsrecht an der Universität Wrocław

Magister Krzysztof Wygoda
Fakultät für Rechtswissenschaften der Universität Wrocław

Die Presse und der Datenschutz

„Die Presse übt laut der Verfassung der Republik Polen die Aussagefreiheit aus und verwirklicht das Recht der Bürger auf redliche Information, Öffentlichkeit des gesellschaftlichen Lebens und gesellschaftliche Kontrolle und Kritik."[1] Diese wichtige Erklärung mit einer allgemeinen Bedeutung eröffnet die grundsätzliche Rechtsakte, die die Tätigkeit von Journalisten und Massenmedien regelt. Sie wird aber in einem aus einer „anderen Epoche" der polnischen Staatlichkeit stammenden Gesetzt vom 26. Januar 1984 enthalten und in ihrer ersten Fassung ließ sie sich nicht an die nach 1989 entstandenen Bedingungen anpassen.[2] Die Transformation der Staatsform und der Rückkehr zu den Grundsätzen eines demokratischen Staa-

[1] Art. 1 des Pressegesetzes in der Fassung die durch Art. 1 des Gesetztes vom 11. April 1990 über Aufhebung des Gesetztes über Kontrolle von Veröffentlichungen und Veranstaltungen, Abschaffung der Organe dieser Kontrolle und Änderung des Gesetztes – Presserecht (Gbl. 90.29.173) gegeben wurde

[2] Zur Bestätigung dieser These kann man hier Art. 1 des Pressegesetzes in seiner Erstfassung nennen: „Die Presse übt gemäß der Verfassung der Volksrepublik Polen die Aussage- und Druckfreiheit aus, realisiert das Recht der Bürger auf Information und auf den Einfluss auf den Lauf der öffentlichen Angelegenheiten, verstärkt die Verfassung der Volksrepublik Polen und insbesondere: 1) veröffentlicht Informationen und äußert Meinungen, die der Entwicklung der sozialistischen gesellschaftlichen Verhältnissen, der Nationalwirtschaft, der Wissenschaft und Kultur und der internationalen Zusammenarbeit im Friedenssinn dienen, 2) verwirklicht den Grundsatz der Öffentlichkeit des öffentlichen Lebens und der gesellschaftlichen Kontrolle und offenbart und kritisiert die negativen Ereignisse des gesellschaftlichen und wirtschaftlichen Lebens, darüber hinaus führt Organisations- und Interventionstätigkeit, 3) ermöglicht den Bürgern die Teilnahme an gesellschaftlichen Konsultationen und Diskussionen und dadurch auch derer Teilnahme an Entscheidungen über die wichtigsten Probleme des Staates und andere gesellschaftliche Angelegenheiten." Dazu kamen auch viele andere Elemente, wie das Bestehen und die Tätigkeit der Zensur, die Nichtbeschäftigung der „unbequemen" Journalisten oder Einschränkung des Zugangs zum Papier, zu den polygraphischen Geräten oder Radiofrequenzen (es gab natürlich viel mehr Einschränkungen, wir werden uns aber mit diesen hier nicht beschäftigen)

tes verursachte zugleich die Reform des fast ganzen Rechtssystems. Dessen Änderung erforderte viel Zeit und ist noch bis heute nicht beendet worden. Zweifelsohne leben wir aber unter anderen Bedingungen – die Pressefreiheit ist für uns offensichtlich – was sowohl in der Praxis bestätigt wurde als auch als ein fundamentaler Grundsatz der Verfassung der Republik Polen in Art. 14 des Grundgesetzes vom 1997 gefasst wurde.

Das polnische Grundgesetz widerspiegelt die Werte, die typisch für eine freie, in ihrer Anschauungen und Handlungen vielfältige Gesellschaft, die in einem demokratischen Rechtsstaat lebt, sind. Mit dem Grundsatz des demokratischen Rechtsstaates, der „auch materielle Inhalte, insbesondere die, die mit Rechten und Freiheiten des Menschen verbunden sind ...“[3] beinhaltet, ist auch die Pressefreiheit oder noch ausführlicher betrachtet - die für die Kontrolle der Behörden unentbehrliche Aussagefreiheit – stark verbunden. Aber nicht nur diese, weil der Meinung des Verfassungsgeber nach, ist die Quelle aller Rechte und Freiheiten des Menschen die unveräußerliche, jedermann zustehende Menschenwürde.[4] Öffentliche Behörden sind verpflichtet, diese Würde zu wahren und zu schützen und die Erfüllung dieser Pflicht erfordert, dass viele Handlungen vorgenommen werden müssen und dabei ist die Sicherung einer bestimmten, wenn auch nur minimalen Privatsphäre des Menschen eine der notwendigen Voraussetzungen.

Das Recht auf die Privatsphäre begann erst vor kurzem eine wesentliche Rolle in den verfassungsrechtlichen Regelungen und Rechtsprechung, nicht nur in den Staaten des früheren „Ostblocks“ , der sog. „Völkerdemokratie“ sondern auch allgemein zu spielen, seit längerer Zeit beeinflusste aber die Position des Menschen in den gegenwärtigen demokratischen Staaten. Seine Bestandteile sind

---

[3] Vergleiche das Urteil des Verfassungsgerichts TK U 5 / 97 OTK 1998/4/46

[4] Der Begriff der Menschenwürde, der in die Verfassung vom 1997 eingeführt wurde, wurde bis jetzt weder in der Rechtslehre noch in der polnischen Rechtsprechung genau bestimmt. Bis jetzt (außer eines Falls) berief sich sogar das Verfassungsgericht nicht darauf als auf die einzige Grundlage seiner Entscheidungen, dadurch ist auch unmöglich, eine juridische Definition der Würde anzugeben. Beim Gebrauch dieses Begriffs muss man sich also ausschließlich auf die intuitive Bedeutung stützten, so hat aber dieser Wert einen sehr subjektiven Charakter. Mehr zu diesem Thema in Godność człowieka jako kategoria prawna (red. i wprowadzenie) K. Complak, *Menschenwürde als Rechtsategorie (Hrsg. und Einleitung) ,* Wrocław 2001,

Grundsätze und Regel, die verschiedene Sphären des menschlichen Lebens betreffen. Das Gemeinsame ist die Gewährung dem Menschen des Rechtes „... auf das eigene Leben, gemäß seinem eigenen Willen, bei Einschränkung aller Eingriffe von Außen auf das notwendige Minimum“.[5] So begriffene Privatsphäre bezieht sich im allgemeinen auf das Privat-, Familien- und Gesellschaftsleben, die Unverletzlichkeit der Wohnung, das Korrespondenzgeheimnis und den Schutz von personenbezogenen Daten – lakonisch könnte man dieses Recht als „das Recht auf In-Ruhe-Lassen“ oder „das Recht des Menschen auf sich selbst gelassen zu sein“ bezeichnen. [6]

Manche von den oben genannten Bestandteilen der Definition der Privatsphäre werden als selbständiges Gut geschützt. Dadurch wird aber die Tatsache, dass dessen Schutz eine Garantie der Unverletzlichkeit des Privatlebens bildet und gleichzeitig die Wahrung der Menschenwürde und der Existenz des Menschen sichert, nicht beeinflusst. Man könnte sogar feststellen, dass für die Wahrung der Würde der Schutz von der Privatsphäre des Menschen, der sich in der Nichteingriff (durch den Staat und durch andere Rechtsträger) in eine bestimmte (in Polen auch in der Verfassung) Lebenssphäre des Menschen und derer Sicherung vor unberechtigten Handlungen, deren Zweck die Verletzung dieser Sphäre ist, unentbehrlich ist, ausgedruckt wird. Damit ist auch die Sicherung des Rechtes des Menschen auf den Zugang zu den Daten, die die Identität betreffen (samt der Berechtigung auf deren Berichtigung oder Beseitigung), wenn solche sich in Besitz von anderen Rechtsträgern befänden,[7]

---

[5] Mehr zu diesem Thema siehe z.B. A. Kopff, Koncepcje prawa do intymności i do prywatności życia. zagadnienia konstrukcyjne, *Die Konzeption des Rechtes auf Intimität und Privatsphäre des Lebens Konstruktionsbegriffe*, Studia Cywilistyczne, B. XX/1972; W. Sokolewicz, Prawo do prywatności [w:] Prawa człowieka w Stanach Zjednoczonych*, Das Recht auf die Privatsphäre [in:] Menschenrechte in den Vereinigten Staaten,* Warszawa 1985 .

[6] Die am häufigsten berufene Bezeichnung des Rechtes auf Privatsphäre – „a right to be let alone” – erschien in der ersten Auflage von Law of Trots T. Cooley (1880, 2. Auflage1888), ist auch in dem Artikel The Right to Privacy von S. Warren und L. Brandeis, veröffentlicht in Harvard Law Review 4/1890, S. 193 zu finden. Dieser durch die Amerikaner populär gemachte Begriff *right to privacy* ist stark mit dem gegenwärtigen Sinn des Rechts auf Privatsphäre verbunden.

[7] Der Sicherung der Privatsphäre würde am besten die Garantie des Rechtes auf „Informationsselbstbestimmung des Menschen“ dienen, ihm steht also das Recht auf ausschließliche Bestimmung wer, wovon und auf welche Weise von ihm erfahren darf, *nota bene* ist diese Forderung stark mit der Definition der Privatsphäre, die von A. Westin (zitiert nach L. Kanski: op. cit. , S. 328) gefaßt wurde und in der

weil wir in diesem Fall nicht mehr mit der Privatsphäre zu tun haben.

Wie kann man aber das Recht auf Privatsphäre mit der Pressefreiheit, der Freiheit der Aussage oder dem Recht auf Information – die auch verfassungsrechtlich garantiert werden, in Einklang bringen. Ist das überhaupt möglich?

Es wäre einfach, wenn wir annehmen könnten, dass eine von diesen Freiheiten in jedem Fall zwingend übergeordnet ist – so ist es aber nicht. In allen bestimmten Fällen muss entschieden werden (manchmal entscheiden die Gerichte), welcher von den strittigen, wie es auch scheinen mag, Werten den Vorrang hat. Es kann sehr kompliziert werden und die Beschreibung dieser Erscheinung in derer allen Aspekten scheint unmöglich zu sein. Zum Glück ist das Ziel dieses Vortrages nur die Darstellung der gegenseitigen Verhältnisse zwischen „einem Fragment" der Privatsphäre und zwar dem Schutz der personenbezogenen Daten und einem besonderen Aspekt der Aussagefreiheit, also der Tätigkeit der Massenmedien im polnischen Rechtssystem.

Wir versuchen also den Personendatenschutz mit dem Recht auf die Privatsphäre zu verbinden? In der Rechtslehre „... wird allgemein angenommen, dass sich das Recht auf Privatsphäre u.a. auf den Schutz der personenbezogenen Informationen und die Garantie einer bestimmten Unabhängigkeit, im Rahmen dieser kann der Mensch über den Bereich des Zugänglichmachens und Kommuni-

---

dem Begriff privacy die „....Forderung des Menschen zum Entscheiden darüber wann und in welchem Umfang die Informationen über ihn zugänglich und anderen kommuniziert sein sollen." Dieser Zustand, wie man meinen kann, wird nie erreicht, schon wegen der zugelassenen Einschränkungen, die in den Art. 8 – 11 der EMRK oder in Art. 31 Abs. 3 der Verfassung der Republik Polen vorgesehen wurden und die auch für allgemein begründet gelten. Es ist auch notwendig, dass die gemäß bestimmten Erfordernissen formuliert werden, weil die Einschränkung eines Rechtes oder einer Freiheit kann nur dann erfolgen, wenn eine andere Norm, ein Grundsatz oder ein Wert dies erfordert und der Grad dieser Einschränkung muss im entsprechenden Verhältnis zu dem Interesse, dem die Einschränkung dient, bleiben – bei der Berufung der Notwendigkeitsklausel in der demokratischen Gesellschaft soll ausgewiesen werden, dass es ein dringender gesellschaftlicher Bedürfnis für diese Einschränkungen und derer Verhältnismäßigkeit zu dem zu realisierenden Zweck besteht, dabei darf man nicht vergessen, dass alle Einschränkungen in den gesetzlichen Akten vorgesehen werden müssen.

zieren mit anderen Personen über sein Leben entscheiden, bezieht ...“[8], ist also ein umfangreicherer Begriff als nur der Schutz von personenbezogenen Daten. Es besteht aber ein wesentlicher Zusammenhang zwischen den beiden – die Quelle der beiden ist die Menschenwürde (was sich direkt aus dem Grundgesetz ergibt) und der Zweck derer Schutzes ist die Sicherung der Unverletzlichkeit dieser Würde. Jedoch ist die direkte Funktion, die der Datenschutz zu erfüllen hat, zweifelsohne die Sicherung des Rechtes auf die Privatsphäre. Nach der Auffassung des Verfassungsgerichtes besteht zwischen den Art. 47 und 51[9] des geltenden Grundgesetzes ein folgendes Verhältnis: „... das in Art. 47 bestimmte Recht auf die Privatsphäre, wird u.a. unter dem Gesichtspunkt des Schutzes von personenbezogenen Daten, der in Art. 51 vorgesehen wurde, garantiert. Die letzte sehr ausgebaute Vorschrift, die sich sogar fünf mal auf die Bedingung der Legalität - *expressis verbis* in den Absätzen 1, 3, 4 und 5 und indirekt durch Bezug auf den Grundsatz des demokratischen Rechtsstaates in Abs. 2 - beruft, ist auch eine Konkretisierung des Rechtes auf Privatsphäre unter dem prozesuallen Gesichtspunkt ...“[10]

So sieht dies heutzutage, aber das Recht auf Privatsphäre war auch vor dem Inkrafttreten des neuen Grundgesetzes geschützt. In dem polnischen Rechtssystem waren auch Elemente des Datenschutzes zu bemerken. Sichtbar war vor allem das Streben nach Festlegung von fragmentarischen Regelungen, die die Grundsätze der Verar-

---

[8] Vergleiche das Urteil des Verfassungsgerichtes TK U 5/ 97 OTK 1998/4/46. Es muss betont werden, dass das Oberste Gericht schon 1984 in dem Urteil vom 18.01.1984 festgestellt hat, dass die Privatsphäre des Lebens ein persönliches Gut bildet, das aufgrund Art. 23 und 24 des Zivilgesetzbuches in bezug auf den offenen Katalog der in diesem Gesetzbuch formulierten persönlichen Güter geschützt wird. Das Bestehen des Rechtes auf Privatsphäre wurde auch in späteren Rechtsprechung des Obersten Gerichtes bestätigt, z.B. in dem Urteil vom 8. April 1994 (III ARN 18/94) in dem das Oberste Gericht die Konzeption des Schutzes von persönlichen Gütern (Art. 23 und 24 des ZGB) auf die Sphäre des Privatlebens und der intimen Sphäre bezieht.

[9] Art. 47 und 51 sind für dieses Thema von wesentlicher Bedeutung, der erste garantiert das Recht auf die Privatsphäre und der zweite den Schutz von personenbezogenen Daten. Für die Pressefreiheit sind dagegen Art. 14 und 54 bedeutsam. Die garantieren die Pressefreiheit, die Aussagefreiheit (darunter auch die Freiheit auf freie Gewinnung und Verbreitung von Informationen) und das Verbot der präventiven Zensur.

[10] Vergleiche das Urteil des Verfassungsgerichtes TK U 5/97 OTK 1998/4/46

beitung von personenbezogenen Daten bestimmten.[11] Von wesentlicher Bedeutung war hier deutlich die Garantie des Rechtes auf Privatsphäre durch völkerrechtliche Regelungen vom Bereich der Menschenrechte (vor allem Art. 12 der Erklärung der Menschenrechte, Art. 17 des Internationalen Paktes der bürgerlichen und politischen Rechte und Art. 8 der Europäischen Menschenrechtskonvention[12]), und die Verbindung dieses Rechtes – durch die europäische Rechtsprechung – mit dem allgemeinen Grundsatz des Rechtsregierung. Dies ermöglichte die Annahme, dass die Anerkennung und Gewährung von entsprechendem Schutz des Rechtes auf die Privatsphäre ein notwendiges Bestandteil des demokratischen Rechtsstaates ist, man könnte sich also auf Art. 1 des damals geltenden Grundgesetzes (in der Fassung vom 1989) berufen.

Früher gab es eigentlich keinen Schutz der Privatsphäre im Bereich des Schutzes von personenbezogenen Daten in dem Verhältnis der Staat – der Staatsbürger.[13] Zum Glück waren Computers in Polen erst Ende 80er Jahre allgemein zugänglich und erst dann begann man die Sammlung und Verarbeitung von personenbezogenen Da-

---

[11] Mehr zum Thema der Grundlagen der späteren als in anderen europäischen Staaten Regelung der Grundsätzen des Schutzes von personenbezogenen Daten und über Regelungen, die vor dem Inkrafttreten des Datenschutzgesetzes (es handelt sich hier um Art. 2 Abs. 1 Pkt.2 des Gesetzes vom 14. Dezember 1982 über den Schutz des Dienstgeheimnisses und des Staatsgeheimnisses, sog. Lustrationsgesetz des Sejm vom 28. Mai 1992 oder Art. 81 Abs. 5 Pkt.4 der Wahlordnung zum Sejm vom 1993) siehe auch z.B. B. Banaszak, Prawo do ochrony danych ososbowych w Polsce, w: T. Jasudowicz, C. Mik (red.) , O prawach człowieka w podwójną rocznicę Paktów, Księga pamiątkowa w Hołdzie Profesor Annie Michalskiej, *Das Recht auf den Schutz von personenbezogenen Daten in Polen*, *in: T. Jasudowicz, C. Mik (Hrsg.)Über Menschenrecht zum doppelten Jahrestag der Pakte. Gedenkbuch zur Ehre Frau Professor Anna Michalska,* Toruń 1996, S. 251- 254: B. Banaszak, Lustracja i dekomunizacja w Polsce w świetle praw jednostki w prawie wewnętrznym i międzynarodowym, w B. Banaszak (red.) Prawa Człowieka, Genza, koncepcje, ochrona, *Lustartion und Dekommunisierung im Lichte der Menschenrechte in dem Innen- und Völkerrecht in: Menschenrechte, Genese, Konzeption und Schutz,* Wrocław 1993 und die dort angegebene Literatur.

[12] Weil sogar der Pakt als auch die Konvention durch Polen ratifiziert wurden, waren und sind auch weiterhin die in diesen Akten bestimmten Normen auch für den polnischen Gesetzgeber das geltende Recht - obwohl man zugeben muss, dass der Ratifizierungsprozess (insbesondere bezüglich der Fragmente, die die Kontrolle und die Individualbeschwerden an das Europäische Gerichtshof für Menschenrechte) erst in 90er Jahren beendet wurde (Inkrafttreten am 10.10.1994 und am 01.11.1998)

[13] anders sah es aus auf der horizontalen Ebene

ten im größeren Ausmaß. In der ersten Phase der Computerisierung sah man den Bereich des technischen Fortschritts vor allem als Beitrag zur Zivilisationsentwicklung und als ein bequemes Verwaltungswerkzeug, man achtete damals nicht auf die damit verbundenen Gefahren. Damals war es schwer jemanden zum Schutz von personenbezogenen Daten als eines selbständigen Wertes (stark mit der Wahrung des Rechtes auf Privatsphäre verbunden) zu überzeugen. Interessanter ist, dass wir auch später, nach der Transformation, als die elektronischen Datenverarbeitungssysteme breiter wurden (nach der Computerisierung der öffentlichen Verwaltung) mit einer solchen Situation zu tun hatten.

In den ersten Entwürfen des neuen Grundgesetzes erschien das Problem des Schutzes von personenbezogenen Daten überhaupt nicht, erst Ende 1994 bemerkte man in verschiedenen Diskussionen und Arbeiten des Verfassungsausschusses der Nationalversammlung mehrere Aspekte dieses Problems.[14] Eine solche Stellungnahme, die dieses Problem am Rande stellte, war auch sehr oft in den Diskussionen über den Beginn der Arbeiten an dem polnischen Datenschutzgesetz zu bemerken (Anfang der 90 er Jahre). Neben den Vorschlägen der gesamten Regelung des Problems, gab es auch Anschauungen, die sich nur auf manche gewählten Aspekten des Datenschutzes konzentrierten, die mit bestimmtem Bedarf an Lösung der in Praxis vorkommenden Probleme verbunden waren. Es handelt sich vor allem um die sog. Lustration. In Bezug auf die Lustration merkte man oft die Unvollständigkeit der Archiven des Innenministeriums. Sehr oft betonte man, dass dies unmöglich macht, die genauen Informationen über die Mitarbeiter des ehemaligen Geheimdienstes der VRP zu bereiten, deshalb bemühte man sich auch darauf hinzuweisen, dass es in solcher Situation keine Bedingungen für genaue und objektive Prüfung der Daten gibt.[15]

---

[14] Die ersten Bemerkungen über die Gefahren, die mit der Verarbeitung von personenbezogenen Daten sind in den Berichten des Unterausschusses für Rechte und Pflichte der Bürger vom 23.11.1994, Biuletyn Komisji Zgromadzenia Narodowego nr X, Wydawnictwo Sejmowe Warszawa 1995, S. 95. Im Laufe der weiteren Arbeiten kehrte dieses Problem immer wieder zurück, vom 12 –absätzigen Artikel, der gleichzeitig das Recht auf die Privatsphäre und den Schutz von personenbezogenen Daten garantieren sollte, durch verschiedene Abkürzungen und Synthesen (Teilung von den beiden Fragen – der Artikel über personenbezgenen Daten hatte 2 Absätze) bis zu der endgültigen Fassung von Art. 51

[15] Vergleiche u. a. B. Banaszak, Die Aktualität des Lustrationswohlhabens in Polen in: Datenschutz und Datenfreiheit 3/97, S. 142 – 145

Das Ende war jedoch glücklich und die am 2. April 1997 verabschiedete Verfassung änderte grundsätzlich die allgemeine, mit dem Schutz des Rechtes auf Privatsphäre verbundene Situation. Das expressis verbis garantierte allgemeine Recht „....auf den Rechtsschutz des Privat- und Familienlebens, der Würde und des guten Rufes und des Rechtes auf Entscheidung über sein Privatleben....“ – Art. 47 und unabhängig davon die Garantie des Schutzes von personenbezogenen Daten gemäß Art. 51 ließen den Verzicht auf Ableitung des Rechtes auf derer Schutz aus den Vorschriften von Art. 23 und 24 des Zivilgesetzbuches zu (natürlich gibt es keine Hindernisse für die Berufung auf diese Vorschriften des Zivilgesetzbuches, vor allem im Falle eines Entschädigungsanspruches). Zu einem verfassungsrechtlichen Grundsatz wurde also der Schutz des Rechtes auf Privatsphäre, der nur in Ausnahmefällen, aufgrund des Grundgesetzes oder anderer Gesetze aufgehoben werden kann. Dies betrifft alle sich auf dem Gebiet der Republik Polen aufhaltenden Personen, weil dieses Recht als Menschenrecht und nicht ausschließlich als Bürgerrecht gilt. Etwas anders ist es im Falle des subjektiven Bereichs von Art. 51 der Verfassung, der wichtigsten Regelung bezüglich der personenbezogenen Daten. In Abs. 2 dieses Artikels ist nur von den Staatsbürgern die Rede – daraus könnte man die Schlussfolgerung ziehen, dass die öffentlichen Behörden die Informationen, die sich auf andere Personen beziehen verarbeiten dürfen, dabei müssen diese Daten gleichzeitig keine Bedingung der Unentbehrlichkeit in einem demokratischen Rechtsstaat erfüllen.[16]

[16] Und hier haben wir mit dem ersten Problem zu tun, weil die Formulierung: „... die in einem demokratischen Rechtsstaat unentbehrlichen Informationen über die Staatsbürger (...) ...” kann Auslegungsprobleme verursachen, weil man nicht genau weiß, was eigentlich diese unentbehrlichen Informationen sind und ob man sie mit den personenbezogenen Daten identifizieren kann? „... allgemein betrachtet könnte man die unentbehrlichen Informationen als Daten, die ein gewöhnliches Funktionieren des Menschen in einer zu einem Staat organisierten Gesellschaft ermöglichen und dessen Offenbarung Verletzung seiner Privatsphäre verursacht.”, B. Banaszak, M. Jabłoński, Konstytucje Rzeczypospolitej oraz komentarz do Konstytucji RP z 1997, *Verfassungen der Republik Polen und Kommentar zur Verfassung der RP von 1997*, (Hrsg.) J. Boć, Wrocław 1998, S. 99. Wenn man über dieses Problem aus dem Gesichtspunkt der Verwaltungsbehörden überlegt , wird als unentbehrlich jede Information ohne die diese Behörden nicht im Stand sind eine Handlung im Rahmen ihrer Zuständigkeit aufzunehmen (oder zu beenden), gesehen. Was den zweiten Teil der Frage anbetrifft, dann soll man mit ja beantworten, eine Folge dessen wird (natürlich nur in Bezug auf die Staatsbürger der

Art. 51 der Verfassung ist neben der Berechtigung des Bürgers im Bereich des Schutzes seiner Privatsphäre (z.B. gesetzliche Form für die Offenbarung von den auf ihn bezogenen Informationen) eine wesentliche Regelung, die ihm den Zugang zu den auf ihn bezogenen Informationen, die sich im Besitz der Staatsorgane oder der Organe der territorialen Selbstverwaltung befinden (es ist auch eine zusätzliche Verstärkung des in Art. 61 der Verfassung bestimmten Rechtes auf Gewinnung von Informationen über die Tätigkeit der öffentlichen Behörden oder des noch breiteren Rechtes auf Gewinnung und Verbreitung von Informationen – das sich aus Art. 54 Abs. 1 der Verfassung ergibt). Der in Art. 51 Abs. 2 gebrauchte Begriff : „amtliche Dokumente und Datensammlungen) weist darauf hin, dass es sich um alle möglichen Informationsquellen,[17] die sich in

---

Republik Polen – nach dem Beitritt zur EU soll es sich auf alle Bürger beziehen) eine Begrenzung der Möglichkeit der Sammlung von bestimmten Datenkategorien im Rahmen der schon bestehenden und der zu gründenden Datenbanken. Diese Meinung vertritt auch I. Lipowicz, die die Möglichkeit des Funktionierens von landesweiten und internationalen Datenbanken oder polizeilichen oder medizinischen informatischen Systemen nicht verneint und sie stellt folgendes fest: „... Wenn der Umfang von solchen informatischen Systemen wegen der Bequemlichkeit für die Verwaltung zu breit wird (für den Notfall werden größere Gruppen der Gesellschaft invigilliert, das einheitliche Informationskonto des Bürgers, das aus der Integrierung von hunderten Verwaltungsdaten von mehreren Bereichen entsteht) oder die Besonderheit der Daten zur Bildung von Personenprofilen führt (eine vereinfachte Charakteristik des Menschen) oder es kommt auch zu einer verborgenen oder offenen Bezeichnung der Bürger mit Identifizierungsnummern, die keinen Ordnungscharakter haben, sondern bezeichnen, dass wir mit einem Fall zu tun haben, der das was in einem demokratischen Rechtsstaat notwendig ist, überschreitet." (in: Konstytucje..., op. cit., *Verfassungen... op. cit*. S. 99 über das Verhältnis zwischen dem Datenschutzgesetz und der Verfassung siehe auch. K. Wygoda, Polska ustawa o ochronie danych ososbowych jako jedna z gwarancji prawa do prywatnosci*, Das polnische Datenschutzgesetz als eine der Garantien des Rechtes auf die Privatsphäre*, Prawa Człowieka – Humanistyczne Zeszyty Naukowe Nr. 5 / 1998, S. 119- 140.

[17] Es scheint, dass das Anbringen von personenbezogenen Informationen in irgendeinem für den Bedarf der öffentlichen Behörden verfassten oder veröffentlichten Schreiben (z.B. in einem Bericht, einer Entscheidung, einer Stellungnahme usw.) lässt auch die Möglichkeit der Wendung an diesen Rechtsträger mit dem Antrag auf Zugänglichmachung solcher Unterlage zu. was anderes ist die Feststellung, dass ein Schreiben den Erfordernissen eines amtlichen Dokuments erfüllt (z.B. kann man eine Dienstnotiz, die von dem Mitarbeiter einer bestimmten Institution verfasst wurde als amtliches Dokument betrachten?) oder ob die Frage des Informationsträgers von Bedeutung ist – reicht die elektronische Speicherung von Daten aus. Einiges erklärt das am 25. Juli 2001 vom Sejm (man wartet noch auf die Stellungnahme des Senats) verabschiedete Gesetz über den Zugang zu den öffentlichen Informationen in Art. 6.2: „ein amtliches Dokument (...) ist der Inhalt ei-

Besitz einer der drei Gewalten befinden , zu bemerken ist auch, dass er den Zugang zu den einzelnen Eintragungen, die keine größere Sammlung bilden auffordern lässt. Der Verfassungsgeber schloss keine der Sammlungen von Dokumenten oder Informationen im voraus aus (z.B. die Sammlungen die sich im Besitz von UOP - Amt für Staatsschutz oder Polizei befinden), es ist aber möglich, den Zugang zu diesen zu beschränken, wenn sie aufgrund eines Gesetzes eingeführt werden. An dieser Stelle muss man zum Art. 31 Abs. 3 der Verfassung greifen, der den Bereich der verfassungsrechtlich garantierten Rechte und Freiheiten ausschließlich auf die Situationen begrenzt, in denen es „... in einem demokratischen Staat wegen seiner Sicherheit oder öffentlichen Ordnung oder zum Schutz der Umwelt, Gesundheit, oder öffentlichen Moral oder Freiheiten und Rechte anderer Personen notwendig sind. Diese Einschränkungen dürfen nicht verletzen...“ Dies bezieht sich völlig auf die zu besprechende Berechtigung und wenn man berücksichtigt, dass „... die Verletzung des Wesens der Freiheiten und Rechte dann vorkommt, wenn eine gesetzliche Regelung in der Praxis die Ausübung der bürgerlichen Rechte und Freiheiten unmöglich macht....“[18], scheint die Meinung begründet zu sein, dass kein der Staatsorgane die Informationen über die Bürger nicht verarbeiten kann ohne dabei mit der Möglichkeit der Kontrolle durch diese zu rechnen. Bei der Berücksichtigung des, in diesem Kontext von wesentlicher Bedeutung, Grundsatzes der Verfassungsrechtlichkeit, stellen wir fest, dass die direkte Berufung der Verfassungsvorschriften gegenwärtig zu einer Norm in dem Prozess der Rechtsanwendung wurde, sowohl die Gerichte als auch die vollziehende Gewalt müssen gemäß den Vorschriften und auch gemäß dem Geist der Verfassung handeln.[19] Deshalb können auch Samm-

---

ner Willens- oder Wissenserklärung, der in beliebiger Form durch einen öffentlichen Funktionär im Sinne der Vorschriften des Strafgesetzbuches, im Rahmen seiner Zuständigkeit befestigt und unterschrieben wurde und an einen anderen Rechtsträger gerichtet wurde oder den Akten beigelegt wurde“ Obwohl diese Definition dem breiter verstandenen Recht auf Information dient (bezieht sich nicht nur auf personenbezogene Daten) scheint es berechtigt zu sein, dass die Konkretisierung der Verfassungsnormen Anwendung im Wege einer Analogie (in beiden Fällen haben wir mit dem Zugang zur Information zu tun) in der in Art. 51 Abs. 2 der Verfassung beschriebenen Situation finden kann.

[18] Vergleiche B. Banaszak, M. Jabłoński (in: Konstytucje... op. cit., *Verfassungen... , op. cit*., S.69

[19] Mehr zum Thema dieses Grundsatzes siehe z. B. K. Działocha, Zasada bezpośredniego stosowania konstytucji w dziedzinie wolności i praw obywateli (in:) Oby-

lungen, die als geheim qualifiziert wurden (z.B. wegen der Sicherheit des Staates) auch auf Antrag einer Person, auf die sie sich beziehen, verifiziert werden. Diese Verifizierung erfolgt sicher nicht in Form von direktem Zugang des Interessierten zu diesen Daten (und wenn schon, dann nach Einführung von bestimmten zeitlichen Beschränkungen für die Offenbarung dieser Informationen), dann wird dank der Möglichkeit der Berufung an den Generalinspektor für den Schutz der personenbezogenen Daten (weiter GIODO) und dann an das Hauptverwaltungsgericht der inländische Rechtsweg ausgenutzt [20] und über die Sache kann dann das Europäische Gerichtshof für Menschenrechte entscheiden. Es wird die Angelegenheit in Bezug auf die Bestimmungen der Europäischen Konvention der Menschenrechte prüfen und kann auch die Offenbarung der als geheim geltenden Informationen verlangen. [21]

Das Gesetz über Schutz von personenbezogenen Daten[22], die eine Erweiterung des Art. 51 der Verfassung ist, soll immer und wird auch im Kontext der Verfassungsnormen gelesen werden. Es ist schon in der allgemeinen Anerkennung (sogar durch die Rechtsleh-

---

watel – jego wolności i prawa, Zbiór studiów przygotowanych z okazji 10 – lecia urzędu Rzecznika Praw Obywatelskich, *Der Grundsatz der direkten Anwendung der Verfassung im Bereich der Freiheiten und Rechte der Bürger, in: Der Bürger – seine Freiheiten und Rechte, Eine Sammlung von Studien zum 10. Jahrestag des Amtes des Bürgerbeauftragten.,* Warszawa 1998, S. 26 – 44 und die dort angegebene Literatur.

[20] Der Bürger kann auch die Verfassungsklage einreichen, was ähnliche Folgen wie die Handlungen des Hauptverwaltungsgerichts verursachen wird, wenn man sich an das Verfassungsgericht wendet, um die Feststellung der Verfassungsrechtlichkeit der Vorschriften aufgrund denen die Daten als geheim gelten – dann wird es von dem Verfassungsgericht abhängig, ob es diese Einschränkung als begründet findet. Im Zweifelsfall wird es sicher den Zugang zu den „strittigen" Informationen verlangen. Wenn sich eine Personen an die internationalen Organe wenden will, dann ist die Klage an das Verfassungsgericht (falls das Hauptverwaltungsgericht keine entsprechende Handlungen vornimmt) grundsätzlich obligatorisch.

[21] Das Gerichtshof in Straßburg wird die eingereichte Klage in folgender Reihenfolge prüfen: ob die durch den Klagenden genannten Fakten eine Verletzung eines bestimmten Rechtes oder einer bestimmten Freiheit bilden, ob der Eingriff gemäß des Landesrechtes zugelassen war und ob er in einer demokratischen Gesellschaft notwendig war. In der letzten Phase, kann für die richtige Beurteilung der Situation die Offenbarung der geheimen Informationen, zu denen der Bürger keinen Zugang hatte, notwendig werden.

[22] Mehr über das Gesetz über den Schutz von personenbezogenen Daten siehe B. Banaszak, K. Wygoda „Polish Legal Regulations Concercing the Protection of Personal data in Light of the Law of 29 August 1997" (in:) Constitutional Essays (editor) ; . Wyrzykowski, Warsow 1999

re als auch den GIODO) zu bemerken, dass die bisherige, ohne Zweifel wegen der Verengung des Begriffes, fehlerhafte Definition der personenbezogenen Daten, die in Art. 6 des Datenschutzgesetzes formuliert wurde, gemäß den Verfassungsbestimmungen, in denen von den personenbezogenen Daten die Rede ist (wenn man nur diese Sprachauslegung des Gesetzes anwenden möchte, dann würden die meisten der Daten nicht dem Schutz unterliegen) ausgelegt wurde. Die Verfassung lässt anzunehmen, indem sie darauf hinweist, dass eine Information als personenbezogen betrachtet werden kann bis zu diesem Moment wenn die Feststellung der Identität einer bestimmten Person, die sie betrifft, möglich ist, dass unser Gesetz (nach entsprechender Auslegung) die Erfordernisse, die gegenüber Polen durch die Europäische Union gestellt wurden, erfüllt.[23]

Zu bemerken ist, dass die Bestimmungen der Verfassung vor allem an die Staatsorgane gerichtet werden (es wird von öffentlichen Behörden oder von amtlichen Dokumenten und Datensammlungen gesprochen), man kann jedoch daraus nicht ziehen, dass die nichtöffentlichen Rechtsträger keinen sich aus Art. 51 ergebenden Einschränkungen unterliegen. Wie schon richtig I. Lipowicz bemerkte: „...in Art. 51 gibt es keine Teilung in das öffentliche und private Sektor. Dies bedeutet, dass auch wenn ein Kraftwerk oder die Telekommunikation nach Informationen verlangt, wird eine gesetzliche Grundlage notwendig, wenn dies zu einer Informationspflicht werden soll. Die Erteilung von Informationen über eigene Person kann ein Teil des Vertrages sein, sie muss aber in den Grenzen des Vertrages bleiben und eine freie Wahl lassen...“[24] Dasselbe betrifft auch die Tätigkeit der Journalisten.

So sind wir endlich zum Problem des Schutzes von personenbezogenen Daten in der Pressetätigkeit gelangt. Man braucht nieman-

---

[23] Die durch den Gesetzgeber am Anfang angenommene Definition war (worauf sehr oft die Rechtslehre und der GIODO aufmerksam machten) nicht zufriedenstellend, insbesondere bezüglich der internationalen Standards – die Novelle vom 26.07.2001 ändert diese Situation. Die neue Fassung des Art. 6 des Datenschutzgesetzes entspricht völlig den europäischen Erfordernissen.

[24] vergleiche I. Lipowicz, Konstytucyjne prawo do informacji a wolnosc informacji (w:) Wolnosc informacji i jej granice (Hrsg.) G. Szpor, *Verfassungsrechtlich garantiertes Recht auf Information und die Informationsfreiheit, in: Informationsfreiheit und derer Grenzen*, Katowice 1997, S. 14

den zu überzeugen, dass die in verschiedenen Veröffentlichungen personenbezogenen Informationen genutzt werden – die Frage ist, ob diese Tätigkeit rechtlich geregelt wurde.

Am Anfang haben wir und auf das Pressegesetz berufen, weiter haben wir auch einige verfassungsrechtliche Grundsätze erwähnt, es bestehen also bestimmte allgemeine Normen. Leider bleibt vieles durch diese Normen ungeklärt. Die Tatsache, dass das Pressegesetz für den Bedarf einer anderen Staatsverfassung gebildet wurde (als Massenmedien vor allem ihre Propagandarolle zu erfüllen hatten) disqualifiziert es nicht als eine Rechtsquelle - es wurde doch mehrmals novelliert – zusätzlich verschärft noch die Spannung (sogar den Konflikt) zwischen dem Schutz von personenbezogenen Daten und dem freien Zugang und Nutzung von diesen Informationen durch die Journalisten. Die Situation wurde noch schwieriger wegen der Nichtverabschiedung des „Informationsgesetzes“ – obwohl die Arbeiten an diesem Gesetz während jeder Amtszeit des Parlaments seit 1989 bis 2001 vorgenommen wurden.[25] Es fehlte also an der Grundbestimmung, die die Weise der Informationsgewinnung regelt und zugleich eine Ergänzung des Pressegesetzes ist (*nota bene* versuchte man auch im Fall des Pressegesetzes eine völlig neue Regelung zu verabschieden – bis jetzt aber ohne Erfolg). Wir waren darauf gewiesen, die allgemeinen und in dem prozessualen Aspekt[26] nicht präzisierten Normen anzuwenden. Das

[25] Am 25.07.2001 verabschiedete der Sejm endlich das Gesetz über Zugang zu den öffentlichen Informationen, was die Ausübung der Verfassungsgarantien erleichtern soll. Diese Akte (als das Referat geschrieben wurde, dauerte noch der Legislationsprozess und der Senat konnte noch Berichtigungen anordnen - im schlimmsten Fall konnte das Gesetz überhaupt nicht angenommen werden – das Gesetz soll theoretisch am 1.Januar 2002 in Kraft treten) soll samt dem Gesetz über den Schutz von personenbezogenen Daten und dem am 22.01.1999 verabschiedeten Gesetz über den Schutz der nicht offenen Informationen – das die Grundsätze für den Zugang und die Verarbeitung von solchen Daten bestimmt - soll eine Grundlage für einen einfacheren und mehr vorsehbaren Zugang zu Informationen für alle bilden.

[26] Das Gesetz über den Zugang zu den Öffentlichen Informationen wird gerade in den prozessualen Angelegenheiten besonders gebräuchlich. Es bestimmt drei alternative Weisen der Gewinnung von Informationen und den Berufungsweg im Falle der Absage der Informationserteilung. Ausnahmen von dem Öffentlichkeitsgrundsatz wird im Sinne des neuen Gesetztes die Einschränkung, die sich aus anderen Gesetzen ergibt (am häufigsten aus dem Gesetz über den Schutz von unöffentlichen Informationen und anderen gesetzlich geschützten Geheimnissen, z.B. dem Datenschutzgesetz) oder auch in Bezug auf die Wahrung der Privat-

Pressegesetz, obwohl es genauer als die Verfassung ist, beruft sich selten auf den Begriff der personenbezogenen Daten,[27] häufiger werden andere Formulierungen gebraucht. Es gebraucht dabei, was auch zu verstehen ist, Begriffe, die sich mehr auf die Privatsphäre als eine solche beziehen, wie z.B. „persönliches Gut“ (Art. 12.2), „Informationen und Daten die die Privatsphäre des Lebens betreffen“ Art. 14.6), „Daten, die Identifizierung des Verfassers eines Presseartikels ermöglichen“ (Art. 15.2) – der letzte Begriff ist zweifelsohne ein Synonym für die personenbezogenen Daten. Daraus erfolgt, dass bei der Prüfung des Verhältnisses zwischen dem Schutz von personenbezogenen Daten und den Massenmedien soll man diese unter dem Gesichtspunkt der in dem Datenschutzgesetz gefassten Grundsätze wahrnehmen (auch wenn man annimmt, dass das Gesetz über den Zugang zu Informationen in der gegenwärtigen Fassung in Kraft tritt, wird dadurch das Verhältnis zwischen den Journalisten und den Vorschriften des Datenschutzgesetzes nicht wesentlich geändert – mit Ausnahme dieses Teils der personenbezogenen Daten, die die öffentliche Ämter bekleidenden Personen betreffen).

Es kommt also die Frage, ob alle Fälle der Verarbeitung von personenbezogenen Daten durch die Presse den rechtliche Regelungen, die aus dem Datenschutzgesetz erfolgen, unterliegen? Natürlich nicht. Viele haben ihre Grundlagen in dem Pressegesetz oder in der Verordnung des Ministerrates vom 7. November 1995 über die Weise auf die Informationen der Presse zugänglich gemacht werden

---

sphäre von natürlichen Personen (unter Vorbehalt mancher Informationen über die Personen die im öffentlichen Dienst bleiben) oder des Geheimnisses eines Unternehmers. Es ist schwer zu sagen, ob dieses Gesetz ausreichend wird, es ist jedoch ein großer Fortschritt.

[27] Nur in Art. 13.2 und 3 des Pressegesetzes wird dieser Begriff gebraucht: „2. Es ist verboten in der Presse personenebezogene Daten und Bilder von Personen zu veröffentlichen, gegenüber denen eine Ermittlung oder ein Gerichtsverfahren geführt wird, dies betrifft auch personenbezogene Informationen und Bilder von Zeugen, Verletzten und , es sei, diese Personen haben es zugestimmt. Geschädigten . 3. Die Einschränkung die in Abs. 2 erwähnt wurde verletzt die Vorschriften von anderen Gesetzen nicht. Der zuständige Staatsanwalt oder das zuständige Gericht kann wegen eines wichtigen gesellschaftlichen Interesses genehmigen, die personenbezogenen Daten und das Bild der Personen gegenüber denen eine Ermittlung oder ein Gerichtsverfahren geführt wird, zu veröffentlichen.” wie es aber scheint stimmt diese Weise nicht mit dem Datenschutzgesetz überein, wo das Bild einer Person ohne Zweifel zu den personenebezogenen Daten gehört und dessen Ausschluss zwecklos wäre.

und über die Organisation und Aufgaben der Pressesprecher der Behörden der Regierungsverwaltung (erlassen aufgrund Art. 11 Abs. 4 des Pressegesetzes). Die Grundlagen für die Informationserteilung, die insbesondere die Handlungsweise bestimmen, sind, im Grunde genommen, die einzelnen Verfahren gemäß dem Verwaltungs-, Zivil- und Strafrecht. Welche Vorschriften soll man also anwenden, wenn man ein richtiges Modell der Nutzung von personenbezogenen Daten in der Tätigkeit der Journalisten schaffen möchte?

Es gibt einige Situationen, in denen es keine Zweifel bestehen, dass man sich nach den Vorschriften des Datenschutzgesetzes richten soll. Zu solchen gehören:

a) alle Radaktionsdatensammlungen, sowohl die aktuellen Sammlungen als auch die Archive (die in meisten Fällen in elektronischen Form geführt werden – die Vorschriften des Datenschutzgesetztes gelten aber unabhängig von der Form), die eine große Zahl von personenbezogenen Daten enthalten und immer öfter auch den Personen von außerhalb des Journalistenkreises;

b) das Bestehen von Informationsagenturen, die Service vorbereiten (wie z.B. PAP, AFP, Reuter – die verbinden immer öfters mehrere Medien, von Presseservicen, über Radio- und Fernsehservicen bis zu Internetservicen), die alle Informationen zwecks weiterer Verarbeitung sammeln (manche enthalten auch personenbezogenen Daten), darunter auch die Übersendung von diese Informationen an verschiedene, auch ausländische Empfänger;

c) die Gewinnung von Informationen durch Journalisten, insbesondere die Nutzung von verschiedenen Sammlungen von personenbezogenen Daten (oder solchen, die neben anderen Daten auch personenbezogene Daten enthalten).

Der letzte Punkt kann eine Anregung für die weitere Diskussion bilden, insbesondere in Bezug auf das Fehlen an eine Presseklausel in dem polnischen Gesetz über den Schutz von personenbezogenenen Daten oder im Pressegesetz, die vor allem nach der Erleichterung des Zugangs zu den personenbezogenen Daten gerichtet

sind oder sogar manche Vorschriften über derer Schutz ausschließen. Die Ausnahme von Art. 5 Abs. 2 des Gesetzes über den Zugang zu öffentlichen Informationen, die die Informationen über die Personen, die öffentliche Ämter bekleiden, betreffen, die mit diesen Funktionen verbunden sind, darunter auch über die Bedingungen der Bekleidung von diesen Ämtern und wenn eine natürliche Person oder ein Unternehmer allein auf ihre Rechte verzichtet oder die Informationen selbst veröffentlicht, wird dieses Problem nicht lösen. Die europäischen Erfordernisse in diesem Bereich sind streng.[28] Die Weise der Informationsgewinnung – auch der echten Informationen - ist doch nicht gleichgültig (Diebstahl oder Abhorchen u. ä. sind in jedem Fall zu tadeln), sie soll im Einklang mit den Rechtsvorschriften und mit den Grundsätzen der Journalistenethik belieben. Wenn die zu verarbeitenden (für Journalistikzwecke) Daten zusätzlich noch zu den sensitiven Daten gehören, ist es besonders einfach die Grenze zwischen dem Schutz von Personen und dem Interesse der Redaktion zu überschreiten. Das Gewicht und der Charakter der Information muss dem Zweck, dem derer Offenbarung dient, entsprechen, weil der Verhältnismäßigkeitsgrundsatz in diesem Fall der einzige ist, der uns die Meinung des Journalisten, dass in einem bestimmten Fall das Interesse der Gesellschaft wichtiger war als das Interesse des einzelnen Menschen, zu beurteilen lässt und diese eventuell zu teilen.[29]

Wie es schon erwähnt wurde, fehlt es in dem polnischen Gesetz an solche Regelungen. Einige Ähnlichkeiten könnte man in Art. 1 Abs. 2 des Datenschutzgesetzes finden, in dem die Ursachen, für die die Verarbeitung von Daten überhaupt möglich ist angegeben wurden.[30]

---

[28] z. B. Der Text der Resolution der Parlamentsversammlung des Europarates 428 (1970, der eine Erklärung über die Massenmedien und Menschenrechte enthält, oder Pkt. 37 der Präambel der Richtlinie 95/46/EU vom 24. Oktober 1995

[29] In dem englischen Gesetz über den Schutz von personenbezogenen Daten (Data Protection Act 1998) gibt es in Art. 32 ein interessantes Beispiel für die Einführung von Voraussetzungen, die erfüllt werden müssen, damit man für journalistische Zwecke (also mit der Absicht der Veröffentlichung eines Materials aufgrund der verarbeiteten Daten) auf den Grundsatz des Datenschutzes verzichten kann (mit Ausnahme des Verzichtes auf die Standards der Verarbeitungssicherheit). Mehr zu diesem Thema siehe z.B. S. Rasaiah, Current Legislation, privacy and the media in the UK, Communikations Law 1998, Band 3, Nr. 5, S. 183 und folgende.

[30] Art. 1 Abs. 2 besagt folgendes: „Personenbezogene Daten können im öffentlichen Interesse, im Interesse des Betroffenen, oder eines Dritten in dem Umfang und in der durch dieses Gesetz bestimmten Weise verarbeitet werden."

Wenn wir unsere Aufmerksamkeit auf dem ersten und dem letzten Teil dieses Absatzes konzentrieren, erhalten wir einen Hinweis, der uns die Datenverarbeitung in bezug auf das öffentliche Gut in dem im Gesetz bestimmten Umfang und auf eine gesetzliche weise lässt. Aus diesem Artikel erfolgt aber auch, dass die Verarbeitung von allen sich auf eine Person beziehenden Informationen vor allem mit derer Zustimmung möglich ist - als ein Grundsatz soll diese Vorschrift in den meisten Fällen des Gebrauchs von Informationen für die medialen Zwecke Anwendung finden (es scheint, dass sie auch eventuelle Probleme der Verletzung von persönlichen Gütern beseitigen könnte).

Weitere Voraussetzungen (die unabhängig von der Zustimmung der Person, auf die sich die Daten beziehen) sind in Art. 23 Abs.1 des Datenschutzgesetzes zu finden. Unter fünf Punkten scheinen drei in Bezug auf Medien anwendbar zu sein (jeder kann als eine selbständige Grundlage für die Verarbeitung von personenbezogenen Daten dienen). Gemäß diesen ist die Verarbeitung von Daten in folgenden Fällen zugelassen:

– es wird durch die Rechtsvorschriften zugelassen (Pkt.2),

– es ist für die Erfüllung der gesetzlich bezeichneten Aufgaben, die für das öffentliche Gut realisiert werden, unentbehrlich (Pkt. 4)

– es ist unentbehrlich für die Erfüllung der berechtigten Zwecke der Datenverwalter, die in Art. 3 Abs. 2 (natürliche und juristische Personen und Organisationseinheiten ohne Rechtspersönlichkeit, die die Daten im Zusammenhang mit Erwerbs- oder Berufstätigkeit oder zum Erreichen von Satzungszwecken verarbeiten), und die Datenverarbeitung verletzt keine Rechte und Freiheiten der Person, auf die sich die Daten beziehen (Pkt. 5).[31]

[31] Nach der Novelle erhält diese Vorschrift einen neuen Wortlaut und zwar: „ unentbehrlich für die Erfüllung der rechtlich begründeten Zwecke der Datenverwalter, die in Art. 3 Abs. 2 erwähnt wurden, oder der Dritten, denen diese Daten übergeben werden – und die Datenverarbeitung keine Rechte und Freiheiten des Betroffenen verletzt.“ – es scheint dass diese Fassung die Lage der Journalisten verbessert, weil in dem Pressegesetz dieser „rechtlich begründeter Zweck“ einfach zu finden ist und die Berücksichtigung der anderen Rechtsträger vergrößert die Möglichkeit des Informationsaustausches.

Eine andere Situation wird in Art. 27 Abs. 2 des Datenschutzgesetzes beschrieben, in dem die Ausnahmefälle von dem Verbot der Verarbeitung von sensitiven Daten bestimmt werden. Für uns sind insbesondere Punkte 2 und 8, die die Verarbeitung von sensitiven Daten in folgenden Fälle zulassen:

– wenn eine besondere Vorschrift eines anderen Gesetzes die Verarbeitung von solchen Daten ohne Zustimmung der Person auf die sie sich beziehen zulässt und völlig deren Schutz garantiert,

– die Verarbeitung betrifft die Daten, die durch die Person auf die sie sich beziehen, öffentlich bekannt gegeben wurden.

Bemerkenswert ist, dass die sensitiven Daten bis jetzt keine „... Daten, die Verurteilung, Bestrafung, Strafmandaten und andere Entscheidungen, die im Gerichts-, oder Verwaltungsverfahren erlassen wurden, betreffen, [deren Verarbeitung] kann ausschließlich aufgrund des Gesetztes geführt werden“ (Art. 28 Abs. 1 des Datenschutzgesetzes)[32] umfassten. Die Probleme der Ermittlungsjournalistik und der Gerichtsverfahrensberichte werden noch am Ende dieses Vortrages erwähnt.

Unter den für unsere Analyse notwendigen Regelungen befindet sich noch Art. 47 Abs. 3 Pkt. 4 des Datenschutzgesetzes (besonders nützlich in der Tätigkeit der Agenturen), der die Übergabe von personenbezogenen Daten ins Ausland zulässt, wenn dies in Bezug auf das öffentliche Gut notwendig ist. In solchen Fällen wird es sogar unwichtig, ...“ob dieses Zielland auf seinem Gebiet mindestens einen solchen Schutz von personenbezogenen Daten, wie auf dem Gebiet der Republik Polen gilt, garantiert ...“, was die Grundlage für den grenzüberschreitenden Informationsverkehr bildet.

Wir hoffen, dass es uns gelungen ist, trotz des Fehlens von den strikte medialen Regelungen in dem Datenschutzgesetz, auf einige

[32] Die erwähnte Novelle ändert diesen Tatbestand indem es sie zu dem Katalog der besonders sensitiven Daten zufügt – so wird die Möglichkeit derer Verarbeitung aufgrund derselben Vorschriften erfolgen, wie der Fall der übrigen sensitiven Daten ist.

Bestimmungen, die in der Journalistentätigkeit nützlich sein können, hinzuweisen. Wir möchten die jetzt näher betrachten.

Primo, bei Berücksichtigung der Aufgaben die die Presse in den demokratischen Staaten zu erfüllen hat (bestätigt u.a. in Art. 1 des Pressegesetzes, in der Verfassung und in den völkerrechtlichen Akten) dient sie aufgrund der gesetzlichen Rechtsvorschriften, ohne Zweifel, dem öffentlichen Gut (grundsätzlich) - dies ist mit dem Grunderfordernis für die die Daten verarbeitenden Subjekte verbunden.

Secundo, man kann annehmen, dass die Vorschriften des Pressegesetzes den Erfordernissen entsprechen, die notwendig sind, um die als die Datenverarbeitung zulassenden Vorschriften, die in Art. 23 Abs. 1 Pkt. 2 des Datenschutzgesetzes und Art. 27 Abs. 2 Pkt. 2 erwähnt wurden, zu betrachten. Auch trotz der Zweifel, die mit der Genese des Presserechts verbunden sind, ist die Freiheit der Erhebung, Sammlung und weiterer Verarbeitung von Informationen, darunter auch personenbezogener Informationen ein festes Bestandteil des darin beschriebenen Rechtes auf Information, Aussagefreiheit und Freiheit der Kritik, die sowohl verfassungsrechtlich als auch gesetzlich bestätigt wurden (darunter auch derer Zugänglichmachen – weil das letztendlich der Zweck ist). Eine Rolle der völligen Garantie des Schutzes dieser Daten erfüllen die Vorschriften über das Journalistengeheimnis.[33] Ähnliche Bedeutung hat auch Pkt. 4 Abs. 1 des Art. 23 des Datenschutzgesetzes. Er führt die Voraussetzung der

[33] Laut Art. 15 des Pressegesetzes werden durch den Umfang des Journalistengeheimnisses die Daten gefasst, die die Identifizierung des Verfassers eines Pressematerials, eines Briefes an die Redaktion oder eines anderen Materials mit solchem Charakter ermöglichen, wenn sich diese Personen sich Anonymität vorbehalten haben und die Veröffentlichung ihrer personenbezogenen Daten sowie Daten der Personen, die die veröffentlichten oder zur Veröffentlichung übergebenen Information erteilten, wenn auch diese die Anonymität vorbehalten haben, nicht zustimmten. Darüber hinaus werden als Journalistengeheimnis auch alle Informationen betrachtet, mit denen sich der Journalist vertraut machte und derer Veröffentlichung die rechtlich geschützte Interesse der Dritten verletzen könnten. Über die Befreiung von der Pflicht der Geheimhaltung bestimmt Art. 16 des Pressegesetzes, sie wird nur nach Zustimmung der geschützten Personen möglich (Verfasser oder Personen die Informationen unter Vorbehalt der Vertraulichkeit erteilen), oder wenn es sich um Informationen, die mit der in Art. 240 §1 des Strafgesetzbuches bezeichneten Straftat verbunden sind. Diese Geheimhaltung gilt für alle Mitarbeiter der Redaktion (sowohl für den Hauptredakteur als auch Personen, die keine Journalisten sind).

„Unerlässlichkeit“ in der Ausübung seiner (gesetzlich bestimmten – in diesem Fall in dem Gesetz und in der Verfassung) Aufgaben ein und zugleich die Voraussetzung derer Realisierung für das öffentliche Gut. Wir wollen nicht behaupten, nach dem Beispiel der amerikanischen Rechtslehre, dass die Presseaussagen dem öffentlichen Gut dienen (in manchen Situationen können sie sogar schädlich sein – z.B. absichtliche falsche Darstellung von Tatsachen – und oft scheinen sie gleichgültig zu sein - z.B. die rein kommerzielle Tätigkeit der Massenmedien), es ist aber nicht einfach die wichtige gesellschaftliche Rolle der freien Medien in dem gegenwärtigen Staat nicht zu beachten. Wenn also die Datenverarbeitung der Journalistentätigkeit, die zwecks Erfüllung der öffentlichen Aufgaben der Presse unternommen wurde und für derer richtige Erfüllung notwendig ist, dann erfüllt sie auch die Bedingungen der Legalität.

Tertio zweifelsohne sind wir damit einverstanden, dass die Verarbeitung von personenbezogenen Daten sehr oft für die berechtigten Zwecke der Datensammlungenverwalter (Datenverwalter sind alle Redaktionen und Informationsagenturen) notwendig sind, die die Daten im Zusammenhang mit der Erwerbs- oder Berufstätigkeit oder für die Durchführung von Satzungszwecken verarbeiten. Wenn eine solche Verarbeitung gleichzeitig keine Rechte und Freiheiten der Personen, auf die sie sich beziehen, verletzt, dann erfüllt sie die in Art. 23 Aba.1 Pkt. 5 des Datenschutzgesetzes vorgesehenen Bedingungen.

Die oben genannten Grundsätze der Nutzung von personenbezogenen Daten scheinen das Unternehmen von solchen Tätigkeiten durch die Medien zu ermöglichen. Jedoch ist es für die Rechte und Pflichte, deren die Redaktionen und Journalisten unterliegen, nicht gleichgültig, aufgrund welcher dies erfolgt. Wenn wir annehmen, dass die Voraussetzungen von dem Art. 23 Abs. 1 Pkt. 4 und 5 des Datenschutzgesetzes am besten die Lage widerspiegeln, dann werden dem Betroffenen folgende Rechte zustehen:

– das Recht auf Einreichung einer schriftlichen, begründeten Forderung auf Aufhören der Datenverarbeitung in bezug auf seine besondere Lage,

– das Recht auf Einreichung eines Widerspruchs gegen die Verarbeitung von Daten in bestimmten Fällen, der Verarbeitung für Marketingzwecke oder der Übergabe von Daten an einen anderen Verwalter.[34]

Die Ausübung von diesen Rechten kann die Tätigkeit der Medien wesentlich erschweren. Noch mehrere Probleme erscheinen im Falle der Verarbeitung von sensitiven Daten (vom Art. 27 des Datenschutzgesetzes) oder von den in Art. 28 Abs. 1 des Datenschutzgesetzes bestimmten Daten über „Überschreitung des Grenzen des Rechtes".

Eine viel bessere Lösung scheint die Befürwortung der Stellung über die Freiheit der Datenverarbeitung durch die Medien im Rahmen der Pressefreiheit (mit derer Einschränkung, die sich aus der Verfassung, dem Presserecht und den völkerrechtlichen Akten ergibt), die für das öffentliche Gut handelt, was eine den Einfluss des Datenschutzgesetztes auf die Journalistik „mildernde" Voraussetzung bilden könnte (eine quasi Presseklausel) – die Grundlagen für die Handlungen der Presse würden Art. 1 Abs. 2 und Art. 23 Abs. 1 Pkt2 des Datenschutzgesetzes. Auch in solchem Fall wird die schützende Rolle des Datenschutzgesetztes nicht völlig ausgeschlossen – welche Grundsätze sollten also immer beachtet werden?

Für unverletzlich gelten die Normen, die sich aus den allgemeinen Vorschriften ergeben (Kapitel 1 des Datenschutzgesetzes) und aus dem Kapitel über den Inspektor für den Schutz personenbezogener Daten (Kapitel 2). Es besteht auch keine Möglichkeit des Ausschlusses der Sicherheitsgrundsätze der Datenverarbeitung in den Sammlungen (Kapitel 5 und die Ausführungsverordnungen), derer Registrierung (Kapitel 6) und der strafrechtlichen Verantwortlichkeit (Kapitel 8). Der Charakter von diesen Regelungen hat keinen Einfluss auf die Einschränkung der Aussagefreiheit und bildet Garantie für die Sicherung des Rechtes auf die Privatsphäre in bezug auf die personenbezogenen Daten. Solche Bedeutung hat Art. 2 Abs. 1 und 2 des Datenschutzgesetzes, der besagt: „ ... das Gesetz bestimmt

[34] Die in Art. 32 Abs. 1 Pkt. 7 und 8 bestimmten Rechte finden keine Anwendung in der in Art. 23 Abs. 1 Pkt. 2 bezeichneten Situation, also im Falle der Verarbeitung von Daten aufgrund der Rechtsvorschriften.

die Grundlagen des Verfahrens für die Verarbeitung personenbezogener Daten und die Rechte natürlicher Personen, deren personenbezogene Daten in Datensammlungen verarbeitet werden oder verarbeitet werden können. 2. Das Gesetz findet auf die Verarbeitung personenbezogener Daten in Computersystemen sowie in Karteien, Verzeichnissen, Büchern, Aufstellungen und in anderen Sammlungen von Daten Anwendung.“ Der Gesetzgeber vertritt die Ansicht, dass weder das Ort noch die Form der Datenspeicherung oder der Datenverwalter grundsätzlich für die Sicherung des Schutzes der Privatsphäre bedeutend ist - alle sollen immer die Sicherheit der Daten gewährleisten und auch in den Fällen, in denen eine Abweichung von den bestimmten Verarbeitungsregeln möglich ist (aufgrund gesetzlicher Vorschriften) kann man auf die Anwendung der Vorschriften des Gesetzes über den Schutz personenbezogener Daten nicht völlig verzichten.

Die Massenmedien müssen also die in Art. 26 des Datenschutzgesetzes bestimmten Regel, die den Datenverwalter zur Beachtung der erforderlichen Sorgfalt zwecks Schutzes der Personen, auf die sich diese Daten beziehen verpflichten, beachten. Insbesondere geht es um Sicherung, dass die Daten:

1. gemäß dem Recht verarbeitet werden,

2. für einen gesetzlich bestimmten Zweck erhoben werden und keiner weiteren diesem Zweck widrigen Verarbeitung unterzogen werden,

3. sachlich richtig werden und dem Zweck für den sie verarbeitet werden entsprechen werden,

4. in solcher Form aufbewahrt werden, die die Identifizierung der Betroffenen nicht länger als dies für den Zweck der Verarbeitung notwendig ist, ermöglichen werden.

Diese Bestimmungen sind eine Art. der Erweiterung – in bezug auf die personenbezogenen Informationen – der in Art. 12 des Pressegesetzes bestimmten Regeln, aufgrund deren der Journalist u.a. :

– zur Beachtung der besonderen Sorgfalt und Redlichkeit bei der Sammlung und Nutzung von Pressematerial und insbesondere zur Prüfung der erworbenen Informationen nach der Wahrheitsübereinstimmung oder zur Angabe derer Quellen,

– das persönliche Rechtsgut und darüber hinaus das Interesse der im guten Glauben handelnden Informatoren und anderer Personen, die ihm vertrauen zu schützen

verpflichtet.

Das Gebot der Beachtung der besonderer Sorgfalt betrifft auch Handlungen die eine Antwort auf die Rechte der betroffenen, die in Art. 35 des Datenschutzgesetzes[35] bestimmt wurden. In der Novelle dieses Artikels wurde noch Abs. 3 eingeführt: „... der Datenverwalter ist verpflichtet, andere Verwalter, denen die personenbezogenen Daten zugänglich gemacht wurden, über die Vervollständigung, Aktualisierung oder Berichtigung der Daten unverzüglich zu informieren.“. Wenn wir eine Redaktion als einen Verwalter betrachten (oder einen in deren Auftrag handelnden Journalisten, der eigene Datensammlung besitzt) dann sehen wir die Ergänzung des Rechtes auf Berichtigung, die auf die ebene des Austausch von Nachrichten und Servicen zwischen Informationsagenturen, übertragen wurde. Wir haben also mit einer noch größeren Sorgfalt um die Richtigkeit und Adäquanz personenbezogener Daten – nicht nur eine einfache Berichtigung einer Nachricht an der Stelle, wo sie veröffentlicht wurde aber auch die Verpflichtung zur Benachrichtigung anderer Rechtsträger, die diese Nachricht nutzen können, unabhängig davon, ob solche an die Gesellschaft gerichtete Berichtigung überhaupt veröffentlicht wurde.

[35] Art. 35 Abs. 1 des Datenschutzgesetzes hat folgenden Wortlaut: „Kann der Betroffene nachweisen, dass die auf ihn bezogenen Daten nicht vollständig, nicht aktuell, unrichtig sind oder unter Verletzung des Gesetzes erhoben wurden oder für das Erreichen des Zweckes für den sie erhoben wurden nicht mehr benötigt werden, ist der Datenverwalter verpflichtet, die Daten unverzüglich zu vervollständigen, zu aktualisieren oder zu berichtigen, die Verarbeitung der betreffenden Daten vorübergehend oder dauerhaft einzustellen oder sie aus der Sammlung zu löschen, es sei denn, dass personenbezogene Daten betroffen sind, deren Vervollständigung, Aktualisierung oder Berichtigung durch andere Gesetze geregelt wird.“ – hier wird der Schutz durch die Vorschriften des Kapitels 7 des Pressegesetzes, der das Recht auf die Berichtigung und Antwort betrifft, verstärkt.

Ein weiteres wichtiges Problem ist die Frage der Erfüllung der Informationspflichten die aus den Art. 25, 26 und 33 des Datenschutzgesetzes erfolgen durch die Journalisten. [36] Unserer Meinung nach gibt es Möglichkeiten für die Abweichungen, bei der Berufung auf die in diesem Gesetz enthaltenen zugelassenen Ausnahmen – jedoch bei der Annahme, dass die Datenverarbeitung durch die Medien aufgrund eines anderen Gesetztes erfolgt, das die Erhebung von personenbezogenen Daten ohne Wissen des Betroffenen vorsieht oder zulässt. *Interpretatio restrictiva* vom Abs. 2 des Art. 25 und 26 des Datenschutzgesetzes befehlt die Hinweisung auf eine bestimmte Vorschrift eines Gesetzes (was eigentlich der Fall sein soll), in bezug auf das Fehlen an Presseklauseln ist es aber unmöglich. Selbst in dem Pressegesetz könnte man sich theoretische auf Art. 11 in Verbindung mit Art. 4 berufen, aber der gegenständliche und subjektive Bereich dieser Bestimmungen bildet keine Begründung für die Verarbeitung personenbezogener Daten in den meisten Fällen derer tatsächlicher Nutzung. Deshalb ist dann die Anwendung der ausdehnenden Auslegung dieser Normen (bei gleichzeitiger Berufung der systematischen Auslegung) die einzige Lösung. Das ganze Presserecht stützt sich auf der Annahme der kontrollierenden Rolle der Medien in ihrem gesellschaftlichen Dienst. Das öffentliche Interesse erfordert sehr oft unkonventionelle Handlungen der Journalisten. Wenn sie dabei nicht direkt *contra legem* sind, dann bei dem Vergleich der geschützten Güter sind wir in der Regel bereit, den Journalisten die Freiheit der Informationsgewinnung zu gewähren. In manchen Situationen kann man sogar vermuten, dass die Gesellschaft mit dem Rechtsbruch einverstanden wäre, wenn

[36] Dies betrifft u.a. die Information über: seine Sitzanschrift, seinen vollen Namen und, wenn der Datenverwalter eine natürliche Person ist, seinen Wohnsitz und seinen Vor- und Nachnamen, 2) den Zweck der Datenerhebung und insbesondere die ihm in dem Moment der Datenerhebung bekannten oder vorgesehenen Empfänger der Daten und die Kategorien der Datenempfänger, 3) die Freiwilligkeit oder die Pflicht der Datenangabe und wenn eine solche Pflicht besteht, auch über derer Rechtsgrundlagen, 4) das Recht auf Einsicht in seine Daten und auf derer Berichtigung - die aktive Pflicht aus Art. 25 und 26 und die passive Pflicht aus Art. 33.1. Auf Antrag des Betroffenen ist der Datenverwalter verpflichtet, den Betroffenen über die ihm zustehenden Rechte mit einer Frist von 30 Tagen zu benachrichtigen und insbesondere in verständlicher Form hinsichtlich der ihn betreffenden Daten folgendes mitzuteilen: 1) welche personenbezogenen Daten in der Sammlung enthalten sind, 2) auf welche Weise die Daten erhoben wurden, 3) für welchen Zweck und in welchem Umfang sie verarbeitet werden, 4) in welchem Umfang und wem sie zugänglich gemacht wurden.

dieser zur Offenbarung von drastischen Fällen des Machtmissbrauchs, z.B. großen wirtschaftliche Affären, führen würde. Ohne aber so weit zu gehen, nehmen wir an, dass das Presserecht Grundlagen für die Feststellung, dass die Journalisten nicht immer verpflichtet sind, die Informationsgewinnung zu offenbaren, mehr noch, sie können auch, indem sie sich auf die Vorschriften über das Journalistengeheimnis berufen, die Offenlegung der Quellen einer bestimmten Information (und derer einzelnen Bestandteile, die die Identifizierung des Verfassers ermöglichen könnten) verweigern.

Schlimmer ist es im Falle der passiven Informationspflicht.[37] Das Datenschutzgesetz bildet eigentlich keine Möglichkeiten der Milderung der sich aus Art. 33 ergebenden Folgen (in der Antwort auf einen individuellen Antrag des Betroffenen). In Bezug darauf, das wir manchmal mit einer offenen Kollision der Vorschriften über die Einhaltung des Journalistengeheimnisses und des Art. 33 Abs. 1 Pkt. 2 (Information über die Art. der Datengewinnung) des Datenschutzgesetzes zu tun haben, kann man nur die Argumentation des vorigen Absatzes wiederholen und auf die schnelle juridische Lösung von ähnlichen Fällen, die dem Gesetzgeber die Richtung der Novellierung, die *de lege lata* stattfinden sollte, zeigen würde, hoffen.

Der Mühe wert ist noch eine kurze Analyse der rechtlichen Grundsätze der Ermittlungstätigkeit der Journalisten. Wir haben schon einige Arten der Informationsgewinnung erwähnt – was auch keine Kontroversen verursacht. Wir haben jedoch bis jetzt ein in Polen heftig diskutierte Problem nicht besprochen. Es geht um den Zugang der Journalisten zu den Daten, die in den Akten (der Gerichte oder der Staatsanwaltschaft) erfasst wurden. Die Aussagen des Generalinspektors, die darauf hingewiesen haben, dass diese Akten viele personenbezogene Daten enthalten und dass deren Zugänglichmachen für die Journalisten die Handlungen vorangehen sollen,

---

[37] Im Falle der sich aus Art. 32 Abs. 1 Pkt. 2 ergebenden Pflicht ist den Spannungszustand nicht so eindeutig – wir haben hier nur mit der Verpflichtung zur „... Informierung über den Zweck, den Umfang und die Art der Verarbeitung der in der Sammlung erfassten Daten," zu tun – die Offenbarung von bestimmten Daten, die zur Verletzung des Journalistengeheimnisses führen könnte, ist also nicht notwendig. Die übrigen die Tätigkeit der Presse „erschwerenden" Tätigkeiten Berechtigungen, die aus diesem Artikel erfolgen, können mittels der in dem Teil über Art. 25 und 26 des Datenschutzgesetztes angebrachten Argumenten „gemildert" werden.

die die Möglichkeit der Bekanntmachung mit diesen Daten eliminieren (was die Erfordernisse des Datenschutzgesetzes erfüllt) stießen auf sehr unterschiedliche Reaktionen. Einige Richter betrachteten sie als einen Vorwand (in bezug auf das Fehlen der praktischen Möglichkeit solcher Änderungen – die nur auf dem Ausschluss einiger Unterlagen aus den alle Informationen über das Verfahren enthaltenden Daten Bändern) für das völlige Zugangsverbot der Journalisten zu solchen Akten. Die Journalisten reagierten mit einer Attacke auf den Generalinspektor und die Justiz, dabei beriefen sie sich auf die verfassungsrechtlich bestätigte Presse- und Aussagefreiheit und das Recht auf den Zugang zu Informationen.

Zu überlegen ist also ob sich die Ansichten der beiden Parteien in der geltenden Rechtslage in Einklang bringen lassen. Am Anfang schon soll es bemerkt werden, daß die Gerichtsakte eines bestimmten Verfahrens nicht allen Vorschriften des Datenschutzgesetzes unterliegen müßten – im Sinne dieses Gesetztes sind Gerichtsakte keine Datensammlungen – die Tatsache, daß sie immer einen Bestandteil einer größeren Sammlung (der Sammlung aller Akten der durch das bestimmte Gericht entscheidenden Sachen oder durch eine bestimmte Staatsanwaltschaft geführten Ermittlungen) bilden, verursacht, dass sie unbedingt als Informationssammlungen, die u.a. auch personenbezogene Daten enthalten, betrachtet werden müssen. Die Datenverwalter sollten also die Vorschriften des Datenschutzgesetzes anwenden, es sei „... die Vorschriften anderer Gesetze, die die Datenverarbeitung betreffen einen weitergehenden Schutz vorsehen als sich aus dem Datenschutzgesetz ergibt, sind die Vorschriften dieser Gesetze anzuwenden...“ (Art. 5 des Datenschutzgesetzes). Gibt es solche besonderen Vorschriften, die einen weitergehenden Schutz der personenbezogenen Daten gewährleisten? – Eher nicht. Die Bestimmungen sind nicht ausreichend, nur in zwei Absätzen des Art. 156 des Strafgesetzbuches wird die Möglichkeit derer Zugänglichmachen erwähnt (in den Ausnahmefällen im Ermittlungsverfahren – es gibt aber keine Beispiele dafür), in dem Strafverfahrensgesetzbuch fehlt es auch an solchem Hinweis (die Rechtslehre vertritt aber die Ansicht, dass mit der Zustimmung der Verfahrensparteien solche Handlungen zugelassen sind), das Presserecht stellt folgendes fest:

„...1. die Presse darf keine Ansichten über die Entscheidung in dem Gerichtsverfahren vor der Urteilsfällung in der ersten Instanz äußern.
2. Die Presse darf keine personenbezogenen Daten oder Bilder von Personen gegen die eine Ermittlung oder ein Gerichtsverfahren geführt wird sowie keine personenbezogenen Daten und Bilder von Zeugen, Beschädigten und Verletzten veröffentlichen, es sei, die Betroffenen stimmten es zu.
3. Die Einschränkung vom Abs. 2 verletzt keine Vorschriften anderer Gesetze. Der zuständige Staatsanwalt oder das zuständige Gericht kann, wegen eines wichtigen gesellschaftlichen Interesses die Offenbarung der personenbezogenen Daten und Bilder von Personen gegen die eine Ermittlung oder ein Gerichtsverfahren geführt wird, genehmigen." (Art. 13 des Pressegesetzes). Alle diesen Normen gewährleisten keine weitergehende Garantie, man kann aber mit der Rechtslehre[38] einverstanden sein und annehmen, dass die Vorschriften anderer Gesetze auch Abweichungen von den Bestimmungen des Datenschutzgesetzes einführen können, die den Zugang zur Information erleichtern (bei der Einhaltung von demselben oder niedrigerem Niveaus derer Schutzes). Dies wurde in dem neuen Gesetz über den Zugang zu den öffentlichen Informationen bestätigt, wo eindeutig der Zugang zu Informationen über die Personen, die öffentliche Ämter bekleiden ausgedehnt wird. In Bezug auf die Gerichtsgewalt verschärfte diese Akte die Unklarheiten. Wenn in dem Gesetz über öffentliche Information vorbehalten wird, dass es keine mit verschiedenen Geheimnissen verbundenen Normen nicht verletzt und das Datenschutzgesetz sieht besondere Bedingungen für die Verarbeitung von „pönalen" Daten vor (behält eine solche Möglichkeit ausschließlich für die Rechtsträger die aufgrund besonderer Vorschriften handeln), wie kann das Zugänglichmachen von Akten anderen Rechtsträger, worüber die Vorschriften des Verwaltungsgesetzbuches bestimmen, anders ausgelegt werden als eine Ausnahme von dem Grundsatz des Nichtzugänglichmachens dieser Akte an andere Personen als die rechtlich Interessierten. Man tut es doch nicht um bestimmte personenbezogene Informationen zu offenbaren (in bezug auf das Pressegesetz soll das zu keiner Offenbarung von diesen Daten führen – und selbst die

[38] vergleiche z.B. die Meinung von J. Barta und R. Markiewicz in „Ochrona danych ososbowych – komentarz, *Schutz von personenbezogenen Daten – Kommentar*, Zakamycze 2001, S. 175 - 188

Neugier des Journalisten bildet keine Grundlage für derer Zugänglichmachen) – diese Funktion erfüllen Steckbriefe[39] oder die öffentliche Bekanntgabe des Urteils - aber um die Gesellschaft über bestimmte Mechanismen zu informieren. Zu derer Beschreibung sind die echten Daten der Täter, Opfer oder zeugen nicht nötig – davon zeugen die Tatbeschreibungen mit geänderten Realien (andere Ortschaften, andere Personen), die zwar bei den Lesern nicht so beliebt sind, aber viel besser die Privatsphäre der Teilnehmen schützen. Es entsteht also die Frage, ob Journalisten die Personen sind, deren das Recht die Einsicht in alle Gerichtsakten gewährleistet?

Die Vorschriften über den Zeuge inkognito oder über nichtöffentliche Gerichtsverhandlungen weisen darauf hin, daß man auf diese Frage mit einem „nein“ antworten soll. Das Zugänglichmachen von Akten einem Journalisten kann nur in dem mit sog. äußerer Öffentlichkeit umfassten Bereich erfolgen (betrifft also das Material, das Gegenstand einer öffentlichen Gerichtsverhandlung war oder sein konnte). Geschützt werden auch Unterlagen, die das ärztliche Berufsgeheimnis offenbaren könnten – ausgeschlossen werden die Schlussfolgerungen der Gutachter, die ihre Meinung über die Zurechnungsfähigkeit des Täters im Moment der Begehung der Straftat oder über die Art, den Charakter und Dauer von Verletzungen der Verletzten äußern. Die letzten Informationen gehören ohne Zweifel zu der Kategorie der sensitiven Daten – und wenn man berücksichtigt, dass diese Unterlagen den Akten beigelegt werden und zusammen eine untrennbare Ganzheit bilden, werden unsere Zweifel, die mit der Offenbarung von solchen Informationen verbunden sind noch größer. Indem wir solche Akten den Journalisten zugänglich machen, sind wir zugleich damit einverstanden, dass sie sich auch mit diesen Daten bekannt machen und es ist doch schwer einen Medienvertreter als einen berechtigten Depositar des ärztlichen Berufsgeheimnisses zu betrachten. Ist also das Zugänglichmachen dieser Unterlagen ohne vorheriges Vornehmen von Änderungen, die die Identifizierung der Teilnehmer unmöglich machen, begrün-

[39] Von der Zusammenarbeit der Journalisten mit der Polizei oder der Staatsanwaltschaft zeugen zahlreiche Fernsehprogramme (von einem „Ermittlungscharakter” in denen Tatablauf rekonstruiert wird, Gedächtnisbilder der vermutlichen Täter gezeigt werden oder Daten von den gesuchten Personen veröffentlicht werden) – dabei werden nur diese Daten dargestellt, derer Offenbarung in Bezug auf das gesellschaftliche Interesse notwendig ist.

det? Unserer Meinung nach, ist das in der gegenwärtigen rechtlichen Situation nicht begründet.

Wie sollen also Medien über die Gerichtsverhandlungen berichten? Es gibt mehrere Möglichkeiten.[40] Sie können sich an die Leiter der in Art. 4 des Pressegesetzes erwähnten Einheiten, derer Vertreter, Pressesprecher und andere zur Erteilung von Informationen berechtigte Personen wenden. Die Gerichtspräsidenten, Gerichtssprecher und die einzelnen Richter (dasselbe gilt auch für die Staatsanwaltschaft) sind verpflichtet über die Gerichtsverhandlungen aufzuklären (die Rechte der Journalisten umfassen auch die Möglichkeit der Kontakte mit anderen Mitarbeitern dieser Institutionen, die können aber das Gespräch – ausschließlich aus eigenem Willen – verweigern). Eine andere Möglichkeit gibt die Öffentlichkeit der Gerichtsverhandlung - während der Verhandlung kann man Notizen machen und sogar mit der Zustimmung des Gerichtes und gemäß den durch das Gericht festgelegten Bedingungen (oder im Falle, wenn dies nicht verboten wurde – und wenn die Richter davon wissen) Aufnahmegeräte gebrauchen (darunter auch das Fixieren von Bildern). Man kann auch versuchen Informationen von den Teilnehmern der Verhandlung – Zeugen, Verfahrensparteien – Informationen zu gewinnen – und wenn sie damit einverstanden sind, auch ihre personenbezogenen Daten veröffentlichen.

Die Medien sind also auch in der geltenden Rechtsordnung nicht ratlos und die Tatsache, dass sie oft die geltenden Normen verletzten (zu nennen ist hier die Offenbarung von personenbezogenen Daten von bekannten Personen, gegen die ein Verfahren geführt wird oder Überreden zum Verraten der Berufsgeheimnisse[41]) verur-

---

[40] Diesem Thema ist das Werk von J. Sobczak „Dziennikarz – sprawozdawca sądowy. Prawa i obowiązki, *Journalist – Gerichtsberichtserstatter. Rechte und Pflichten*, Warszawa 2000 gewidmet, auf ca. 200 Seiten werden genau alle möglichen Situationen, die mit dem Berichten über Gerichtsverfahren verbunden sind, analysiert.

[41] Die Offenbarung von solchen Daten erfolgt in einer „verkappten" Form, z.B. „... General J., der ehemalige Staatspräsident der Republik Polen" usw. aber es bestehen keine Zweifel, um wen es sich handelt. Die Journalisten stellen oft Fragen, obwohl sie es genau wissen, dass die eventuelle Antwort die Grundsätze eines der rechtlich geschützten Geheimnissen, z.B. aufgrund Art. 4 Abs. 2 des Pressegesetzes, der die Möglichkeit der Antwortverweigerung in diesem Bereich gewährleistet, verletzen wird. Dies erfolgt in unterschiedlichen Formen, z.B. das Befragen der Schöffen nach ihrer Stellungnahme während der Beratung oder das Befragen

sacht sicher keine Milderung des Widerwillens der Gerichts- und Strafverfolgungsorgane gegen Journalisten und gibt keine Anregung zur Erteilung von Informationen.

In der Zusammenfassung stellen wir fest, dass das Grundproblem des polnischen Rechtssystems das Fehlen an eindeutigen und klaren Normen, die die Bestimmungen des Datenschutzgesetzes in Bezug auf die Medientätigkeit mildern, ist. Diese Situation soll zweifelsohne geändert werden. Es gibt Gründe um festzustellen, dass die Verarbeitung von personenbezogenen Daten in dem für das Funktionieren der Presse notwendigen Bereich mit dem Recht übereinstimmt. Dies befreit aber die Medien nicht von den Pflichten, die auf die Datenverwalter auferlegt wurden. Alle eventuell akzeptablen Abweichungen von den aus dem Datenschutzgesetz erfolgenden Grundsätzen sind nur dann zugelassen, wenn es auf keine andere rechtlich zugelassenen Weise möglich ist, ohne sie die Zwecke, die die Presse in einer demokratischen Gesellschaft zu erfüllen hat zu erreichen und wenn in einem bestimmten Fall diese Zwecke klar auf die Notwendigkeit der Einschränkung der Menschenrechte hinweisen.

---

der Priester ob der Verdächtige die Tat während der Beichte gestanden hat. – mehr zu diesem Thema siehe J. Sobczak, Dziennikarz... (op. cit), *Journalist ... (op. cit.),* S. 70 – 71, 171 – 186 und andere.

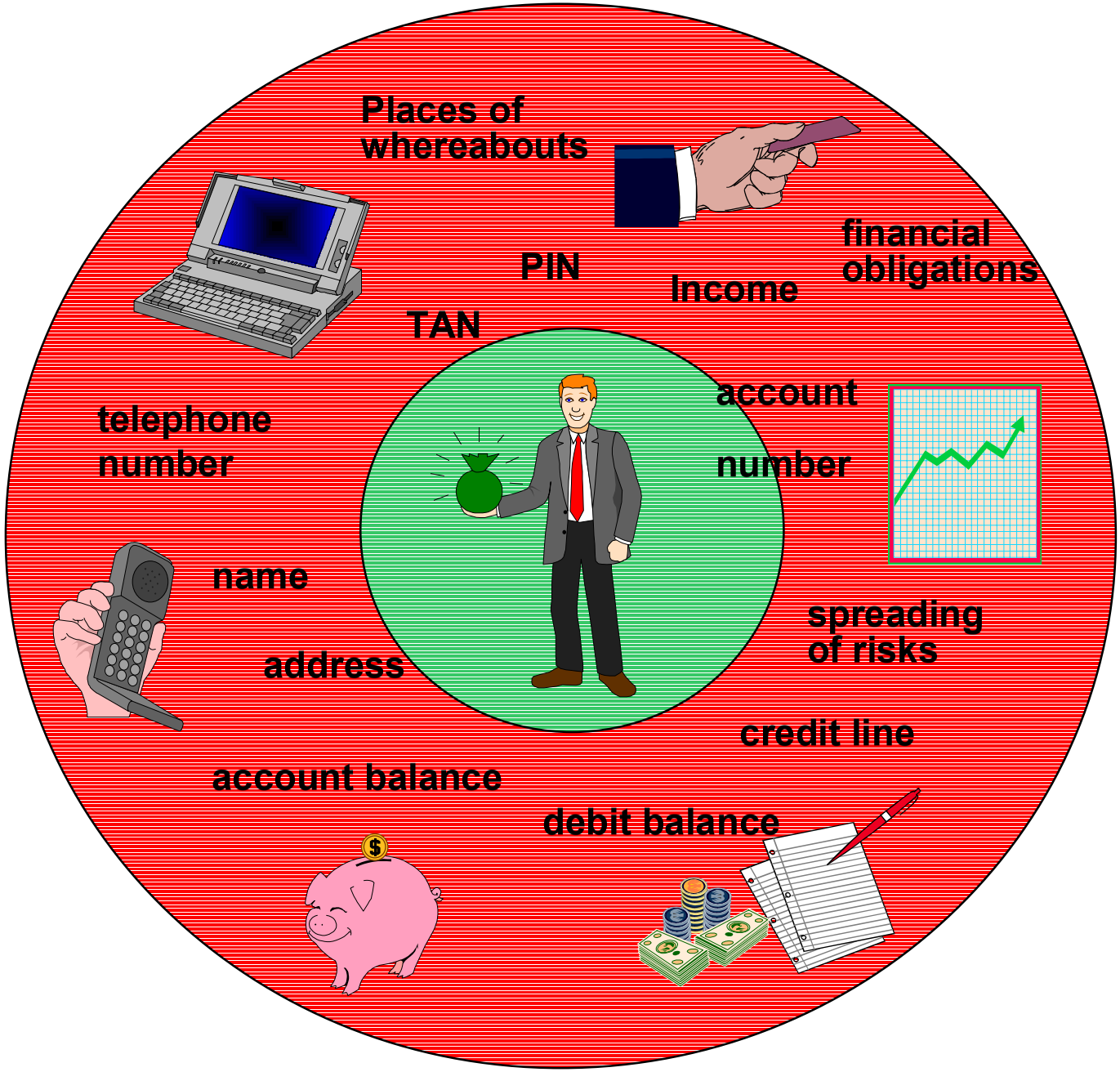
DAIMLERCHRYSLER

Financial Privacy and Data Protection in the enlarged European Union

Prof. Dr. Alfred Büllesbach, Chief Corporate Data Protection Officer

DAIMLERCHRYSLER

customer data



Prof. Dr. Alfred Büllesbach
October 2001

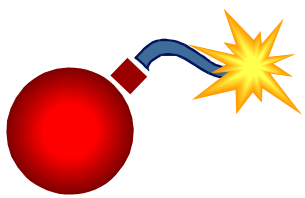
DAIMLERCHRYSLER

Risks and Dangers

- Creation of User profiles
- Manipulation of transferred or stored data
- Unauthorised knowledge of data
- Misuse of data for purposes they were not collected for
- Unauthorised use of data
- Deletion of data by unauthorised persons

➔ **Objective of Data Protection:**

Protection of the personal rights of those whose data is being processed



Prof. Dr. Alfred Büllesbach
October 2001

DAIMLERCHRYSLER

Basic Principles of Data Protection in Europe I

- ➔ Data Avoidance and Economy
- ➔ Legal authorisation or customer consent
- ➔ Data integrity and accuracy
- ➔ Compliance with the purpose
- ➔ Restrictions on data transfer to foreign countries
- ➔ Binding employees to data secrecy and limitation/control of access to personal customer data
- ➔ Assuring technical data security

Prof. Dr. Alfred Büllesbach
October 2001

DAIMLERCHRYSLER

Basic Principles of Data Protection in Europe II

Prof. Dr. Alfred Büllesbach
October 2001

➔ Rights to individuals:

- notice
- access
- correction an deletion
- objection against data use for marketing purposes
- right not to be subject to an automated individual decision

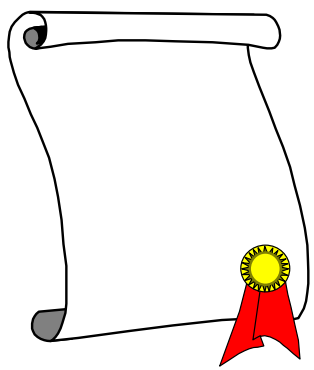
➔ *Only in Germany*:

- According to Section 6c of the BDSG, mobile storage media (chip cards) must be submitted to prior data-protection checks by the corporate data-protection officer.
- Section 6b of the BDSG restricts the optical supervision of rooms open to the public. The concerned individual must be informed about the supervision and where he can address to claim his rights.

DAIMLERCHRYSLER

International data-protection regulations in Europe:

Conventions and Charters



- Article 8 of the Convention of the Council of Europe for the Protection of Human Rights and Fundamental Freedoms:

  "Everyone has the right to respect for his private and family life, his home and his correspondence."

- Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of personal Data

- Article 8 Section 1 of the Charter of Fundamental Rights of the European Union:

  "Everyone has the right to the protection of personal data concerning him or her."

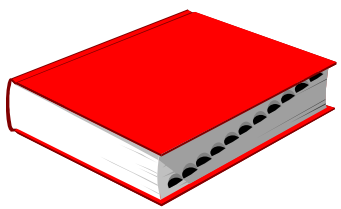
➡ The right to data protection is a human right in Europe

Prof. Dr. Alfred Büllesbach
October 2001

DAIMLERCHRYSLER

International data-protection regulations in Europe:

Directives I



Prof. Dr. Alfred Büllesbach
October 2001

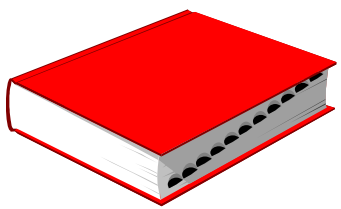
- 1991: Council Directive on money laundering
- 1995: Data Protection Directive
  - implementation still not successful in France, Luxembourg, Ireland
  - will create a standardised legal data protection in the member states, allow data transfer within the EU domestic market and facilitate the cross-border flow of financial data within the EU
- 1997: Telecommunication Data Protection Directive

  Article 12:
  - The use of automated calling systems or fax for the purposes of direct marketing are only allowed if addressees have given their prior consent.
  - Member States take appropriate measures by national legislation.
  - Right to choice applies to subscribers who are natural persons.
  - Member States shall also guarantee that the legitimate interests of subscribers other than natural persons with regard to unsolicited calls are sufficiently protected.

DAIMLERCHRYSLER

International data-protection regulations in Europe:

Directives II



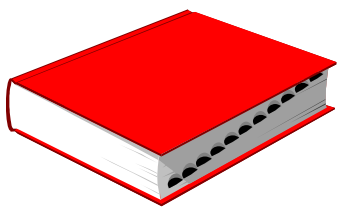
Prof. Dr. Alfred Büllesbach
October 2001

- 1999: Directive about Electronic Signatures
  - ➔ objective: facilitating the use of electronic signatures and contributing to their legal recognition
  - ➔ distinction between “electronic” and “advanced electronic” signatures
  - ➔ creates the conditions that ensure safe use of digital signatures in legal and business transactions
  - ➔ opportunities have been little used
- 2000: E-Commerce Directive
  - ➔ objective: ensuring the free movement of information society services between the Member States
  - ➔ approximates national provisions on information society services relating to the internal market, the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlements, court actions

DAIMLERCHRYSLER

International data-protection regulations in Europe:

Proposal of the EU-Commission



Prof. Dr. Alfred Büllesbach
October 2001

- 1999: Amended proposal for a Directive concerning the distance marketing of consumer financial services
  - ➔ objective: access without discrimination to the widest possible range of financial services available in the Community, so that the consumer can choose the best suited to their needs
  - ➔ guarantees high level of consumer protection ensuring the free movement of financial services in order to enhance consumer confidence in distance selling
  - ➔ „financial service“ means any banking, insurance, investment or payment service
  - ➔ Covers all financial services liable to be provided at a distance
  - ➔ „distance contracts“: offer, negotiation and conclusion are carried out at a distance
  - ➔ Member States may not adopt provisions other than those laid down in this Directive

Problems:

- Disparities in legal provisions concerning contracts and financial services, especially stock brokerage
- Applicability of national law on new providers during the implementation period

DAIMLERCHRYSLER

Data-protection and bank secrecy

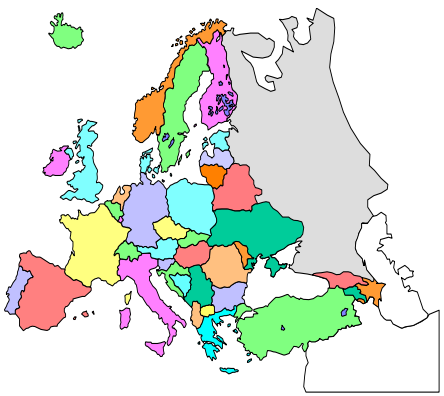
- Bank secrecy is a product of the contractual relationship between bank and customer, data protection is imposed by act of law
- Unlike bank secrecy, the German BDSG only protects natural persons
- Bank secrecy is relevant only in connection to third parties, data protection also regulates the collection, storage, changing or use of data by the bank
- Before a bank discloses customer data to third parties, it must observe both sets of legal obligations, if its customers are natural persons

➡ data protection and bank secrecy represent two separate regulations that do not oppose one another

Prof. Dr. Alfred Büllesbach
October 2001

DAIMLERCHRYSLER

National data protection regulations I



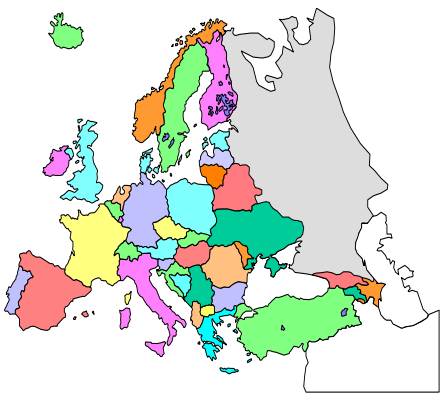
Prof. Dr. Alfred Büllesbach
October 2001

Right of the concerned individual to

	Notice	Access	Correction/ Deletion
Belgium	x	x	x
Denmark	x	x	x
Germany	x	x	x
Finland	x	x	x
France	-	x	x
Greece	x	x	x
Great Britain	x	x	x
Ireland	x	x	x
Italy	x	x	x
Luxembourg	x	x	x
The Netherlands	x	x	x
Austria	x	x	x
Portugal	x	x	x
Sweden	x	x	x
Switzerland	-	x	x
Spain	x	x	x

DAIMLERCHRYSLER

National data protection regulations I

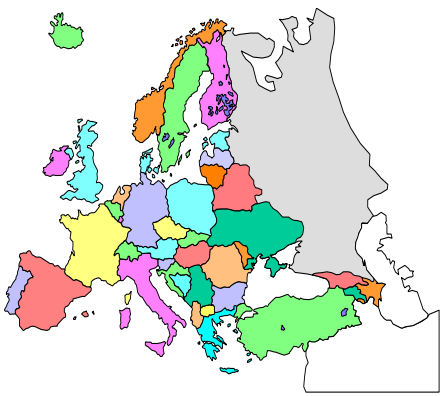


Prof. Dr. Alfred Büllesbach
October 2001

	Right of the concerned individual to Notice	Access	Correction/ Deletion
Bulgaria	(*Draft*)		
Cyprus	(*Draft*)		
Czech Rep.	x	x	x
Estonia	if consent necessary	x	x
Hungary	x	x	x
Latvia	x	x	x
Lithuania	x	x	x
Malta	(*Draft*)		
Poland	x	x	x
Romania	(*Draft*)		
Russia	x	x	x
Slovak Rep.	x	x	x
Slovenia	if consent necessary	x	x
Turkey	(*Draft*)		

DAIMLERCHRYSLER

National data protection regulations II

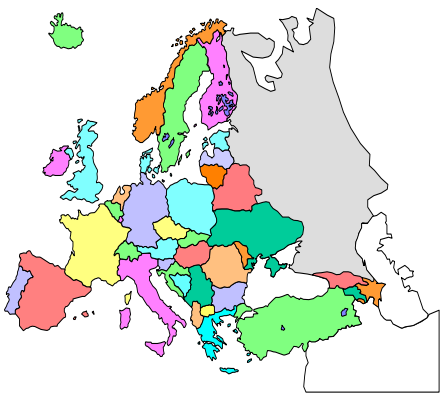


Prof. Dr. Alfred Büllesbach
October 2001

	Right of the concerned individual to		
	Choice	**Onward**	
Enforcement	(opt-out)	**Transfer**	
Belgium	x	x	x
Denmark	x	x	x
Germany	x	x	x
Finland	x	x	x
France	x	-	x
Greece	x	x	x
Great Britain	x	x	x
Ireland	x	-	x
Italy	x	x	x
Luxembourg	x	-	x
The Netherlands	x	x	x
Austria	x	x	x
Portugal	x	x	x
Sweden	x	x	x
Switzerland	x	-	x
Spain	x	x	x

DAIMLERCHRYSLER

National data protection regulations II

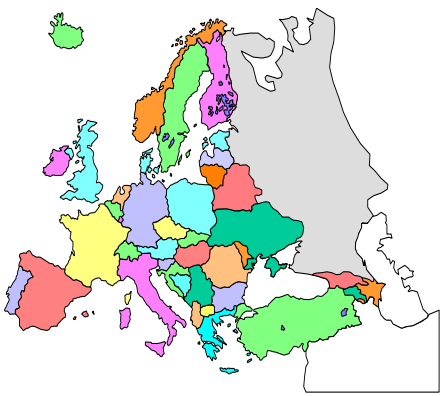


	Right of the concerned individual to		
	Choice	**Onward**	
Enforcement	(opt-out)	**Transfer**	
Bulgaria	(*Draft*)		
Cyprus	(*Draft*)		
Czech Rep.	x	x	x
Estonia	x	-	x
Hungary	x	x	x
Latvia	x	x	x
Lithuania	x	x	x
Malta	(*Draft*)		
Poland	x	x	x
Romania	(*Draft*)		
Russia	x	-	x
Slovak Rep.	x	x	x
Slovenia	x	-	x
Turkey	(*Draft*)		

Prof. Dr. Alfred Büllesbach
October 2001

DAIMLERCHRYSLER

National data protection regulations III

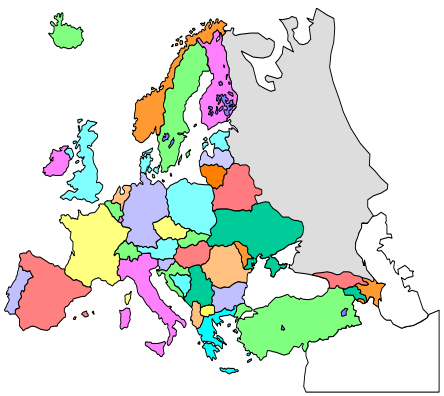


Prof. Dr. Alfred Büllesbach
October 2001

	Protection automated decisions	Restrictions concerning	Obligation to notify	Corporate Data Officer
Belgium	x	x		possible
Denmark	x	x		-
Germany	x	x		x
Finland	x	x		-
France	x	not generally		-
Greece	x	x		-
Great Britain	x	x		-
Ireland	-	x		-
Italy	x	x		-
Luxembourg	-	x		-
The Netherlands	x	x		x
Austria	x	x		-
Portugal	x	x		-
Sweden	x	x		x
Switzerland	-	x		-
Spain	x	x		-

DAIMLERCHRYSLER

National data protection regulations III



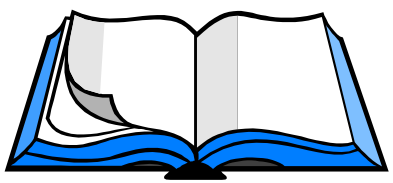
Prof. Dr. Alfred Büllesbach
October 2001

Protection	Restrictions concerning automated decisions	Obligation to notify	Corporate Data Officer
Bulgaria	(*Draft*)		
Cyprus	(*Draft*)		
Czech Rep.	-	x	-
Estonia	-	processing of sensitive data	-
Hungary	-	x	-
Latvia	-	x	-
Lithuania	-	x	-
Malta	(*Draft*)		
Poland	-	x	-
Romania	(*Draft*)		
Russia	-	x	-
Slovak Rep.	x	x	-
Slovenia	-	x	-
Turkey	(*Draft*)		

DAIMLERCHRYSLER

Applicability of the BDSG to Financial-Service Providers

- ➔ Financial-service providers under private law: general provisions of the BDSG, as well as specific regulations for the private sector apply (Sections 27-38a)
- ➔ Federal credit institutions under public law in free competition: Sections 27-38a apply as well
- ➔ The BDSG does not recognise any so-called corporate privileges: associated corporations in a corporate group are considered third parties in relation to one another

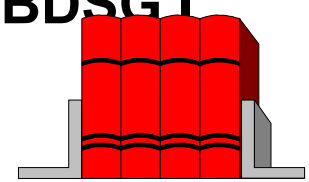


Prof. Dr. Alfred Büllesbach
October 2001

DAIMLERCHRYSLER

Collecting, processing and use of personal data by financial-service providers:

Relevant legal regulations outside the BDSG I

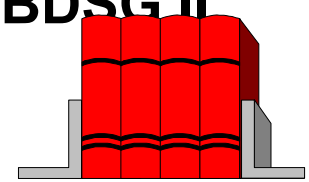


- ➔ Data collected according to Section 31 of the Securities Trading Act about the financial situation of the client may be stored according to Section 34
- ➔ According to Sections 2 and 9 of the Money Laundering Act in connection with Section 154 of the Fiscal Code, financial institutions must store the acquired data of depositors of cash amounts over 30.000 DM
- ➔ General accounting or recording obligations (Section 257 of the Commercial Code, Section 319 of the Fiscal Code) can legitimise data-processing activities according to commercial and fiscal regulations
- ➔ Sections 915 ff. of the Code of Civil Procedure and the List of Insolvent Debtors Code contain special data-protection regulations for the accessing of data in the debtors' index and their use in credit industry

DAIMLERCHRYSLER

Collecting, processing, and use of personal data by financial-service providers:

Relevant legal regulations outside the BDSG II

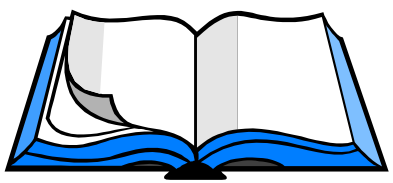


- According to Sections 13 and 14 of the Act Regulating Banking and Credit Business specific loans are to be disclosed
- In the case of the decease of a bank customer, transmission obligations of the bank are applicable to the revenue authority according to the Inheritance Tax Law
- Credit institutions have information obligations for the control of investment-income-tax payment and have to respect official inspection rights in other taxation procedures, public-investigation procedures and criminal proceedings
- Employment offices have information rights before they agree to pay unemployment benefits (Section 315 of the Social Security Code Vol. III)
- Finally, an institution that acts as an employer has information-collecting obligations towards Social Security carriers

DAIMLERCHRYSLER

Collecting, processing, and use of personal data by financial-service providers:

Legal basis in the BDSG

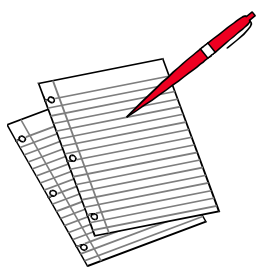


- ➔ Section 28 of the BDSG concerns data processing for an entity's own corporate purpose
- ➔ Data processing offered as a service, such as credit-information systems or directory distributors, is regulated by Section 29
- ➔ Data processing on behalf of others is regulated in Section 11 of the BDSG and Section 25a of the Act Regulating Banking and Credit Business

DAIMLERCHRYSLER

Collecting, processing, and use of personal data by financial-service providers:

Section 28 of the BDSG



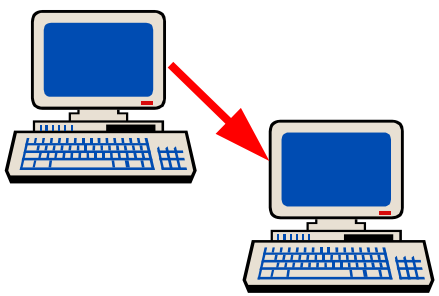
- ➔ Data processing to **fulfil a contract** with a client is permitted according to Section 28 of the BDSG
- ➔ **Pre-contractual relationships** are equivalent to contract
- ➔ Producing user profiles is included by **credit-card contracts** only for the purpose to minimise the risk for the customer and not for advertising
- ➔ Data processing and use **without contract** or exceeding the contract is allowed if it is required to preserve the justified interests (even advertising, marketing in coherence with the contract) of the financial institution and protection-worthy interests of the concerned individual do not predominate
- ➔ According to Section 6a of the BDSG **Credit Scoring** and "**Automated individual Decisions**" may not cause infringement to the concerned individual

Prof. Dr. Alfred Büllesbach
October 2001

DAIMLERCHRYSLER

Data exchange with credit-protection systems:

Section 29 of the BDSG

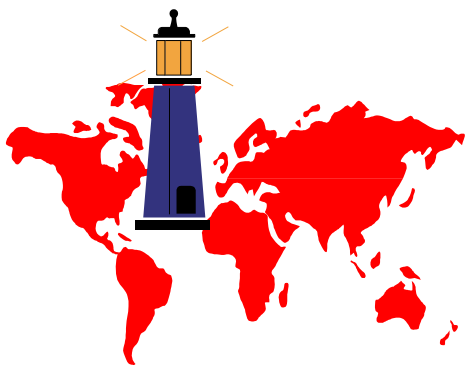


- ➔ The customer releases the credit agency from the bank secrecy in the contract, e.g. by signing the German SCHUFA clause
- ➔ The transfer of data from the database of the credit protection system is based on the justified interest of associated corporations, e.g. Sections 29 Paragraph 2 of the BDSG for the SCHUFA organisations in Germany
- ➔ The credit protection system is obligated to document all retrievals from their database

Prof. Dr. Alfred Büllesbach
October 2001

DAIMLERCHRYSLER

Cross-border data and payment transactions



- According to Art. 25 I of the Data protection Directive, data transfer is permitted by law if an adequate level of protection is ensured
- If the third country does not ensure an adequate level of protection, the transfer is exceptionally permitted according to Art. 26 I
  - if the data subject has given his consent
  - if the data transfer is part of a contract
  - if the transfer is necessary in the interest of the data subject
  - if the transfer is made from a register according to a law
- If none of these exceptions applies, **Contract Clauses** or **Codes of Conduct** may guarantee an adequate level of protection
- The **safe harbor principles** can guarantee an equivalent standard for data transfers between the EU and USA, but are not applicable on financial services

Prof. Dr. Alfred Büllesbach
October 2001

DAIMLERCHRYSLER

Data-protection obligations for financial services offered by teleservice providers

- To facilitate anonymous use and use based on a pseudonym if economically reasonable
- To secure data protection using information technology
- Not to create user profiles related to individuals
- To observe regulation with regard to the use of contract, connecting, and billing data
- To provide a right of access that can be electronically requested and granted

➡ long-term acceptance for electronic commerce

Prof. Dr. Alfred Büllesbach
October 2001

DAIMLERCHRYSLER

Data protection law in Europe is becoming more and more homogenious

Prof. Dr. Alfred Büllesbach
October 2001

multi > channel > chances

Banking im Internet

Nicht nur eine Frage der Sicherheit

Frank Axel

Ostdeutscher Sparkassen- und Giroverband

Abteilungsleiter Markt

Struktur der Online-Nutzer

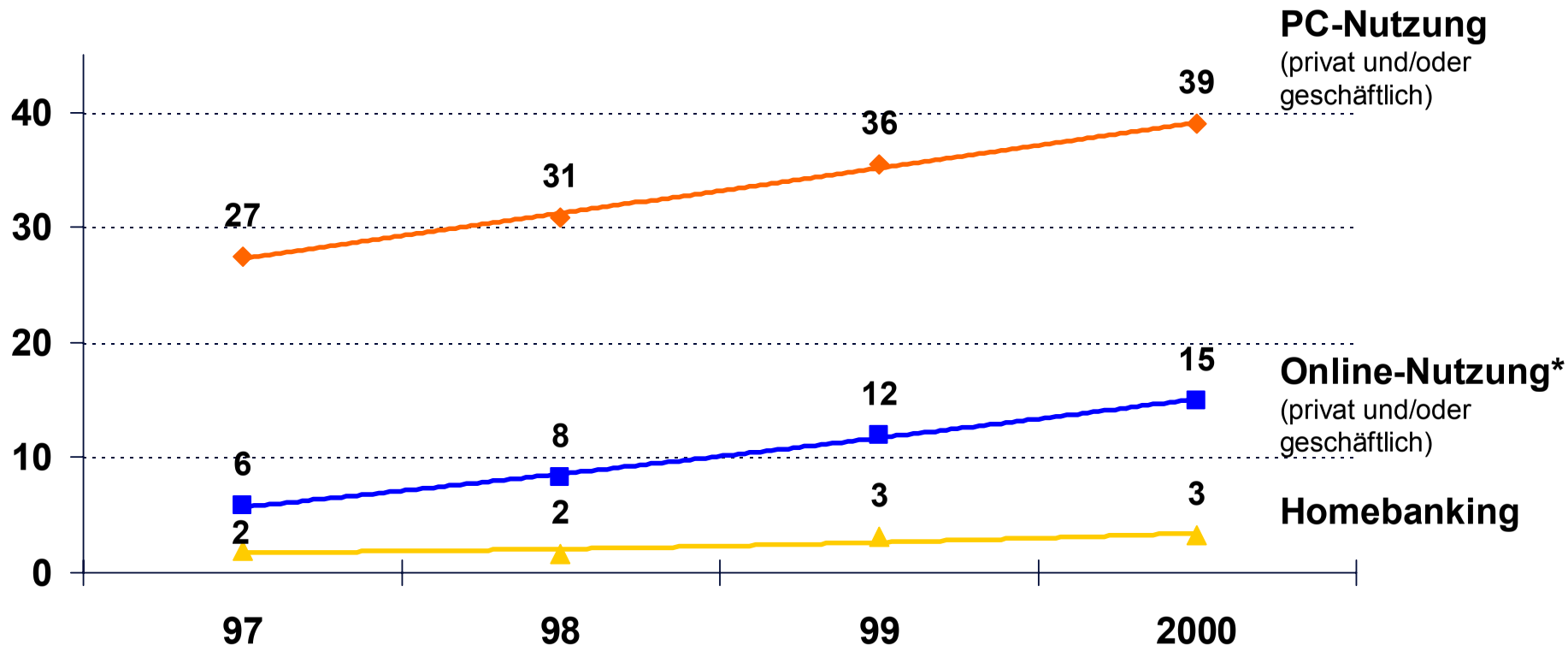
	Bevölkerung	Onliner	Index (Gesamtbevölkerung = 100)
Geschlecht			
Männer	50%	58%	117
Frauen	50%	42%	83
Altersgruppen			
14-29 Jahre	24%	36%	151
30-39 Jahre	22%	25%	116
40-49 Jahre	19%	21%	108
50 Jahre u. älter	35%	18%	52
Schulbildung			
Volks-/Hauptschule	44%	30%	67
Weiterf. Schule o. Abi	35%	39%	111
Abitur, Studium	21%	32%	150

Basis: Bevölkerung 14-69 Jahre
Quelle: GfK Online-Monitor, 7. Welle

Online-Nutzung im OSGV

Nicht-Nutzung von Homebanking

- fehlender Bedarf
- fehlendes Vertrauen in die Sicherheit der Online-Abwicklung von Bankgeschäften
- lieber auf "High Touch" (menschlicher, persönlicher Kontakt) setzen als auf "High Tech“.

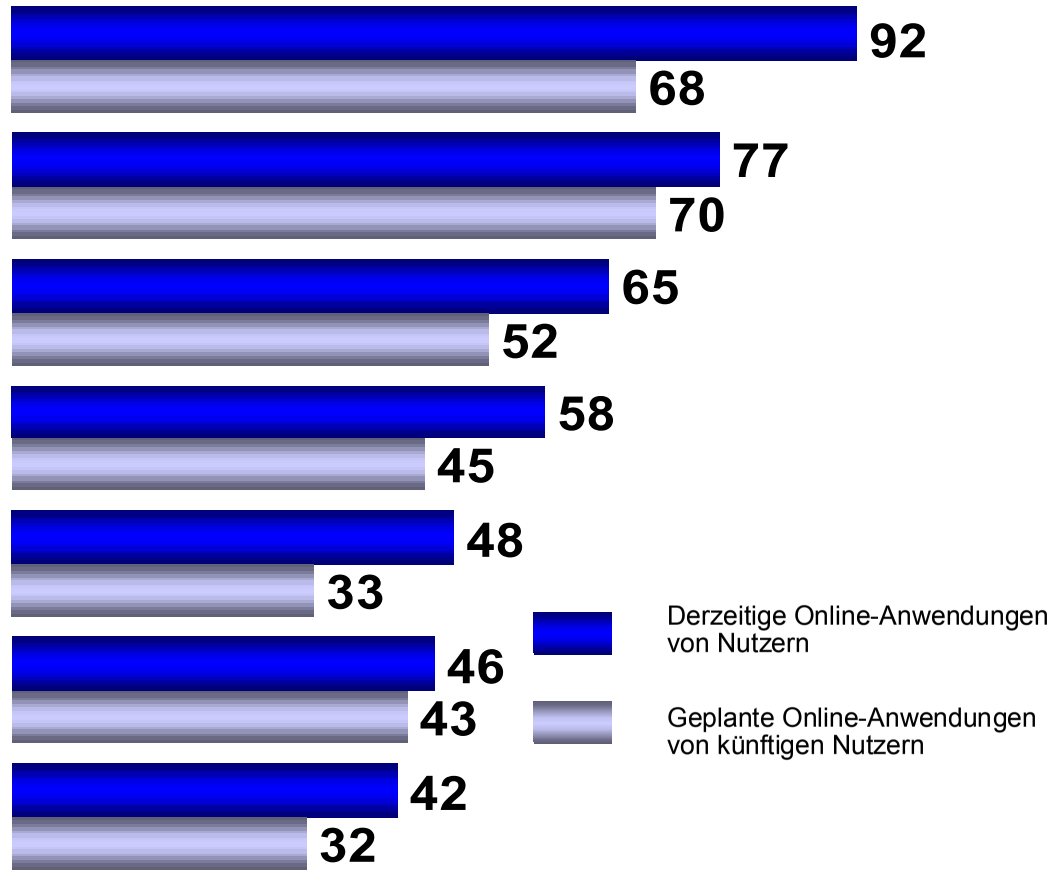


Basis: Befragte des OSGV-Geschäftsgebiets

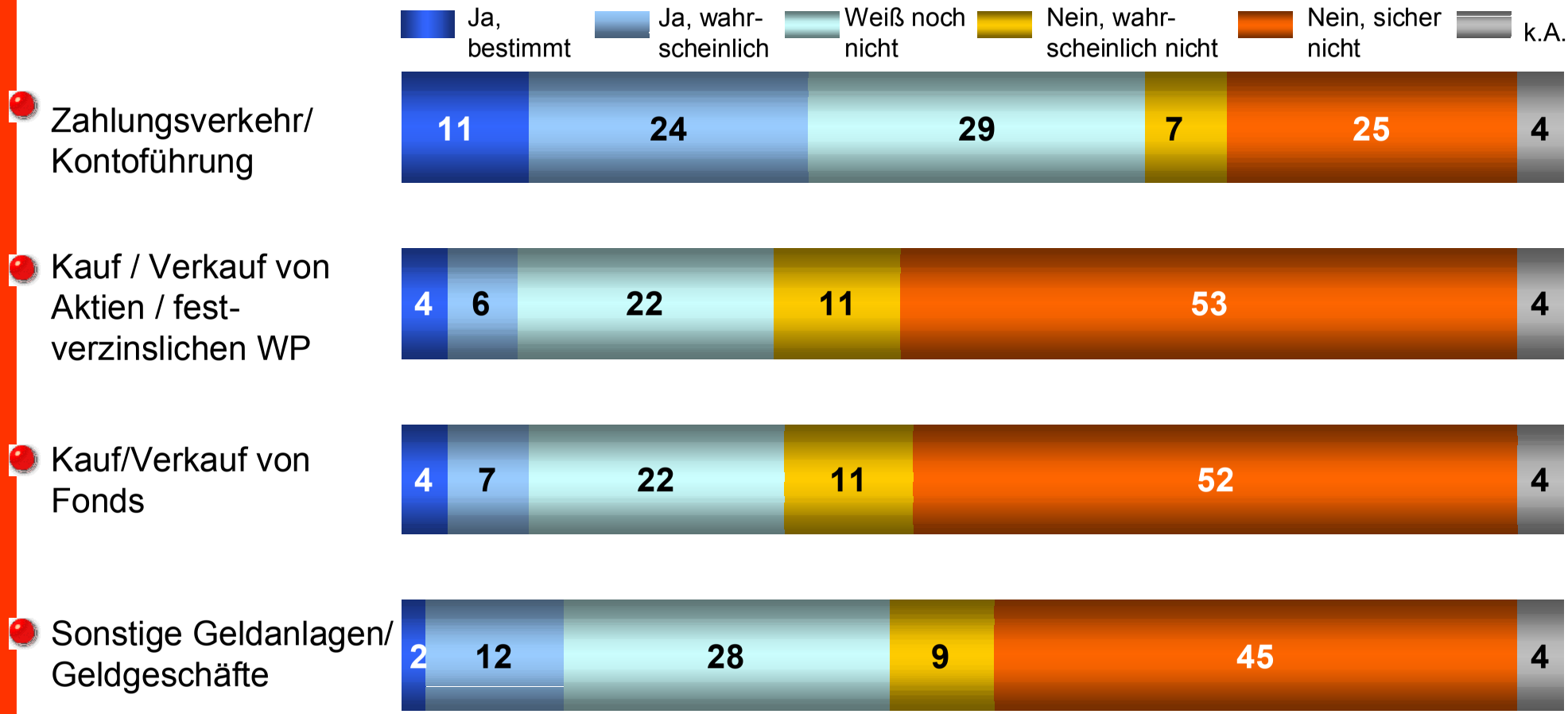
Alle Angaben in %

Was macht der Internetnutzer heute ?

- E-Mail-Versand privater Nachrichten
- Auskünfte einholen über Reisen, Fahrpläne, Veranstaltungen
- Unterhaltung, Spaß und Spiel
- Informationssuche, z.B. Lesen von Zeitungen und Zeitschriften online
- Online-Shopping
- Abfrage aktueller Konditionen von Banken
- Abfrage aktueller Wirtschaftsdaten, z.B. Börsenkurse



Welche Banktransaktionen werden genutzt?



Basis: 158 Befragte des OSGV-Geschäftsgebiets, die bisher kein Homebanking nutzen bzw. sich privat einen Online-Anschluss anschaffen wollen

Alle Angaben in %

Entwicklung Kundensicherungsmitteln der Sparkassenorganisation

➡beleghafter Zahlungsverkehr mit manueller Unterschrift	→...
➡Datenträger mit Begleitzettel und manueller Unterschrift	→1970
➡Btx mit PIN/TAN	→1983
➡ZVDFÜ mit PIN und Diskette	→1987
➡(Multicash) FTAM mit EU	→1995
➡Internetbanking	→1998
➡HBCI mit DES-Chipkarte	→1999

Internetbanking - nicht der erste, aber ein wichtiger Schritt in der elektronischen Kommunikation mit Kunden

Btx-Banking seit ca. 20 Jahren

- Bildschirmtext der Telekom
- ca.50 % aller heutigen Transaktionen über Btx
- keine vergleichbaren Sicherheitsanforderungen wie im Internet, weil
  - Partnersicherheit
    - geschlossenes Netz
  - Datensicherheit (Einsichtnahme, Manipulation)
    - geschlossenes Netz
  - Transaktionssicherheit
    - PIN / TAN
- keine bekannten Schadensfälle
- PIN / TAN als bewährtes Sicherungsmittel

Status Quo

- Initiativen sind leider noch zu stark "technikgetrieben"
- jede mögliche Marktentwicklung wird verfolgt bzw. umgesetzt, ohne zu prüfen, ob der Markt dafür reif ist
- Problem: von Freaks können die Sparkassen nicht leben
- das Gros der Kunden und unserer Mitarbeiter bleibt dabei auf der Strecke, weil sie
  - noch nicht"reif" dafür sind
  - das Angebot zu kompliziert ist oder
  - schlicht nicht verstehen, was wir wollen
- aber selbst wenn die v. g. Faktoren nicht zutreffen, kann ein Produkt nur erfolgreich vermarktet werden, wenn
  - die Mitarbeiter mit der Entwicklung mitgehen
  - den Kunden ein echter Mehrwert, der seinen Bedürfnissen entspricht, geboten werden kann

Ziele des Internetangebotes der ostdeutschen Sparkassen

Schaffung einer vertriebsorientierten Plattform, bei der

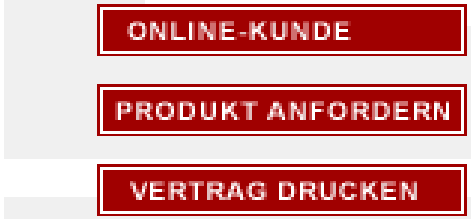
- technisches Spezialwissen nicht erforderlich ist (MA der Marketingabteilung mit Windows-Grundkenntnissen muss damit arbeiten können)
- die Sparkasse ihre eigene Geschäftspolitik abbilden kann
- die Kundengewohnheiten und -interessen im Vordergrund stehen
- dem Multikanalgedanken Rechnung getragen wird
- Internet ein gleichberechtigter Vertriebsweg ist

Wichtig: Wir müssen den Kunden dort abholen, wo er sich befindet und nicht sofort dort hinbringen, wo wir ihn gerne haben wollen.

simple Formel: Masse = Einfachheit bzw. Elite = komplexe Anwendung

multi > channel > chances

Internet - Jeder kann abschließen



Drei Wege der Kommunikation

- **Online-Kunde** gesicherte Transaktion (SSL + PIN/TAN)
  - nach Eingabe aller Daten - online-Weiterleitung des Vertragsformulars an Sparkasse
  - durch Mausklick auf „Formular senden“ öffnet sich die Internet-Banking-Oberfläche (geschützter Bereich) der Sparkasse
  - alle Angaben müssen mit PIN und TAN bestätigt werden
  - Bestätigung und Produktunterlagen von Sparkasse werden per Post zugestellt

- **Produkt anfordern** Senden einer E-Mail (SSL)
  - Weiterleitung aller relevanter Daten per E-Mail an Sparkasse
  - Produktunterlagen und Sparurkunden werden per Post zugestellt

- **Vertrag drucken**
  - alle notwendigen Eingabefelder ausfüllen
  - Vertrag ausdrucken und unterschrieben per Post oder Fax an Sparkasse senden
  - Bestätigung und Produkt von Sparkasse werden per Post zugestellt
  - Feststellung der Identität anhand der Unterschrift (Bestandskunde), sonst Erstlegitimation durch Spk.

SSL-gesicherte Übertragung von Kundendaten beim Produktabschluss

Bitte Antragsformular ausfüllen und absenden. Geben Sie bitte im Anschluss in unserem Internet-Banking-Angebot Ihre Kontonummer und PIN ein und bestätigen den Auftrag mit einer TAN.

Die Übertragung Ihrer Daten erfolgt verschlüsselt über einen sicheren Server.

Ich möchte das Anlageprodukt Spar Plus zu folgenden Bedingungen erwerben:

* Anlagedatum: 02.08.2001

* Einmaliger Anlagebetrag: 2000 DEM

(Mindestanlagebetrag 2000 DEM bzw. 1000 EUR)

Ich ermächtige Sie widerruflich, den einmaligen Anlagebetrag von folgendem Girokonto einzuziehen:

* Konto-Nr.: 1545454

* Institut: Sparkasse Musterhausen

* Bankleitzahl: 30000000

Zusätzlich bitte ich um Einrichtung eines Dauerauftrages: nein

von Konto: 452111

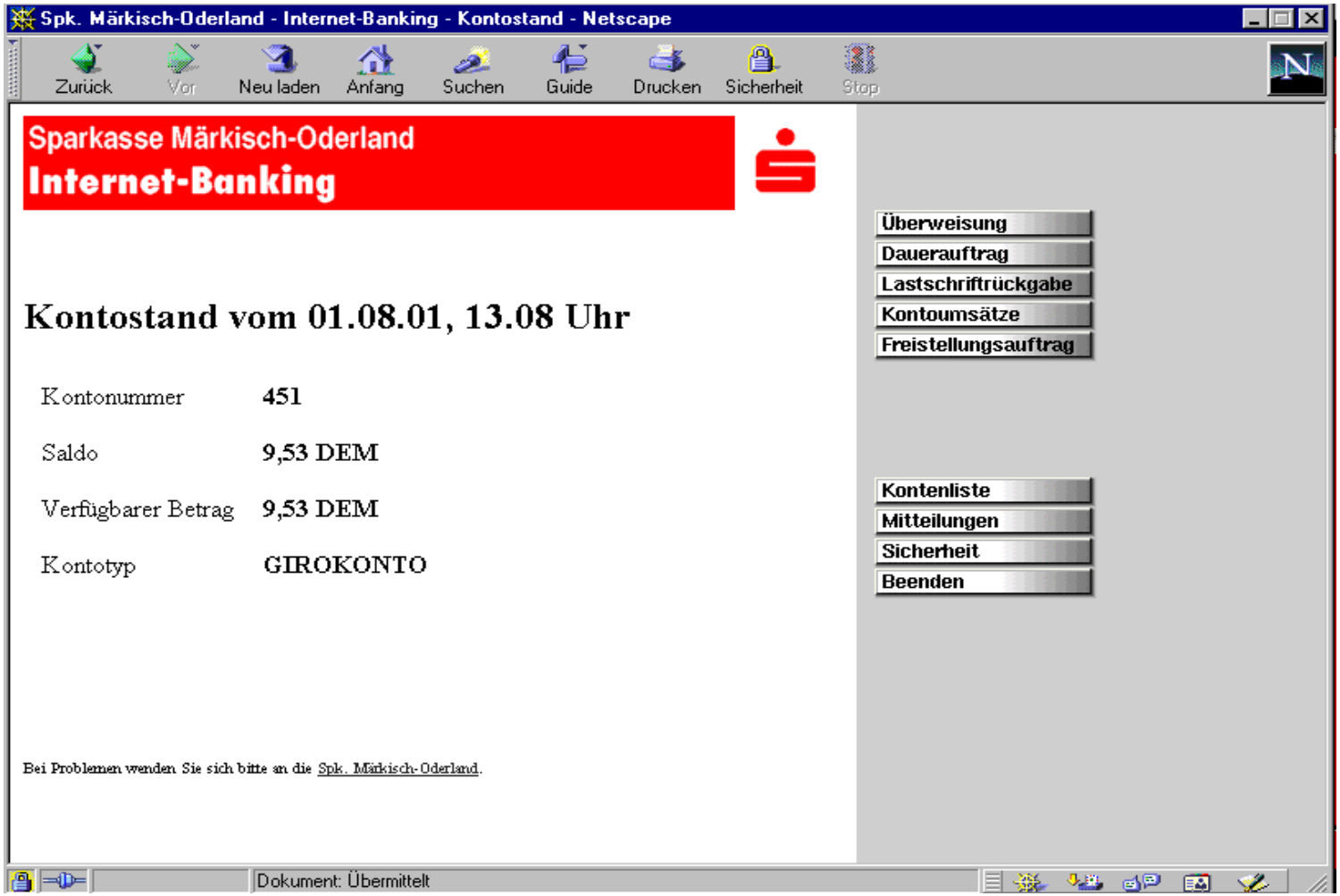
bei: Sparkasse Musterhausen

Ausführung: monatlich

Validierung der Daten serverseitig mit PHP

multi > channel > chances

Sicherheit und Transaktionsmöglichkeiten beim Banking im Internet



Gefahrenpotentiale und Lösungen beim Internetbanking

Simulieren einer falschen Bank

Austausch von Zertifikaten

Fälschung von u. Einsichtnahme in Nachrichten

Verschlüsselung mit SSL

Leugnen einer Transaktion des Kunden

PIN/TAN

Sicherheit durch Zertifikat

Sicherheit durch Verschlüsselung

Netsite: https://ww2.homebanking-brandenburg.de/cgi/anfang.cgi/Spk_Maerkisch-Oderland

Datei MIME Typ: text/html

Quelltext: Gegenwärtig im Speicher-Cache

Lokale Cache-Datei: Keine

Zuletzt bearbeitet am: Unbekannt

Zuletzt bearbeitet am: Unbekannt

Inhaltslänge: 2588

Verfällt am: Dienstag, 28. März 2000 15:10:45

Zeichensatz: Unbekannt

Sicherheit: Dies ist ein geschütztes Dokument, das eine für den ausschließlichen Gebrauch im Inland bestimmte Verschlüsselung hoher Komplexität verwendet (RC4, 128 bit).

Zertifikat:

This Certificate belongs to:
ww2.homebanking-brandenburg.de
dvg Datenverarbeitungsgesellschaft Hannover mbH
Hannover, Niedersachsen, DE

This Certificate was issued by:
www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign
VeriSign International Server CA - Class 3
VeriSign, Inc.
VeriSign Trust Network

Serial Number: 32:60:C5:34:99:FA:D9:AA:BF:7E:77:B2:D7:21:FE:7B
This Certificate is valid from Tue Jul 27, 1999 to Thu Jul 27, 2000
Certificate Fingerprint:
1F:87:70:AF:06:70:E1:77:10:B8:41:C6:79:B6:EC:C0

HBCI-Sicherheit - der neue Standard im Internet?

- Home Banking Computer Interface
- Neuer Bankenstandard für die Kommunikation über beliebige Protokolle (z.B. TCP/IP)
- neue Sicherheitsmechanismen sind Kernstück der HBCI-Entwicklung
  - Elektronische Unterschrift: RSA (1024 Bit)
  - Verschlüsselung: RDH
- Basis: ZKA-Abkommen „DFÜ mit Kunden“
- Berücksichtigung der Anforderungen des Signaturgesetzes
  - Kontext-Signatur → Daten des GV gehen in die Signaturbildung mit ein
  - anders als bei reinen Transportsicherungsverfahren, wo Inhaltsbezug zur Signatur nicht gegeben

Hauptproblem bei Geschäften und Zahlungen im Internet ist die Anonymität

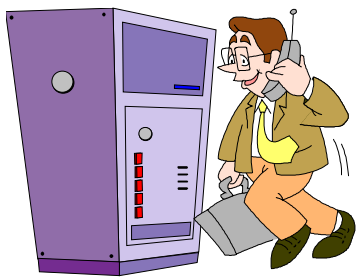
- 1. Aus Händlersicht
  - Wie verhindere ich, dass ich liefere und kein Geld bekomme?
- 2. Aus Konsumentensicht
  - Wie verhindere ich, dass ich zahle und nichts bekomme?
- 3. Wie verhindere ich, dass der Partner Daten erhält, die ihn nichts angehen
- Lösung Ware ⟺ Geld

Wünsche für die Zukunft

- nicht ausschließlich das machen, was gerade "modern" ist
- Strategie ist immer eine Mischung aus kurzfristig Machbarem (Time to market) und möglichen langfristigen Entwicklungstrends
- wird das kurzfristig Machbare vernachlässigt, gehen erfahrungsgemäß Marktanteile verloren
- setzt man zu stark und zu früh auf Entwicklungstrends, besteht die Gefahr der Fehlentwicklung

Fazit:

- weniger Technik- und dafür etwas mehr Marktorientierung
- Bedürfnisse der interessanten Massenkunden müssen in den Mittelpunkt rücken
- auf Marktentwicklungen muss schnell reagiert werden



Data protection in the Czech Republic

Dr. Karel Neuwirt

The Office for Personal Data Protection

Legislation

- Act No. 1/1991 Coll. - Constitution
- Act No. 23/1991 Coll. - Instrument of fundamental rights and freedoms
- Act No.101/2000 Coll.- on personal data protection and on changes to several laws
- Act No.227/2000 Coll. – on electronic signature
- Act No.106/1999 Coll.- on free access to information
- Sectorial laws

Harmonization with Europe

- Convention ETS 108

  signature September 8, 2000

  ratification July 9, 2001

- Directive 95/46/EC

  Act No.101/2000 Coll. – request for harmonization opinion by EC

The Office

- Established by Act No.101 of 2000
- President (elected by Senate, appointed by President CR)
- 7 inspectors (elected by Senate, appointed by President)
- 65 staffs (untill 2001)
- 90 staffs – final (during 2002)
- 15 staffs – electronic signature

Competency of the Office

- Supervision on lawful data processing
  - public sector
  - private sector
  - police
  - other bodies

  exemption – intelligence services
- Notification

  notified 14 000 controllers

Fines and penalties

- Fines to controllers and/or processors

  up to CZK 10 mil. (EUR 300 000) – for single breach of the law

  up to CZK 20 mil. (EUR 600 000) – for repeating breach of the law

Fines and penalties

- To persons working for controllers or processors
  - up to CZK 50 000 (EUR 1500) for breach of duty of secrecy
  - up to CZK 25 000 (EUR 750) for breach another obligation stipulated by the Act
  - up to CZK 25 000 (EUR 750) – disciplinary penalty (not assistance within Office's supervision)

First experiences

- New problem in CEE countries

  (no history, no legislative practice, no experience with supervision)

- Domestic law is not harmonized with data protection principles
- Low willingness to change bad practice of controllers and processors

First experiences – cont.

- Problems with application of the law into daily practice
  - no relevant data collection
  - consent of data subject
  - data transfer
  - no knowledge among citizens
  - lobby effort to amend the law

First experiences – cont.

- Problems in public sector

  - national public registries (citizens, economic activity, properties, debtors)
  - data sharing
  - conflict with public access to information
  - statistical service (census)
  - abuse of national citizen´s ID number
  - health and social sectors
  - access to documents of former State Security Service

First experiences – cont.

- Problems in private sector
  - direct marketing
  - insurance, banking sectors
  - registr of bad payers
  - public transport
  - telecommunication providers

Terrorist attack

- A new world after September 11
- Council of Europe – Declaration on the fight against international terrorism (12 Sept.)
- New debate on human rights and data protection (Germany, U.K., France, Czech Rep.)
- **It is necessary to reduce data protection principles ?**

Contacts

- The Office for Personal Data Protection

  Havelkova 22, CZ-130 00 Prague 3

  Czech Republic

  tel.: +420 2 2100 8288

  fax: +420 2 2271 8943

  info@uoou.cz

  www.uoou.cz

Ona Jakštaitė
Head of the State Data Protection Inspectorate of the Republic of Lithuania

Data protection in Lithuania – first practical experiences

Introduction

At the end of the year 1995 Lithuania submitted the official application for the EU membership. Lithuania will be able to accomplish her aims by 1 January 2004. We strive for being ready not only to fulfil the requirements of the Community laws, but also to participate in the making of EU common decisions at that time.

The legal basis of data protection

The grounds of modern data protection have been created in Lithuania recently *(http://www.is.lt/dsinsp)*.

The fundamental principles on privacy and personal data protection are contained in the Constitution of the Republic of Lithuania, adopted in 1992, and the Law on Legal Protection of Personal Data, adopted in 1996 and amended in 2000 according to Directive 95/46/EC.

Liability for the violation of data processing has been provided for lately. In 1998 the Administrative Code has been supplemented with regulations on illegal processing of personal data and on preventing a person from access to his personal data or to information about this data. The Penal Code, adopted in 2000, determines liability for illegal collection, disclosure or use of information on private life as well as for the destruction, alteration or dissemination of computer information.

In 1997 the Government approved general requirements on data protection in state and municipal information systems. In 2000 the Regulations on the State Register of Personal Data Controllers were passed. The State Data Protection Inspectorate approved the

Form of Contract on Personal Data Disclosure in 1997 and the Requirements and Form on Description of Data Protection Measures in 2001.

Lithuania has ratified the Council of Europe Convention on the Protection of Human Rights and Fundamental Freedoms in 1995 and the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data in February this year.

The problems are the following:

1) The Directive's inapplicability to cooperation in the field of Justice and Home affairs.

The Convention ETS 108, the Europol Convention and the Schengen acquis require to to fix the basic principles of data protection in domestic law.

The Law with exceptions according to Directive 95/46/EC has been adopted last year, but these exceptions become an obstacle in the negotiations for cooperation. Therefore the law is being amended.

However we still have to solve the problem to what extent the law should apply to the processing of personal data containing state secrets?

2) Public registers containing personal data

The Public State Registers are: the Mortgage Register, the Real Estate Register, the Register of Legal Persons, the Register of Acts of Property Arrests, etc. The Public Registers contain personal data and everyone is able to access this information if he/she indicates the purpose. However some persons complain when unexpected guests visit them and ask to explain how and why visitors have got their address or birth date.

We discuss what limits of publicity should be determined for Public Registers, so that they wouldn't cause an infringement of personal data regulations.

3) Integrated information systems

The Law on the Population Register obliges the state and municipal institutions using personal data to update data in accordance with data of the Population Register. The Law of State Registers defines that all state registers must take data from the Population Register and the Real Estate Register. It is intended to integrate state information systems and sometimes it is considered that information about individuals should be collected in one place from various sources. There is a risk of an infringement of personal data regulations.

Not only public institutions but also private companies intend to use the opportunities of information technologies in full. Companies are being founded as mediators for others - which have contracts with individuals - and collect personal data from different sources (often in order to process debtors' data). Therefore a problem arises because such mediators don't act as data processors on behalf of other companies. Mediating companies combine data received from different sources which are necessary for the purpose of the legitimate interests pursued by the data controllers. At the same time the interests of data subjects, who don't fulfil the contract obligations, are taken into account. However the risk of an infringement of personal data regulations rises inevitably.

It is not easy to balance opportunities of information technologies with the requirement to ensure that personal data should not be processed excessively.

The system of data protection supervision

The independent data protection supervision system is still under construction.

The State Data Protection Inspectorate has been founded at the end of 1996. The Inspectorate takes care of data protection and supervises the lawfulness of personal data processing. There is an exception – the processing of personal data for journalistic purposes is supervised by the institution of the Inspector of Journalistic Ethic.

The State Data Protection Inspectorate is being restructured into an independent authority. A general model of fully independent institutions has not been established in Lithuania, so the solution to such a problem on the top level is a long and difficult process. At the end of September the government adopted a resolution on the structural reform of the Inspectorate. From 1 October 2001 the State Data Protection Inspectorate is an independent governmental institution.

The Inspectorate has been active for more than 4 years and has a staff of eight employees. After the structural reform the number of employees has increased up to 22. The first years of its activity were directed to transposition according to European legislation and prevention of violations of data processing regulations in information systems. The number of achievements is quite large. A data protection legislation has been created on the basis of EU law. In September we held a meeting with experts of the Council of Europe and the European Commission in order to evaluate the compatibility of the Law on Legal Protection of Personal Data with Directive 95/46/EC and the Convention ETS 108. The result of the experts' evaluation was positive. However we should correct the law aiming to fulfil the Directive 95/46/EC exactly. To some extent we created a methodological basis for the supervision of thousands of data controllers which are inspected following complaints (requests etc.). We draw protocols of administrative law violations very rarely but mostly we provide instructions for data controllers. The rapidly increased number of requests and the small number of complaints do actually prove the rightness of our chosen strategy of prevention instead of punishment.

The problems and possible solutions are the following:

1) Data security. How should we evaluate whether a data controller has established the appropriate level of data security and implemented sufficient data protection measures? We have requirements, standards and methods, but we don't have a clearly defined system of evaluation and so far it is problematic to come to comprehensive conclusions on data security. We will solve this problem in the nearest future.

2) Information of the public. We have training programmes on data protection at universities and at the Institute of Public Administration, but we still don't have enough skilled specialists on data protection.

There is a lack in understanding of data protection in the public, although more and more media publications deal with the dangers of personal data processing. We must raise public awareness of privacy rights in order to achieve that individuals themselves take a more active interest in the processing of their data.

The peculiarities of the national data protection law

Some peculiarities, introduced in Lithuanian laws, should be mentioned.

1) Since 1997 we have approved a model for a data disclosure contract between data processors and data recipients. This way of provision of personal data disciplines data controllers and data recipients, forces them to notify the supervision authority of personal data processing, to introduce safeguards and to undertake to keep personal data secret.

2) According to the Law on Legal Protection of Personal Data the supervision authority will provide its service to data subjects from the year 2003. It is intended to facilitate access to data about oneself for individuals. Each person will be able to apply to the supervision authority and to request to collect his/her data from the registered data controllers. The supervisory authority shall make the collected data available to each person at a central location.

Conclusion

We intend to create a reliable and efficient system of data protection, fulfilling requirements of the European Union and properly acting in the environment of information society. We can be proud today of a very positive evaluation by the Director of Europol stating that data protection in Lithuania has reached a high standard and is

getting close to the best level of all EU countries. We remember the words of honourable Mr. J. Storbeck that it is important for us not only to have the laws and an independent institution, but also citizens using and institutions implementing these laws.

Lothar Koch
Landrat des Landkreises Potsdam-Mittelmark

IuK-Technik verändert Kommunalverwaltung - Reformprojekt im Landkreis Potsdam-Mittelmark

Die Überlegungen, dass der effektive Einsatz der IuK-Technik den Verwaltungsreform-Prozess wesentlich bestimmen wird, führen zwangsläufig zum Electronic-Government.

Dieser Ansatz allerdings übertrifft bezüglich der Gestaltungsentscheidungen in den öffentlichen Verwaltungen alles bisher Dagewesene, denn Electronic Government muss als umfassendes neues Konzept verstanden werden.

Es geht um wesentlich mehr, als um Internetkontakte zwischen Bürgern, Wirtschaft und Verwaltung. Das Neue in dem Konzept sind die Informations- und Kommunikationsstrukturen, die in ihren wechselseitigen Beziehungen zwischen Bürgern, Wirtschaftsunternehmen sowie allen Ebenen von Politik und öffentlicher Verwaltung in Arbeitsabläufen und Entscheidungsprozessen völlig neue Lösungsansätze erfordern.

Ihre neue Qualität ergibt sich aus der Wechselwirkung der Abkehr von der Verstrohmung alter Prozesse bzw. Hinwendung zu funktionsbezogenen verknüpften menschlichen und maschinellen Beiträgen, die sich herausbilden müssen und interaktiv auf unsere Arbeit und Wahrnehmung wirken. Es entsteht eine neue Qualität der Selbstverwaltung unserer komplexen Bedürfnisse.

In diesem Blickwinkel erscheint Electronic Government als Innovationsstrategie, die als einzige den neuen Anforderungen der sich verändernden gesamtgesellschaftlichen Verhältnisse gerecht wird und zwar in der Weise, dass sie den hohen Anforderungen und dem Bild einer die Gesellschaft aktivierende und mit ihr in Wechselwirkung stehende Verwaltung entspricht. Den kooperativen Beziehungen von Verwaltungen untereinander kommt in Zukunft die größte Bedeutung zu, weil die Gestaltungsentscheidungen alles bisher Da-

gewesene übertreffen, benötigen wir Leitsätze, die den Prozess strukturieren und die Ableitung von Handlungsgrundsätzen möglich machen.

Es sind dies:

1. Der Verwaltungsbereich ist in seiner Eingrenzung der einzige menschliche und maschinelle Tätigkeitsbereich, bei dem von der Quelle bis zur Senke das Produkt Information (Bescheid, Beschluss, Urteil) bearbeitet wird. Deshalb gilt ihm logischerweise die höchste Aufmerksamkeit der durch neue Medien sich verändernden Welt.

2. Electronic Government als Informationsstrategie bietet die Chance einer wirklichen Verwaltungsmodernisierung in ihrer Gesamtheit des Verwaltungshandelns und führt zu einem neuen Schub der Verwaltungsmodernisierung.

3. Zum ersten mal in der Geschichte der Menschheit ist durch den mit Lichtgeschwindigkeit ablaufenden Informationsaustauschprozesse der Ort des Bedarfs oder Abrufs der Information vom Ort der Bearbeitung der Information zu trennen (Die Postkutsche fährt mit Lichtgeschwindigkeit vom Front- zum Backoffice und umgekehrt)

4. Im Mittelpunkt des Verwaltungsreformprozesses steht der Mensch. Er erwartet ganzheitliche Lösungen, die nur mit Einbeziehung der Wirtschaft gelingen können. (Lebensqualität)

5. Ergebnisse und Erfolge hängen wesentlich von der Lern- und Innovationsfähigkeit der Entscheider auf allen Ebenen ab. Besonders in Politik und Verwaltung ist diese Fähigkeit um Größenordnungen zu steigern.

6. Überkommene und teilweise überbordende rechtliche Beschränkungen, die den IT-Einsatz behindern und teilweise gar verhindern, sind zu überdenken. Die darin sich beschränkenden Anreizstrukturen behindern darüber hinaus vorhandene Innovations- und Leistungspotentiale.

Auf der Grundlage dieser Leitgedanken wurde das Projekt “Integrierte Kommunalverwaltung im Landkreis Potsdam-Mittelmark” entwickelt.

Kerngedanke ist die schrittweise Vernetzung aller Verwaltungsebenen zur Modernisierung und damit Optimierung der Verwaltung.

Dr. Helmut Bäumler
Leiter des Unabhängigen Landeszentrums für Datenschutz
Schleswig-Holstein

Informationszugang als ein neuer Service der Verwaltung

I. Begründung des Rechts auf Informationszugang

Das Recht auf Informationszugang ist in Deutschland bundesweit für Umweltinformationen im Bundesumweltinformationsgesetz sowie auf Länderebene bereichsübergreifend in den Informationsfreiheitsgesetzen der Länder Brandenburg, Berlin und Schleswig-Holstein geregelt. Eine explizite verfassungsrechtliche Grundlage findet sich lediglich in Artikel 21 der Brandenburgischen Landesverfassung. Gleichwohl enthält auch das Grundgesetz Ansatzpunkte für Informationszugangsrechte. Das allgemeine Persönlichkeitsrecht in der besonderen Ausprägung des Rechts auf informationelle Selbstbestimmung wird zwar gelegentlich so interpretiert, als setze es nicht nur Informationsansprüche über die zur eigenen Person gespeicherten Daten, sondern generell den informierten Bürger voraus. Ein allgemeiner Anspruch auf Informationen gegenüber dem Staat ergibt sich aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG jedoch nicht. Auch wenn Art. 5 Abs. 1 GG subjektiv–rechtlich einen Informationsanspruch erst dann begründet, wenn der Zugang zu einer Quelle schon eröffnet ist, darf objektiv-rechtlich die enge Wechselwirkung zwischen Informationsfreiheit und Demokratieprinzip nicht außer Acht gelassen werden! In unserem demokratischen Rechtsstaat kann nur derjenige sinnvoll von seinen Rechten Gebrauch machen, der hinreichend informiert ist.

Das Bundesverfassungsgericht hat im Volkszählungsurteil mit der Formulierung, die informationelle Selbstbestimmung sei eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens, dem Datenschutz ein Fundament in den Staatsformbestimmungen des Grundgesetzes gegeben, das auch Informationsansprüche trägt. Nur der informierte Bürger kann am demokratischen Willensbildungsprozess mitwirken. Informationszu-

gangsrechte gehen zunächst „zu Lasten“ derer, die die Informationen zu gewähren haben. Sie verändern die Informationsbalance zwischen öffentlicher Verwaltung und Bürgern zugunsten Letzterer. So gesehen heißt mehr staatliche Informationen offenzulegen auch ein bisschen mehr Demokratie zu wagen.

Andere Begründungen der Informationsfreiheit nehmen stärker die Verwaltung ins Blickfeld. Man erwartet z. B., dass eine transparente Verwaltung weniger anfällig ist für Korruption. Es ist übrigens interessant, was einer der profiliertesten Mafia-Gegner Italiens, der frühere Bürgermeister von Palermo, Leolucca Orlando, nach seiner Wahl als erstes tat: Er öffnete die Sitzungen und Aktensammlungen der Stadt Palermo für interessierte Bürgerinnen und Bürger.

Schließlich wird auch der Aspekt der Kontrolle des Verwaltungshandelns als Motiv genannt und in § 1 des Berliner Informationsfreiheitsgesetzes sogar als ein Zweck des Gesetzes bezeichnet. Da die bestehenden Informationsfreiheitsgesetze übereinstimmend Gesetzgebung und Rechtsprechung ausklammern (soweit diese nicht im Einzelfall exekutiv tätig werden), zielt ihre Wirkung hauptsächlich auf die Verwaltung. Damit scheint den Informationsfreiheitsgesetzen unausgesprochen das traditionelle Bild einer Verwaltung zugrundezuliegen, die sich mit Hilfe des allgemeinen Akten- und Amtsgeheimnisses, bei Bedarf und in zunehmendem Maße unterstützt durch das Datenschutzrecht, auf eine dem Bürger gegenüber überlegene Informationslage stützt und auf diese Weise eine intransparente Politik betreibt. Träfe dieses Bild uneingeschränkt zu, dann wäre die Auseinandersetzung um Informationsfreiheitsrechte im Kern ein Kampf um den demokratischen Willensbildungsprozess, der vornehmlich gegen die Verwaltung und ihre Verbündeten in der Politik zu führen ist

Richten wir den Blick auf die Bürger. Ihnen kommt bei dieser Sichtweise die Rolle zu, als die um das Wohl der Allgemeinheit besorgten Kontrolleure der Verwaltung aufzutreten. Da die Informationsfreiheitsgesetze eine wie auch immer geartete Ortsbezogenheit nicht verlangen, könnte es sich beispielsweise ein quivis ex populo aus Brandenburg zur Aufgabe machen, das Verwaltungshandeln in Schleswig-Holstein qua Inanspruchnahme des Informationsfreiheitsgesetzes zu kontrollieren und umgekehrt natürlich ebenso. Je-

dermann kann auf der Grundlage von Informationsfreiheitsgesetzen jederzeit und überall die Verwaltung kontrollieren.

Die Praxis sieht freilich anders aus. Zieht man eine erste vorsichtige Bilanz aus eineinhalb Jahren Erfahrung mit dem Informationsfreiheitsgesetz in Schleswig-Holstein, so kann man fast durchgängig feststellen, dass man sich auf Bürgerseite für Informationen bei Behörden interessiert, in deren Zuständigkeitsbereich man wohnt. Mehr noch: zumeist liegt eine subjektive Betroffenheit vor, die früher oder später ohnehin verwaltungsverfahrens- oder prozessrechtliche Informationsansprüche begründet hätte. Das typische Beispiel sind Bürger, die eher als nach bisherigem Recht möglich, über Planungsvorhaben informiert sein wollen, oder Betroffene, die in der Nähe eines Projektes, aber eben nicht nahe genug wohnen, als dass ihnen eine Klagebefugnis zweifelsfrei zustehen würde.

Das Informationsfreiheitsgesetz entpuppt sich jedenfalls in den ersten Monaten seines Bestehens in Schleswig-Holstein überwiegend als eine Chance für die Bürgerinnen und Bürger, die eigenen Interessen früher und wirkungsvoller als im herkömmlichen Rechtssystem wahrzunehmen. Dem aus dem Demokratieprinzip abgeleiteten Gedanken der allgemeinen Kontrolle des Verwaltungshandelns tut dies nicht unbedingt Abbruch. Denn die allgemeine Kontrollmöglichkeit entfaltet schon dann Wirkung, wenn sie tatsächlich gar nicht so häufig ausgeübt wird.

Auch Gerichtsverhandlungen finden überwiegend in leeren Sälen statt, ohne dass die Kontrollfunktion des Öffentlichkeitsprinzips der Gerichtsverhandlungen prinzipiell in Frage zu stellen wäre.

Aus dem gleichen Grund kommt auch der Tatsache, dass sich bislang die Inanspruchnahme der Informationsfreiheit eher verhalten und nicht massenhaft vollzieht, keine allzu große Bedeutung bei. Fast habe ich manchmal den Eindruck, als hielten es viele Bürger für derart unwahrscheinlich, dass sie tatsächlich ohne jede Voraussetzung in die Verwaltungsakten Einblick nehmen können, dass sie es gar nicht erst versuchen. Ich registriere bei meinen Vorträgen jedenfalls immer noch ein gewisses Maß an ungläubigem Staunen, dass es ein so weitgehendes Recht geben soll. Erst ganz langsam beginnt das Publikum offenbar zu begreifen, welche Möglichkeiten

ihm das Informationsfreiheitsrecht an die Hand gibt.

Auch andere Grundrechte werden übrigens de facto selten oder nur von wenigen ausgeübt, obwohl sie für unser demokratisches Gemeinwesen von großer Bedeutung sind. Wie viele Menschen haben tatsächlich schon einmal eine Partei gegründet? Wer hat sein Recht, eine Zeitung herauszugeben, je in Anspruch genommen und wo, außer im Hyde-Park in London, stellen sich Menschen auf die Straße und machen von ihrem Recht auf freie Rede Gebrauch? Und doch möchten wir diese für unser freiheitlich demokratisches Gemeinwesen wichtigen Rechte nicht aus der Verfassung gestrichen haben, nur weil sie nicht jeden Tag massenhaft in Anspruch genommen werden. Auch das Informationsfreiheitsrecht muss seine Bedeutung nicht durch ständig steigende Zahlen der Inanspruchnahme stets aufs neue unter Beweis stellen. Es ist wahrscheinlich sogar ein Vorteil, dass nach Inkrafttreten der Informationsfreiheitsgesetze nicht diejenigen Recht behalten haben, die geradezu den Zusammenbruch der Verwaltung unter der Last der vieltausendfachen Informationsgesuche vorhergesagt haben. Oder anders ausgedrückt: Vornehmlich aus der Verwaltung stammende Bedenken gegen Vorhaben und Entwürfe zum Informationsfreiheitsrecht haben sich in der Praxis nicht bewahrheitet.

Zurück zu den Wurzeln der Informationsfreiheit. Die Kontrolle der Verwaltung ist eine wichtige Motivation, aber nicht die einzige. Die Erfahrung mit dem Informationsfreiheitsgesetz in Schleswig-Holstein zeigt eher, dass Informationswünsche überwiegend dem wohlverstandenen Eigeninteresse dienen. Unmotivierte Querulanten einerseits und der demokratischen Kontrolle der Verwaltung um ihrer selbst willen Verbundene andererseits sind eher die Ausnahme.

II. Das gewandelte Selbstverständnis der Verwaltung

Dem Kontrollgedanken liegt ein Bild der staatlichen Verwaltung zugrunde, das, wie gleich näher zu beleuchten sein wird, im Wandel begriffen ist. Kein Zweifel: in manchen Bereichen begegnet uns die Verwaltung durchaus noch so, wie wir sie uns traditionell immer vorgestellt haben: hoheitlich, mit Herrschaftswissen ausgestattet

und den Bürger eher als Gewalt Unterworfenen wahrnehmend; als preußische Obrigkeitsverwaltung eben. Einer solchen Verwaltung wünscht man als Bürger gerne jedwede Form von Kontrolle an den Hals.

Indes – stimmt dieses Bild überhaupt noch? Werden wir nicht beinahe ohne Unterlass mit den Ideen und Projekten der Verwaltungsmodernisierung vertraut gemacht? Es würde natürlich zu weit führen, hier auf die verschiedenen Aspekte von E-Government und modernisierter Verwaltung einzugehen. Gemeinsam ist ihnen jedenfalls, dass sie privatwirtschaftliche Strategien, Handlungsformen und Erfahrungen für die öffentliche Verwaltung nutzbar machen wollen. Da ist die Rede von neuem Steuerungsmodell, dezentraler Mittelbewirtschaftung, Benchmarking, Querschnittskontrolle und sogar von den Produkten der Verwaltung. Vielerorts werden heute die Dienstleistungen der Verwaltung in Produkten definiert und damit dem Vokabular der Marktwirtschaft angepasst. Wer sein eigenes Angebot als Produkt bezeichnet, der begibt sich auf den Marktplatz der Konkurrenz, denn ein Produkt könnte prinzipiell auch ein beliebiger anderer anbieten. Und in der Tat werden heute vielerorts nüchterne Berechnungen darüber angestellt, welches Angebot günstiger sei: das der Verwaltung oder das ihrer privaten Konkurrenz. Offenbar gibt es dabei keine Tabus, denn wir erfahren z. B. aus den USA, dass private Gefängnisse angeblich günstiger sind als staatliche. Ergo erhalten sie in nicht wenigen Städten den Zuschlag.

Wir sprechen auch in Deutschland, wenn es um Verwaltungsmodernisierung bis hin zur Metamorphose von Verwaltungsdienstleistungen in Produkte geht, keineswegs nur von Plänen auf dem Reißbrett. Der Veränderungsprozess in den Verwaltungen ist bereits in vollem Gange. Eine solchermaßen entzauberte und ihres obrigkeitsstaatlichen Habitus regelrecht beraubte Verwaltung kann im Bürger nicht mehr den Untertanen sehen. Ihr steht der Bürger nunmehr als Kunde gegenüber, dem es tunlichst mit Service und Entgegenkommen zu begegnen gilt. Die Verwaltung als Servicebetrieb ist gewiss noch nicht überall realisiert und es gibt nach wie vor Bereiche der staatlichen Verwaltung, in denen man sich den Bürger kaum als Kunden vorstellen kann. Wenn beispielsweise die Polizei von ihren „Kunden“ spricht, dann meint sie damit etwas ganz ande-

res. Alles in allem kann aber kein Zweifel daran bestehen, dass sich die Verwaltung überall in Deutschland auf den langen Marsch von der preußischen Obrigkeitsverwaltung hin zu einem kundenorientierten Servicebetrieb gemacht hat.

III. Informationszugang als Service

Dieser Wandlungsprozess bleibt nicht ohne Folgen für die Funktion von Informationsfreiheitsgesetzen. Sie sind auch, aber eben nicht nur die der Verwaltung mühsam abgetrotzten Kontrollinstrumente, sondern Teil des Serviceangebotes. Der Bürger als Kunde und Auftraggeber der Verwaltung muss selbstverständlich das Recht haben, von Zeit zu Zeit nach dem Rechten zu sehen und sich über die Arbeitsweise seines Auftragnehmers zu informieren. Verwaltungstransparenz als besonderer Service der modernisierten Verwaltung wird allerdings - soweit für mich ersichtlich – bislang in der einschlägigen Literatur noch kaum thematisiert. Dabei könnte gerade darin ein Konkurrenzvorteil gegenüber privaten Anbietern liegen. Dort kennt man Informationszugangsrechte, von den Publizitätsvorschriften der Kapitalgesellschaften einmal abgesehen, bislang kaum. Über Forderungen, langfristig müsste sich das Informationsfreiheitsgesetz auch auf zumindest große Wirtschaftsunternehmen beziehen, ist zwar hin und wieder zu lesen, aber der Weg dorthin erscheint mir noch sehr weit.

Also: was sollte die öffentlichen Verwaltungen in den drei Ländern Brandenburg, Berlin und Schleswig-Holstein und demnächst hoffentlich auch im Bund daran hindern, die bestehenden Informationszugangsansprüche der Bürger als einen besonderen Service zu begreifen? Eine selbstbewusste Verwaltung, die dem Bürger ohnehin nicht mehr obrigkeitlich kommen möchte, dürfte mit einem solchen Ansatz eigentlich keine Probleme haben. Mehr noch: Informationsansprüche gehören auf Sicht in das Benchmarking, wenn die Leistungen der Verwaltung mit denen der Privaten verglichen werden.

Eine Sichtweise, die Informationsrechte nur unter dem Blickwinkel der Verwaltungskontrolle und der Korruptionsbekämpfung sieht, greift deshalb nach meiner Auffassung etwas zu kurz. Besonders

deutlich kann der Servicecharakter der Informationsrechte zu Tage treten, wenn die Verwaltung von sich aus tätig wird. So sind nach § 17 des Berliner Informationsfreiheitsgesetzes bestimmte Informationen von der Verwaltung von sich aus allgemein zugänglich zu machen. Nach § 5 des IFG-SH können die Behörden Informationssuchende auf eine entsprechende Veröffentlichung, insbesondere im Internet, verweisen. Dies lädt geradezu dazu ein, Informationen auch ohne Antrag zu publizieren, statt von Fall zu Fall und auf Einzelantrag hin. Was ist das anderes als Informationsservice?

IV. Erfahrungen mit über zwei Jahrzehnten Datenschutz

Für eine Erweiterung des Blickfeldes bei der Betrachtung der Informationszugangsrechte sprechen auch pragmatische Gesichtspunkte. Gerade die Datenschutzbeauftragten können ein Lied davon singen was es heißt, ein neues Prinzip gegen den Widerstand der Verwaltung durchzusetzen. Von Anfang an wurde der Datenschutz von weiten Teilen der Verwaltung als Fremdkörper betrachtet und genau genommen geschieht dies auch heute noch in manchen Behörden. Die Datenschutzbeauftragten mussten sich notgedrungen auf einen langen Marsch durch die Gliederungen der Verwaltung machen.

Die Frontstellung zwischen Datenschutz und öffentlicher Verwaltung war teilweise so schroff, dass selbst die vernünftigsten Ideen und Vorschläge manchmal allein schon deshalb auf Ablehnung stießen, weil sie eben von Datenschutzseite kamen. Wieviel Energie hat es gekostet, den Datenschutz gegen den Widerstand der Verwaltung zu etablieren! In welch produktive Bahnen, etwa zur möglichst optimalen präventiven Datenschutzorganisation, hätte man diese Energie lenken können. Vielleicht aber auch nicht, denn ich bin mir nicht sicher, ob es Ende der 70er Jahre und in den 80er Jahren tatsächlich eine echte Alternative zur streitigen Durchsetzung des Datenschutzes in der Verwaltung gab.

Der Blick zurück ist müßig, weil man die Abläufe im nachhinein nicht mehr ändern kann. Datenschutz und Verwaltung haben sich inzwischen leidlich arrangiert. Die Bürokratie hat den Datenschutz zuerst widerwillig akzeptiert und beginnt ihn jetzt bisweilen sogar

als interessantes Spielzeug zu entdecken. Man kann ja damit manchen Informationswunsch zunächst einmal abblocken und mancher Reform ein entschiedenes „Njet“ aus Gründen des Datenschutzes entgegenhalten. Andererseits sind die Datenschutzbeauftragten gegenüber den Gründerjahren wohl auch ein wenig bürokratischer, der Verwaltung also ähnlicher und vertrauter geworden. Man versteht sich jetzt gegenseitig besser.

Die Tatsache, dass in den Ländern Brandenburg, Berlin und Schleswig-Holstein die Datenschutzbeauftragten zugleich Informationszugangsbeauftragte geworden sind, birgt auch die Chance, Erfahrungen aus der Frühzeit des Datenschutzes produktiv für die Sache der Informationsfreiheit zu nutzen. Ich plädiere also dafür, das Informationsfreiheitsrecht nicht von vornherein und nicht ausschließlich als Kampfinstrument gegen die Verwaltung zu interpretieren. Wir sollten zumindest die Chance suchen und gegebenenfalls nutzen, die Verwirklichung der Informationsfreiheit gemeinsam mit der Verwaltung anzugehen. Die Bürger hätten etwas davon, wenn z. B. die Akten und Informationssammlungen der Verwaltung mit Hilfe der Beratung der Informationszugangsbeauftragten von vornherein so organisiert würden, dass Informationswünsche schnell und unbürokratisch und unter Schonung etwaiger entgegenstehender Interessen erfüllt werden könnten.

Wir haben in Schleswig-Holstein in den letzten 1 ½ Jahren bei ca. 40 an das Unabhängige Landeszentrum für Datenschutz herangetragenen Streitfällen im Rahmen des Informationsfreiheitsgesetzes nur eine einzige Beanstandung aussprechen müssen. In vielen Fällen gab es durch unsere Vermittlung eine Lösung, mit der beide Seiten leben konnten. Wo immer es möglich ist, sollten wir die Verwaltung mitnehmen in die Informationsgesellschaft, die ohne Informationsfreiheit aus meiner Sicht nicht komplett ist. Eine Perspektive, bei der der Informationszugang nicht nur ein Kontrollmittel, sondern auch und vor allem ein Service der Verwaltung ist, erleichtert einen sanften Übergang der Behörden in die Notwendigkeiten der Informationsgesellschaft.

Deshalb müssen keine Rechte preisgegeben werden und der Informationszugang muss nicht zurückfallen in die alten Zeiten, als er eine huldvoll gewährte Gnade war. Der unbedingte Charakter als

eines gesetzlich verbrieften Anspruchs darf nicht in Frage gestellt werden und gegenüber solchen Behörden, die auf stur stellen, muss dieser Anspruch auch durchgesetzt werden. Da haben wir Erfahrung. Aber ich meine, es ist den Versuch wert, die neuen Informationsrechte im Konsens mit der Verwaltung zu etablieren.

V. Vermeidung von Wertungswidersprüchen

Eine konsensorientierte Umsetzung des Informationsfreiheitsrechts wird erleichtert, wenn Wertungswidersprüche zum Datenschutzrecht vermieden werden. Dies ist für Datenschutzbeauftragte die zugleich Informationsbeauftragte sind, durchaus ein heikles Thema. Haben wir nicht soeben aus dem Volkszählungsurteil abgeleitet und bis in die letzte Amtsstube propagiert, dass es ein von vornherein belangloses personenbezogenes Datum nicht gibt? Haben wir nicht zu Recht darauf verwiesen, dass es entscheidend auf den Verwendungszusammenhang ankommt? Wie vertragen sich damit Informationsansprüche, die unter Umständen auch personenbezogene Daten Dritter einschließen können und deren Spezifikum gerade ihre voraussetzungslose Inanspruchnahme ist. Ein Grund, ein Zweck oder eine Verwendungsabsicht muss nicht genannt werden, weil gerade die Information um ihrer selbst willen, voraussetzungslos eben, verlangt werden kann. Wie kann man da den Verwendungszusammenhang und damit das evtl. Risiko für die Betroffenen prüfen?

Andere Fragen tun sich zu den Zweckbindungs- und zu den Übermittlungsbestimmungen der Datenschutzgesetze auf. Die Übermittlung personenbezogener Daten bedarf einer Rechtsgrundlage, die zumindest die Erforderlichkeit für die Aufgabenerfüllung zur Voraussetzung machen muss. Informationsansprüche müssen aber bekanntlich nicht begründet werden, so dass schon ein Maßstab für irgendwelche Erforderlichkeitsüberlegungen fehlt. Krass ist auch der Übergang personenbezogener Daten aus der öffentlichen Verwaltung, mit dem allenthalben geltenden Prinzip der Zweckbindung in eine völlig zweckfreie Nutzung durch diejenigen, die das Informationsfreiheitsgesetz in Anspruch nehmen.

Man sollte nicht glauben, dass der Verwaltung solche Wertungswi-

dersprüche verborgen bleiben. Wenn man es wie ich in Schleswig-Holstein darauf anlegt, Datenschutz und Informationszugang möglichst im Konsens zu realisieren, muss man an einer Vermittlung dieser Widersprüche besonders interessiert sein. Noch sehe ich keine Patentlösung, denn die Neuorganisation der behördlichen Informationssammlungen mit dem Ziel, Konflikte zwischen Datenschutz und Informationszugang möglichst von vornherein zu vermeiden, wird noch viele Jahre dauern, ehe sie wirksam wird.

Ebenso muss aber dafür gesorgt werden, dass im Überschwang des Informationszugangs nicht die datenschutzrechtlichen Standards abgesenkt werden. Bis dahin muss natürlich vermieden werden, dass der Datenschutz als Blockadeinstrument gegen Informationswünsche missbraucht wird. Vermutlich ist das Problem nur mit einer diffizil aufeinander abgestimmten Konvergenz von Datenschutz und Informationszugang zu lösen. Man sollte die damit verbundene Feinarbeit nicht unterschätzen. Es ist aber notwendig, hier zu befriedigenden Ergebnissen zu kommen. Denn es ist nicht immer einfach zu vermitteln, dass Datenschutzbeauftragte, die gestern noch für eine strikte Abschottung personenbezogener Daten waren, heute vermeintlich die Herausgabe solcher Daten an jedermann ohne Erforderlichkeit und Zweckbindung goutieren.

VI. Der weiße Fleck: Die Geheimdienste

Wieviel Informationsfreiheitsgesetze wirklich wert sind, kann man daran messen, ob sie Zugang zu Informationen auch dort gewähren, „wo es wehtut“. Ich meine damit diejenigen Teile der Staatsverwaltung, die traditionell dem Blick des Publikums entzogen sind: Polizei und Geheimdienste. Hier kommt es sozusagen zum Härtetest, weil staatlicher Geheimhaltungswille und die Neugier der Bürger direkt aufeinanderprallen.

Was die Polizei angeht, so lösen die Informationsfreiheitsgesetze das Problem dadurch, dass sie die Strafverfolgungsbehörden generell von der Anwendung des Gesetzes freistellen. Für den Bereich der Gefahrenabwehr gilt dies nicht, so dass insoweit im Prinzip die Informationsfreiheitsgesetze zur Anwendung kommen. Die besonders interessante sog. vorbeugende Bekämpfung von Straftaten un-

terliegt damit dem Informationsfreiheitsgesetz, je nachdem, ob sie zur Strafverfolgung oder zur Gefahrenabwehr gerechnet wird.

Über die Geheimdienste schweigen sich die Gesetze bzw. Gesetzentwürfe in der Regel aus. Allerdings kann nach dem Brandenburgischen Informationszugangsgesetz der Antrag auf Akteneinsicht abgelehnt werden, wenn „Belange der inneren Sicherheit“ beeinträchtigt würden. Eine ähnliche Formulierung findet sich in Schleswig-Holstein. Das Berliner Informationsfreiheitsgesetz scheint das Problem zu ignorieren. Erst ein Blick in das Verfassungsschutzgesetz offenbart, dass der Verfassungsschutz aus dem Anwendungsbereich des Informationsfreiheitsgesetzes vollständig herausgenommen ist. Nach dem Bundesentwurf für ein Informationsfreiheitsgesetz sollen die Geheimdienste des Bundes nicht von vornherein aus dem Geltungsbereich des Gesetzes ausgenommen sein. Zwar enthält insbesondere § 3 des Entwurfs eine Reihe von einschlägigen Ausnahmebestimmungen zum Schutz von „Gemeinwohlinteressen“. Etwaige Informationsersuchen müssen aber im Einzelfall unter einen der Tatbestände subsumiert werden, eine pauschale Informationsverweigerung kommt nicht in Betracht.

Alles in allem – sieht man einmal von der Berliner Radikallösung ab – steht die Vorenthaltung geheimdienstlicher Unterlagen auf relativ allgemein formulierten Füßen. Zwar hat das Bundesverfassungsgericht in seiner jüngsten Entscheidung zu § 99 VwGO Gesichtspunkte wie „Wohl des Bundes oder eines Landes“ oder „Unterlagen, die ihrem Wesen nach geheimgehalten werden müssen“ als „legitime Anliegen des Gemeinwohls“ bezeichnet. Aber gerade in dieser Entscheidung sind auch die Wege für eine effiziente gerichtliche Nachprüfung der Anwendung dieser Begriffe verbessert worden.

Mir ist bislang noch nicht bekannt, ob bereits Informationszugangsansprüche an die Geheimdienste gestellt worden sind. Einen Versuch wäre es immerhin wert. Vor allem nach Inkrafttreten des Bundesinformationszugangsgesetzes wird sich die Frage stellen, inwieweit etwa Unterlagen des Verfassungsschutzes aus den ersten Jahrzehnten der Bundesrepublik offenbart werden müssen. Wir erleben ja gerade, wie sozusagen der „Unrechtsteil“ dieses Abschnitts der deutschen Geschichte im Wege des Stasi-Unterlagen-Gesetzes der Öffentlichkeit zugänglich gemacht wird. Es wäre

hochinteressant, im Vergleich dazu zu sehen, wie sich in jener Zeit der an Gesetz und Recht gebundene Verfassungsschutz verhalten hat. Aber das ist eine andere Geschichte, die kaum im Konsens oder gar als Service des Verfassungsschutzes zu lösen sein wird.

VII. Abschluss

Ich wollte mit dem Ausflug in das Geheimdienstmetier nur zeigen, wie spannend der Informationszugang auch sein kann. Welche Möglichkeiten sich hier gerade in traditionellen Geheimbereichen auftun, ist vermutlich noch gar nicht überall bedacht. Vielleicht fehlt uns in Deutschland auch ein Stück weit jener investigative Journalismus, den wir aus den USA kennen und der sich vornehmlich für solche Themen interessiert, die der Staat gerne geheimhalten möchte oder zumindest früher einmal streng geheimgehalten hat.

Zugleich wollte ich mit diesem Beispiel dokumentieren, dass mir sehr wohl bewusst ist, dass sich nicht alle Fragen beim Informationszugang im Konsens und als gern erbrachter Service der Verwaltung lösen lassen. Mir ist ebenfalls klar, dass man die Informationsfreiheit als ein Recht der Bürger und nicht als eine Huld der Verwaltung begreifen muss. Dieses Recht muss nötigenfalls auch, mit Hilfe der Informationszugangsbeauftragten oder der Gerichte durchgesetzt werden. Ich wollte nur dafür plädieren, es zunächst im Guten zu versuchen. Es macht keinen Sinn, die Verwaltung von einem Tag auf den anderen zu überfordern. Und ich wollte darauf aufmerksam machen, dass in der Verwaltung zunehmend eine Denkweise anzutreffen ist, die Informationszugangsrechte der Bürger keineswegs als reine Bedrohung empfindet. In diesem Sinne scheint es mir den Versuch Wert, Informationszugang auch als Service der Verwaltung zu interpretieren.

Dr. László Majtényi
First Parliamentary Commissioner for Data Protection and Freedom of Information in the Republic of Hungary

Freedom of Information, the Hungarian Model

1. The notion of freedom of information means that we have the right to get to know information of public interest, that we have the right to inspect official documents. The State, sustained on our own taxes, cannot hide its operations from society. *The shared purpose of data protection and freedom of information is to continue maintaining the non-transparency of citizens in a world that has undergone the information revolution while rendering transparent of the state.*

The principles of freedom of information habitually have their origins ascribed to the ideas of the Enlightenment. However, its first legal source can be found not in the French or American Enlightenment but in Sweden, which was the first country in the world to recognize, in the *Act of Freedom of the Press of 1766*, that every citizen has the right to inform himself on official documents (undoubtedly, this became possible for the sole reason that between 1718 and 1772 Sweden was under parliamentary rule with rivaling parties).

The 14th point of the human rights declaration of the French Revolution announced the transparency of the state's economic management: *"citizens have the right, exercised in person or through representation, to inspect and consent to the necessity of spending public funds and to control the ways in which those funds are put to use..."* It is not difficult to hear the same maxim behind the famous demand of the citizens of the British colonies in North America: *"No taxation without representation." One may perhaps reasonably paraphrase this as "No taxation without information on how those taxes are used."*

In constitutional history, the idea of freedom of information reaches much further back than that of data protection, which did not emerge until quite late in the millennium. Enacted in 1766, the first

freedom of information law seems to have the advantage of two centuries. And yet we must, no matter how strange that may seem, talk about a global deficit of disclosure in the world regarded as civilized. Remarkably, privacy and data protection laws tend to be much more elaborate than freedom of information legislation.

Of course, the meaning of freedom of information, embryonic or full-fledged, is the right to somehow access files of public interest kept by the government. Nonetheless, one often encounters the term used to signify the unimpeded flow of information among countries; sometimes it is equated with the freedom of opinion,[1] publicity, or the freedom of the press. Although the democracies of the world, especially of the Old World, have not really exerted themselves to recognize freedom of information,[2] most European countries today protect this value on the general level, or at least through sectoral regulations (e.g. environmental data).

The first time the Parliamentary Assembly of the Council Europe addressed the issue, it moved rapidly to adopt Recommendation 854 (1979) on the disclosure of government documents and on freedom of information. With gross inaccuracy, the Recommendation handles the access to official documents together with the individual's right to inspect government files maintained about his or her person. Once again, what becomes blurred is the distinction between freedom of information and data protection. The Recommendation affirms that no parliamentary democracy can function without properly informed citizens and elected representatives. Except for a few types of documents, it is desirable to make all government files subject to disclosure, if only as "a useful measure against corruption and the waste of public funds."[3]In other words, taxpayers are entitled to be informed about how their money is spent.

---

1 Even in Sweden, it is referred to as *offetlighetsprincip*, or "the publicity principle."

2 Freedom of information laws were adopted early on by Finland (1951), the US (1966), France (1978), The Netherlands (1978), Canada (1983), Australia (1983), and New Zealand (1983). Since then, many countries have incorporated freedom of information at least in their constitutions, from Russia to Macedonia and Georgia. Poland and Hungary, two good friends, both enshrined this liberty in § 61 of their respective constitutions.

3 Recommendation, clause 5.

2. One of the most important purpose of the rule of law revolution is to guarantee the right of everyone to exercise control over his personal data and to have access to data of public interest in Hungary.

I believe that either and each of these two rights in itself may easily lead to a curtailment of freedom and that it is not only preferable to combine them as such in one Act but even that we place ourselves in the care of a joint protector. Besides general considerations, as we make the transition from a totalitarianism to a constitutional state founded on the principles of liberty, we have an especially good reason to grant equal and concurrent representation to freedom of information and informational self-determination founded on the notion of inviolable of privacy – if we do not, we will make it all the more difficult to face the past. But if we do, society will have a chance not only to get the informational redress that it rightfully demands but also to avoid a tyranny of freedom.

The model of informational rights in Hungary can be best appreciated as a follower of the Canadian model. Beside Canada, Hungary is unique in the degree to which the protection of personal data within its borders is linked with the constitutional values of freedom of information[4]. In Europe, Hungarian legislation stands alone in having opted for the rather common-sense solution to enact a single law to regulate freedom of information in conjunction with the protection of personal data. Here it must be pointed out that exemplary European democracy, such as Germany[5], are still merely planning to pass their own comprehensive federal level freedom of information law. Again pioneering in Europe, the Hungarian Act has assigned the protection of freedom of information and of personal data to the very same specialized ombudsman[6]. While privacy and

---

[4] See DP&FOI Act No. 63 of 1992 and the commentar of that law in The Globaal Encyclopaedia of Data Protection Regulation, Country Reporter László Majtényi, Kluwer Law International 90Yag00022

[5] See the Brandenburg case: Alexander Dix: The influance of Hungariaan Freedom of Information legislation in abroad – The Brandenburg example and experiance, The Door Onto the Other Side, Budapest, 2001

[6] The other examples for integrated approach: Québec, Solothurn (Swiss Canton), and newly Brandenburg (Akteneinsichts- und Informationszugangsgesetz, 1998, Land Berlin and Schleswig-Holstein and in the United Kingdom has changed the function of the Data Protection Registrar to the Information Commissioner with the entry into force of the British Freedom of Information Act (2000).

freedom of information are complementary imperatives, they also impose limits upon each other. Suffice it to mention the limited privacy protection enjoyed by those who hold public office or assume a public role.

The Hungarian freedom of information law can be described as radically liberal legislation, a fruit ripened by the 1989 rule of law revolution which created the constitutional state. As such, the Act is a firm refutation of the single-party power structure which for decades used secrecy as the very foundation it was erected upon.

The obligation to safeguard freedom of information extends to cover the entire Hungarian state administration from the lowest ranks to the highest levels of state power – both horizontally and vertically. Each state-wide or local governmental body, public organization or person is under legal obligation to disseparate data of public interest in its possession. (It is an interesting but not widely known fact that the law of the United States – a nation justly regarded as the yardstick of freedom of information – makes only *government agencies* liable to supply information, which means that the freedom of information principle does not apply to documents controlled, say, by the President.) Freedom of information is a human rather than a civil right, and therefore it also accrues to other than Hungarian citizens.

The Data Protection and Freedom of Information Act (DP&FOIA) of Hungary defines what it calls “data of public interest” *via negativa*, that is by saying what freedom of information is *not*. To risk an exalted exaggeration, one could say that this generous definition in effect creates for freedom of information a veritable legal universe of its own, even though its application can be very problematic and it often makes life difficult for practitioners. In this definition, then, “‘data of public interest’ means any information under processing by an authority performing state or local self-government functions or other public duties, except for personal data.”[7]For all its appeal in terms of the regulatory philosophy behind it, this wording creates a complicated situation in the legal technical sense by only exempting personal data. For instance, under this definition state secrets

[7] DP&FOIA, § 2, clause 3.

would qualify as data of public interest, except that access to them is prevented; in fact, even business secrets acquired by a public authority would literally exhaust these criteria.

Under the DP&FOIA, "the person or body performing state or local self-government functions or other public duties [...] shall, within its sphere of competence, including its management, promote accurate and prompt information for the general public."[8] Government authorities are required to regularly publish information of public interest, including about their competence and powers, organizational structure, operations, and the types of information processed by them. The name and rank of officials acting on behalf of the public authority are subject to disclosure, and the interests of protecting their personal information may not restrict access to data of public interest. Data of public interest must be made known to anyone.

Consistently and correctly, the Hungarian Constitutional Court has discussed freedom of information as one of the communication rights, regarding the freedom of opinion as the "mother" to them all.[9]To support this approach, the Court has no lesser authority to invoke than that of § 10 of the European Convention of Human Rights. I believe, however, that it would be rather difficult to deduce freedom of information from the concept of freedom of opinion. I think that the historical link between the two liberties is entirely different from the logical relation between them. A historic angle may verify the above approach–the one followed by the Convention– simply because of the chronological precedence of freedom of opinion as a recognized right. (It may appear to be a mere matter of arbitrary convention which of the two rights we define as part of the other, but a distinction is indeed necessary if we are to grasp the relationship between data protection and freedom of information.) However, the situation is just the reverse from the point of view of logic, and of the cognitive process in which we arrive at an opinion. In this sense, freedom of information comes before the freedom of opinion, just as information comes before opinion itself. Freedom of information is then a precondition for the freedom of opinion, rather than the other way round. This view is approximated by the Hungarian Constitutional Court in its preamble to Resolution 37/1992,

---

[8] § 19 (1).

[9] Cf. for instance Resolution 30/1992 (V. 26.).

when it says that “The material and procedural guarantees for the right to be informed, that is for the freedom of information, are mainly constructed by the state elsewhere [*that is, not in regulating the freedom of the press–L. M.*], namely while regulating access to information by anyone in general rather than by the media in particular. Democratic public opinion is inconceivable without full and objective disclosure of information.” All I could add to this–not by way of criticism so much as to remind us of the structural complexity of freedom of information–is that the disclosure of data of public interest is more than the right to be informed,[10] simply because it presupposes activity on the part of government.

One of he special features of Hungarian constitutional law in that it employs a rigorous dichotomy between personal data and data of public interest. While this distinction obviously has its benefits, it certainly leads to difficulties that even the Constitutional Court has not always been able to solve in a reassuring manner, as we will see shortly. In many cases, the pitfalls of interpretation can be best bridged by differentiating, as the DP&FOIA does, between data of public interest on the one hand, and public data on the other. In this approach, data of public interest are subject to disclosure as the main rule, while personal data are governed by the principle self-determination. At the same time, some personal information may also be public, and data of public interest may become confidential if so ordered by law for reasons justifiable by the Constitution. This makes it impossible to equate the Hungarian notion of “data of public interest” with the usual concepts of “public data” or “public information,” and in this the Hungarian legal system clearly departs from the international main stream. Lumping together *everyone’s* personal data also threatens–at least theoretically–to empty the category of data of public interest, simply because every manifestation of state power is the work of human beings. The DP&FOIA seeks to neutralize this threat by providing that “Access to data of public interest may not be restricted to protect those data of a person acting on behalf of the authority which are conjunctive to his or her duty.”[11]

---

[10] This of course makes it problematic to group it among the freedom rights (even though it is clearly a liberty regarding its essence), and also questions its status as an “inexpensive right” to provide.

[11] § 19 (4).

Under Hungarian law, any information that is not personal in nature and is controlled by a state or local government authority must be considered data of public interest. Access to data of public interest is not subject to any restrictions except by legally defined categories of secrecy (e.g. bank or insurance secrets, or confidential health-related information).

3. Freedom of information is limited in several ways. Access to data of public interest is restricted by the data protection act itself as a means of protecting personal data. I will not discuss the conflict between personal data and data of public interest. Basically adopting the ruling of the Council of Europe's Convention, the Act on Data Protection (*DP&FOI Act*) permits the restriction of the right to publicity by order of the law for the following categories of data: restriction is allowed in the interest of national defense, national security, criminal investigation and prevention of crimes, the monetary and currency policy of the State, foreign and international relations, and of judicial procedure. In the sphere between the protection of personal data and state secrets, several categories of secret are identified and mostly regulated by law.

Both European law and national legislation such as the Hungarian Act on the protection of personal data and on the publicity of data of public interest grant an exception from the principle of the publicity of files for the category of draft documents used internally and in preparing decisions. The explanation for this lies in the fact that the exclusion of publicity from the decision-making mechanism could be justified no matter how democratically it is run by the administration. Decision-making processes cannot be exposed to the pressure of public opinion at every step of the decision-making procedure.

Governments forced to make unpopular decisions have an appreciable interest in being able to consider undisclosed plans. The disclosure of preliminary drafts not yet given professional shape could make the office look ridiculous even if has not actually done anything worthy of such reaction. If contradictory alternatives come to light the official hierarchy could be undermined. For all these reasons, the restricted publicity of such documents represents a tolerable limitation. Hungarian law declares that *"Unless otherwise provided by law working documents and other data prepared for the*

authority's own use or for the purpose of decision making are not public within 30 years of their creation. Upon request the head of the authority may permit access to these documents or data." By contrast, we have good reason to object to the time period established for the restriction of disclosure of documents used internally and in preparing decisions, which is *thirty years* by effective Hungarian law. This is too long, especially when consider that the longest expiration period of official secrets is *twenty years* only despite the fact that an official secret, as opposed to a document used in decision making, constitutes a "true" secret.

Enjoying the highest level of protection are the secrets of the State, which have been subjected to rigorous–but arguably not the most stringent – legal limitations in terms of procedure and substance (Act No. LXV of 1995). The Secrecy Act provides for two cases of secrecy law.

Data constitute a state secret when they belong to a category of data defined within the range of state secrets, and when, as a result of the classification procedure, the classifier has determined beyond doubt that their *"disclosure before the end of the effective period, their unrightful acquisition or use, their revelation to an unauthorized person, or their withholding from a person entitled to them would violate or threaten the interests of the Republic of Hungary in terms of national defense, national security, criminal investigation and prevention of crimes, the monetary and currency policy of the State, foreign and international relations, or in terms of jurisdiction."* The effective period for the category of state secrets is maximum 90 years.

Official secret means any data whose *"disclosure before the end of the effective period, unrightful acquisition or use, or access by an unauthorized person would interfere with the orderly operation of a body fulfilling a state or public function and would prevent it from exercising its official function and authority free from influence."*

After requesting the Data Protection Commissioner for an opinion, the person authorized for the classification will publish the register of official secret categories in the *Magyar Közlöny ("Hungarian Bulletin")*. Data qualifying as a state secret or an official secret have to

be classified. If the data meet substantive requirements but for some reason have not been classified, they cannot be considered a state or official secret.

Upon request, the classifier controlling the secret may grant the permission to access the data. The petition to access is governed by the same rules and are subject to the same restriction periods that we have already explained in the context of data of public interest. If the request is refused, the classifier can also be sued as provided by *DP&FOI Act.*

Requests for data of public interest must be complied with in 15 days, and any refusal to supply such information must be communicated to the applicant within eight days, together with an explanation. Controllers of data of public interest are under obligation to inform the public periodically anyway. Whenever a request for information is denied, the applicant has the option to file for an inquest by the Commissioner for data protection and freedom of information, or to bring a court case. Such cases will be heard by the court with special dispatch, and the grounds for withholding information must be proved by the party refusing to give out the data.

Should the same plaintiff seek help from the DP&FOI ombudsman, he can count on a procedure that is substantially speedier and definitely free of charge. The ombudsman will issue a recommendation in the case, which is not officially binding, but will be obliged as a rule.

These considerations notwithstanding, Hungarian law provides for an exception that is unheard of in other countries. Whenever the Commissioner for DP&FOI finds that a classification as state or official secret is without grounds, he is entitled in his recommendation to call on the classifier to alter the classification or to abolish it altogether. Such a decision empowers the "recommendation" with administrative force, leaving the addressee with the option to concede or to file a lawsuit against the Commissioner, requesting the court to uphold the classification. Such cases will be heard by the County Court at special dispatch. It is noteworthy that to this date we haven't had a classifier risk a court procedure instead of bowing to the Commissioner's judgment.

And yet, law is not just mere normative form but also social reality. The Commissioner not only watches over freedom of information, but also lobbies for its recognition. To some extent, the institutions created to safeguard constitutional rights have the power to generate the very social demand to have these rights enforced. Legislators are mandated to submit bills with an impact on informational freedom rights to the DP&FOI Commissioner for evaluation, although they are not bound by law to accept the Commissioner's recommendation. This authority is an important tool in the hands of the freedom of information Commissioner, enabling him to shape the legal environment. And yet, we must give some credit to the voices which claim that freedom of information in Hungary – as in many other places of the world – generates more smokescreen than real flame. The statistics in the Commissioner's reports, submitted annually to Parliament, lend themselves to forming a social diagnosis. Hungarians –certainly like other peoples in East Central Europe – have traveled a unique road to civil society, and age-old habits and traditions are not easy to change. Staunch believers in the aphorism "*My house is my castle*," Hungarians tend to be much more sensitive to violations of their privacy than to secrecy over data of public interest. The ancient Latins who grew indifferent to an increasingly corrupt public sphere summed up their wisdom in the advice *"Go not to the Forum, for truth resides in your own soul."* Many in Hungary today subscribe to this view; we can draw a measure of comfort from the exceptions. At any rate, the Commissioner's case statistics provide valuable lessons. While the number of cases investigated by the Commissioner has been changing dramatically, the respective representation of the various informational branches show great consistency. Since 1995, when the Bureau was set up, the number of investigations has multiplied to reach a thousand in a single year. Most of them pertain to data protection, with only 10 percent concerning freedom of information issues. In terms of complaints filed, the share of freedom of information cases is only 7 percent. True enough, statistical figures add their own distortion. Matters involving freedom of information are typically high-profile cases receiving keen social attention and wide publicity. As such, their significance far outstrips their share in the total number of cases investigated.

Freedom of information has been accursed, perhaps because it so often threatens the powers that be which like to represent their interests as the *raison d'être* of the state.

Let us finally recall a word of warning by David Flaherty, the widely respected authority who served, until recently, as Information and Privacy Commissioner for the Province of British Columbia. Writing for a Canadian audience in praise of the Hungarian practice, Mr. Flaherty cautions that information rights will be always beset by the enemies of freedom, old and new.[12]

At last I quote one of the interesting cases of the Hungarian DP&FOI Commissioner which was not accepted by the titled government.

Recommendation concluding the Data Protection Commissioner's inquiry into records taken at government sessions, and the storage and publicity of the documents

I.

Having received a number of petitions in the matter, I brought an investigation into the practices of documenting the sessions of the Government of the Republic of Hungary, including the issue of storing and disclosing the documents. Some of the petitions criticized the practices followed from 1994 to 1998, objecting to the routine of the government – in violation of Hungarian archival law – to destroy subsequently audio tapes recorded at the cabinet's sessions. The petitions inquired about the rules applying to government session records, and whether these rules were in harmony with the relevant legislation in force, namely with Act LXVI/1995 on Public Documents, Public Archives, and the Protection of Private Archival Material (the Archives Act or AA); with Act LXIII/1992 on the Protection of Personal Data and the Disclosure of Data of Public Interest (DP&FOIA); with Act LXV/1995 on State Secrets and Office Secrets

[12] *Commissioner' Message*, Annual Report 1996-97, Office of the Information and Privacy Commissioner.

(the Secrets Act or SA); as well as with internationally accepted norms and local customs.

Another petition raised the question whether the modifications in the rules, effected in June 1998, did not do irreparable harm to the right to access data of public interest, in view of the fact that the Rules of Procedure of the Government currently in force do not require either audio or verbatim written records to be taken at cabinet sessions.

Since the petitions all concerned much the same topic, I examined their proposals together in my investigation.

II.

The history of documenting government sessions offers interesting clues as to the legal view taken of the issue.
According to the General Director of the National Archives of Hungary, the institution keeps documents pertaining to the governments and councils of ministers in power in 1948-49, between 1867 and 1944, and between 1944 and 1983. Unfortunately, the 1948 minutes had been taken in a single copy, only to disappear soon afterwards, in December of the same year. There was only one finalized copy, dated 2 May 1849, which later surfaced in the original version. The current holdings of the National Archives pertaining to government sessions consist of copies, excerpts both certified and uncertified, and drafts. About 95% of the records taken at government sessions between 1867 and 1945 are in fact condensed, abstracted renderings of the contributions, comments and proposals voiced by the cabinet members.

Under the provisions of the AA, these records are open to free research; in fact, they invite nearly a thousand applications a year by researchers wishing to study them. Following the earlier traditions, the records taken at government sessions after 1945 only offer abridged summaries of the officials' comments. These documents, too, are open to general research.

The changes in administrative practices regarding the documentation of the sessions and the storage of the documents can be traced clearly in the alterations in the rules of procedure followed by the various governments in power since 1990. Issued in the form of government decrees, these often modified and amended rules of procedure decide the ways and means of documenting government sessions at any given time.

The cabinet that had risen to power in the wake of the free parliamentary elections of 1990 enacted provisional rules of procedure, issued in Government Decree 1006/1990 (VII. 17), which made it mandatory to prepare verbatim minutes of the sessions, as well as a summary. About two years later, Government Decree 1025/1992 (V. 5) abolished the requirement for verbatim records, leaving the task of documenting government sessions to the Administrative State Secretary of the Prime Minister's Office, who was appointed to compile a condensed version of the proceedings.

The Rules of Procedure were then modified once again by the new government brought to power at the 1994 elections. Paragraph 83 of Government Decree 1088/1994 (IX.20) mandated summaries and audio recordings to be made of government sessions. Under paragraph 88 of the same Decree, the originals of the summaries, together with any and all appendices, as well as the audio tapes, were now to be kept on file by the Prime Minister's Office; the handling of these documents, prohibited from being phased out or discarded, was made subject to the legal provisions governing archives, the protection of private archival material, state secrets and office secrets. Approximately ten months later, the stipulation of audio recordings was abolished again when the Rules of Procedure were modified once more in Government Decree 1070/1995 (VII.29).This meant that, when the issue was first proposed for a debate on the floor of Parliament and in the media in April 1996, the Rules of Procedure then in effect did not make it mandatory to make audio recordings of government sessions. However, not a month had passed after that before the government reinstated the requirement for audio tapes [Government Decree 1035/1996 (IV.24)].

These rules in turn were changed when the cabinet formed in 1998 effected yet another modification in the Rules of Procedure. The then adopted and still in force Government Decree 1090/1998 (VII.15) has resulted in the current situation in which neither audio recordings nor verbatim minutes are required at government sessions. In connection with the documentation of the sessions, the prevailing text of Government Decree 1088/1994 (IX.20), severally modified and amended as explained above, contains the following provisions:

"83. A summary shall be prepared of each Government session. The preparation of the summary, in five days from the date of the session, is the responsibility of the Administrative State Secretary of the Prime Minister's Office.

84. The summary of the Government session shall include a list of those present, the titles of the initiatives, the names of contributors, the fact and numerical distribution of votes if any, reference to any objections made by a cabinet member in exercise of his or her right to coalition approval, as well as the decision or resolution itself.

85. The summary shall be signed by the Prime Minister and the Administrative State Secretary of the Prime Minister's Office.

86. As an appendix to the signed summary, the following documents shall be also kept on file, in one copy each bearing an original signature:

a) initiatives;

b) decrees and resolutions;

c) proposals and their transcripts submitted to the Parliament;

d) guidelines and statements of position;

e) memoranda;

f) documents created in the process defined in paragraph 71;

g) resolutions issued during recess between two Government sessions;

h) reports sent to Cabinet members.

88. The original copy of the summary and its appendices shall be kept on file at the Prime Minister's Office; these documents may not be phased out or discarded, and their handling is subject to the legal provisions governing archives, the protection of private archival material, state secrets and office secrets.

89. The cabinet members, the permanent guests invited to the sessions of the Government, as well as the Administrative and Political State Secretaries, shall each receive a copy of the summary. Subject to the permission of the Administrative State Secretary of the Prime Minister's Office, other persons may also receive a copy of the summary."

Inquiring about the relevant practices prior to 1998, I asked the Administrative State Secretary of the Prime Minister's Office still holding an effective mandate to explain his position on the matter.

The reply came from the Deputy State Secretary of the Prime Minister's Office, who explained that, pursuant to Government Decree 1035/1996 (IV.24) which had modified Government Decree 1088/1994 (IX.20), the sessions were recorded on audio tape and in a written summary, filed by the Prime Minister's Office in its own archives. In accordance with the Government's Rules of Procedure, the Prime Minister’s Office applied to the handling of these documents the legal provisions governing archives, the protection of private archival material, state secrets and office secrets. The acute lack of shelf space in the National Archives of Hungary made it impossible to transfer the documents there in a timely manner and on a regular basis. Such transfers were made whenever the opportunity to do so was signalled in advance by the Archives.

Reflecting on the regulations which came into force in July 1998, the Minister without Portfolio heading the Prime Minister’s Office offered the position that no legal provisions stipulated the manner in which the sessions were to be documented or, for that matter, the

way in which the Government should operate as a body in general – save for the rules of delegating deputies for cabinet members. In tune with the general routine applied to official bodies, the regulation of such matters was within the Government's own sphere of authority. In the Minister's view, what really mattered in a government session were the resolutions and decisions that were made there. The process preceding such decisions could be traced clearly, given that both the summary and the documents in preparation for the decisions were available for posterity to scrutinize. The Minister explained his belief that freedom of information presupposed the public disclosure of decisions. The Government met this obligation in full by regularly publishing its decrees, resolutions, and legislative proposals submitted to the Parliament. To his knowledge, no other country at this time had in force a policy of making tapes or taking verbatim minutes at government sessions, and even summaries of content were not widely required elsewhere. In addition, the Government and the Prime Minister’s Office respected the provisions of the data protection and freedom of information law by informing the public, on a regular basis, of matters within its competence.

Currently, the Minister said, there were no guarantees that would preclude untimely access to the documents or their disclosure to the public. His position was that the government's decision to terminate the use of audio recordings – or the lack of verbatim or abstracted records of the proceedings at a session – did not violate the law, nor did it place freedom of information in jeopardy.

When on 10 December 1998, I held an inquiry on location in the Prime Minister’s Office, the head of the Office offered the following information on the prevailing policy of handling documents:

All initiatives prepared by the various Ministries for the meeting of Administrative State Secretaries preceding the actual cabinet sessions were labelled "Strictly confidential" ,"Confidential" or "Not public" .The latter classification – when the document lacks one at the time it is received at the Prime Minister’s Office – is stamped on the document by the Administrative Office staff. The initiatives are prepared in 90 copies, of which two are kept by the Administrative Office, and the rest are distributed to the participants. About the meeting of Administrative State Secretaries a memo is issued containing

the names of participants, the title and file number of the initiatives, and a brief summary of the opinions and comments contributed. In the upper right corner of the document there is a reference to section 19(5) of the DP&FOIA, followed by the inscription "'Not public' for 30 years". The documents of certain government sessions are classified by the Administrative State Secretary of the Office for 50 years as state secrets, without deliberating on a case-by-case basis.

III.

Democracies around the world employ various means to document the operation of their governments. Some countries insist on verbatim minutes, while others merely mandate summaries of content. Accordingly, there are as many ways to regulate the process of recording and the handling of the documents thus created. In certain countries, freedom of information is a constitutional right; in others it is a privilege guaranteed by law only; in several countries, which lack proper legal regulations on this count, the need for this freedom right is acknowledged and legitimized by custom and an unwritten constitutional code of values. In some places the preferred solution is to exempt a specified range of government papers from under the pledge solemnly that the affairs of the state will be conducted in full view of the public eye. The age of enlightened absolutism heralded a period in which the citizens' rights to exercise control over government have been gradually broadening, despite a number of setbacks in the process. This right also implies the publicity of the government's papers and of its operations. While the freedom of information legislation of Hungary – which refuses to place even the highest circles of the administration above the enforcement of this right – constitute some of the most radical laws ever enacted on the subject, the progress of international law has not yet reached the point where one could talk about the transparency of governments – which would certainly imply the imperative to fully document their activities – as the internationally expected norm. In summary, one can say that the democratic states have not yet evolved a standard that could serve as a yardstick for Hungarian regulations.

IV.

1. Article 61(1) of the Hungarian Constitution declares that "in the Republic of Hungary, every individual is granted the right to free expression, as well as to access and disseminate data of public interest." Article 8(2) states that "the rules of fundamental rights and obligations are set down in the law, which may not, however, restrict the essential content of these fundamental rights."

2. The most important laws with a bearing on the documentation of government sessions and the handling, storage, and publicity of those documents are: Act LXIII/1992 on the Protection of Personal Data and the Disclosure of Data of Public Interest (DP&FOIA); Act LXV/1995 of State Secrets and Office Secrets (SA); Act LXVI/1995 on Public Documents, Public Archives, and the Protection of Private Archival Material (AA).

- Pursuant to section 2(3) of DP&FOIA, "data of public interest means any information under processing by an authority performing state or local self-government functions or other public duties, except for personal data." According to section 19(3), "[the authority] performing state or local self-government functions or other public duties ... shall, within its sphere of competence, including its management, promote accurate and prompt information for the general public. [...] The authority shall grant access for anyone to data of public interest processed by it, except for those data which are classified as state or official secret by authorities entitled to do so under provisions of law, furthermore provided that right to access of certain data of public interest is not specifically restricted by law in the interest of national defence, national security, criminal investigation and the prevention of crimes, monetary or currency policy of the State, international relations and relations to international organizations, judicial procedure." Section 19(5) provides that "unless otherwise provided by law, working documents and other data prepared for the authority's own use, or for the purpose of decision-making, are not public within 30 years of their creation. Upon request, the head of the authority may permit access to these documents or data" prior to the deadline.

- Pursuant to section 6(1)(o) of the SA, "in their respective scope of responsibilities and competence, entitled to classify documents – of the types listed under clause 13 of the Annex – are the head of the Prime Minister's Office, the Political State Secretary of the Office, and the head of the body operating according to the Rules of Procedure approved by the Government." These types of document are the following: "Data created for internal use or in preparation for a decision by convening bodies set up by the Government or according to its Rules of Procedure, and, further, data created in the process of the operation of these bodies, as may fall under any clause of the List of State Secret Categories. The longest permitted period of classification as a state secret is 90 years."

- Section 5(1) of AA declares that "it is hereby forbidden by law to alienate, impair, or in any other way render unsuitable for use, public documents and archival material not qualifying as public documents but kept in a public archive; it is further forbidden to destroy such documents, except in a legally conducted procedure of discarding outdated papers." Under section 3(b), "'public document' means any document, regardless of the date of its creation and the location where it is stored, which belongs, or used to belong, among the archival materials of a body performing public duty." Section 12(1) provides that "save for the exceptions specified in paragraph (5), full and sealed annual volumes of public documents the disposal of which is forbidden shall be handed over to the competent public archives by the end of the fifteenth year from the calendar year in which the documents were created." Pursuant to section 12(5), "indisposable documents created over fifteen years ago which contain state or office secrets shall be handed over to the public archives in competence no later than by the end of the calendar year ending the classification period as determined by the classifier."

3. The matter under review is rife with the difficulties inherent in reconciling a number of mutually contesting constitutional rights and interests. The subsisting regulations must respect the constitutional right to access data of public interest. They must serve the cause of transparency in the work of the government, leave open the opportunity for the scholarly and scientific study of governments past or

present, and they must be conducive to the smooth operation of the administration free of undue influence. In this sense, we have no constitutional grounds to demand full publicity extending to the entirety of the government's activities, as a condition for the said smoothness of its operation.

The constitutional aspects of regulating freedom of information and secrets protection has been examined by the Constitutional Court (AB) in connection with a number of cases. Decision 34/1994 (VI.24) AB declared that the access to information and its free flow were especially vital with regard to the transparency of executive power and the bodies of government. The disclosure of data of public interest and free access to them often stand as the preconditions for the exercise of the right to free expression. A similarly coherent relation obtains between freedom of information and of scientific knowledge, and, in turn, between the freedom of research and of teaching. Because such information, especially when it is stored in archival materials and documents, is often accessed and obtained in the course of research that is typically scientific or scholarly in nature, by guaranteeing free access to information the Constitution indirectly ensures and protects the freedom of scientific knowledge of the given subject.

The disclosure of data of public interest is a fundamental proof for the existence of the democratic state under the rule of law which is declared in Article 2(1) of the Hungarian Constitution. The significance of this was recognized in the Council of Europe's 1982 Declaration on the Freedom of Information, when it affirmed the goal of the member states to follow an informational policy of openness in the public sphere – including one of allowing access to information – in order to help their citizens better understand political, social, economic and cultural issues, and to improve their skills in freely discussing such topics. [clause 8(II)(c)].

Nevertheless, the publicity of data of public interest and the right to free research both encounter constitutional limits in those provisions of secrecy which comply with legal requirements and the rules governing the restriction of constitutional rights.

The Constitutional Court pointed out that the right to access data of public interest had to be given heightened protection by the Constitution, even among all the clearly spelled out basic communicational rights, as one of the conditions for free speech. What this means is that laws placing a restriction upon the freedom of information must be interpreted restrictively in their turn, because freedom of information and the transparency and accountability of the state as the public executive power are prerequisites for exercising criticism and the right to free speech [Decision 34/1994 (VI.24) AB].

V.

The smooth operation of the administration free of undue influence would be thwarted if the law prescribed full publicity for the sessions of the government. Therefore, far from being illegal, placing temporal restrictions upon the freedom of information can be constitutionally well-founded when such restrictions are motivated by the above purpose. It could not properly be regarded as a constitutional exigency to prepare full documentation of government sessions – that is verbatim minutes, audio- and/or videotapes. The manner in which the sessions are to be documented can be legislated in several ways. The thing to keep in mind is that the Government is not a congregation of private individuals but rather a body of officials which plays a crucial role in the system of political institutions. On account of its prominent legal and political position, it is indispensable to have its activities documented, not simply to the extent of publishing its resolutions, but in terms of content and substance. In this light, Government Decree 1090/1998 (VII.15) clearly broke with the traditions of 1848 which had held sway for a century and a half.

In a series of Decisions, the Constitutional Court held that the restriction of fundamental rights could not be considered lawful unless it could be verified that the restriction was both necessary for and proportional to its admitted purpose. Immobilizing the right to access data of public interest by way of ensuring the smooth operation of the administration free of undue influence is not a measure that can reasonably be regarded either as necessary or proportional. The provisions of the SA and the DP&FOIA currently in force concerning the protection of state secrets, office secrets and docu-

ments for internal use or for the preparation of a decision, were worded in a way that respects the above considerations even as it basically serves other interests. When restricting a constitutional right, the State cannot use as the starting point the fact that rights can not only be used, but abused as well – for instance, when the current government has been replaced by another. When the existing legal guarantees are found insufficient, there are lawful means to try and incorporate further assurances into the law. For instance, it could be recommended that the rules governing the documentation of government sessions be included among the laws that need a two-thirds voting majority to pass. But regulating the issue on a constitutional level would not be inconceivable either.

VI.

The classification for a specified period of time of data of public interest controlled by the bodies of the government as a state or office secret can be regarded as a temporal restriction imposed upon freedom of information. As it has been suggested by the Constitutional Court, it is a flaw of the Hungarian Constitution itself that it fails to define the secrets of the State as a barrier erected before the access to data of public interest.

Section 3(1) of the SA states that "a state secret constitutes data belonging to the category of data types indicated in the Annex of the present act (henceforward referred to as the category of state secrets) about which the classifier has established that publication before the expiry of validity and unauthorised acquisition of use, delivery to an unauthorised person and lack of access by an authorised person would no doubt damage or jeopardise the interests of the Republic of Hungary related to defence, national security, criminal investigation and criminal prevention, central finance and exchange policy, foreign affairs, international relations and judicature."

Section 13 of the Annex to the SA, quoted earlier in the context of government sessions, limits the types of documents that can be legally classified as state secrets to data prepared for the internal use, or in preparation for a decision, by bodies established by the Government and in accordance with its Rules of Procedure, as well

as those data arising from the operation of the Government and these bodies that are mentioned in the list of state secret categories.

It follows from this that the routine of classifying as state secrets, without due deliberation on a case-by-case basis, the so-called summaries prepared at government sessions as mandated by the relevant Government Decree is legally unjustifiable in the current situation.

Of all the information emerging in government sessions, only those data may be legally classified – in a process respecting the provisions of the law – that are featured in the list of state secret categories in the Annex to the Secrets Act.

VII.

Based on section 25 of Act LIX/1993 on the Parliamentary Commissioner for Citizens' Rights, and section 23(2) of Act LXIII/1992 on the Protection of Personal Data and the Disclosure of Data of Public Interest, I advance the following Recommendation in the interest of furthering freedom of information:

- I call on the Minister without Portfolio heading the Prime Minister's Office and the Minister of Justice to propose an initiative for a legal regulation of documenting the substance of government sessions that would not only ensure the smooth operation of the Government free of undue influence but also guarantee the citizens' constitutional right to access data of public interest – granted that there may be delays in the enforcement of this right in individual cases;

- Documents classified in disregard of clause 13 of the Annex to Act LXV/1995 on State Secrets and Office Secrets cannot properly be regarded as state secrets, because they are not specifically identified as such in the list of state secret categories of the Secrets Act currently in force.

Gerhard Grill
Hauptverwaltungsrat, Büro des Europäischen Bürgerbeauftragten[1]

Zugang zu Dokumenten auf der Ebene der EU – aus der Praxis des Europäischen Bürgerbeauftragten

I. Amt und Aufgaben des Europäischen Bürgerbeauftragten

Das Amt des Europäischen Bürgerbeauftragten wurde durch den am 7. Februar 1992 in Maastricht unterzeichneten Vertrag über die Europäische Union geschaffen. Dieser Vertrag verfolgte bekanntlich unter anderem das Ziel, die Stellung der Bürger im europäischen Einigungsprozess und damit zugleich die Bürgernähe der europäischen Institutionen zu verbessern. So wurde insbesondere eine eigene Unionsbürgerschaft eingeführt (nunmehr Art. 17 ff. EG-Vertrag) und den Unionsbürgern das Recht eingeräumt, sich an den Europäischen Bürgerbeauftragten zu wenden (Art. 21 EG-Vertrag). Der Bürgerbeauftragte wird vom Europäischen Parlament für die Dauer von dessen Wahlperiode ernannt, übt sein Amt jedoch in völliger Unabhängigkeit aus (Art. 195 EG-Vertrag). Der erste Europäische Bürgerbeauftragte, Jacob Söderman, wurde im Jahre 1995 ernannt und 1999 vom neugewählten Europäischen Parlament für weitere fünf Jahre in seinem Amt bestätigt. Ein Stab von derzeit knapp 30 Mitarbeitern unterstützt den Bürgerbeauftragten bei seiner Arbeit[2].

Nach Art. 195 EG-Vertrag ist der Bürgerbeauftragte befugt, Beschwerden über Missstände bei der Tätigkeit der Organe und Einrichtungen der Gemeinschaft, mit Ausnahme des Gerichtshofs und des Gerichts erster Instanz in Ausübung ihrer Rechtsprechungsbefugnisse, entgegenzunehmen. Außerdem hat er das Recht, von sich aus Untersuchungen durchzuführen, wenn er Grund zu der Annahme hat, dass ein Missstand vorliegen könnte. Von zentraler Bedeutung für die Tätigkeit des Bürgerbeauftragten ist daher der Begriff

---

[1] Der vorliegende Beitrag gibt ausschließlich die persönlichen Ansichten des Verfassers wieder.

[2] Der Sitz der Einrichtung befindet sich in Straßburg; ein kleiner Teil des Personals arbeitet in einer in Brüssel angesiedelten Außenstelle.

des Missstands in der Verwaltung[3]. Da sich im EG-Vertrag keine Definition findet, sah sich der Bürgerbeauftragte mit der Notwendigkeit konfrontiert, den Inhalt dieses Begriffes selbst näher zu bestimmen. Nach der vom Bürgerbeauftragten bereits recht früh aufgestellten Definition liegt ein solcher Missstand vor, wenn eine öffentliche Einrichtung nicht im Einklang mit für sie verbindlichen Regeln oder Grundsätzen handelt[4]. Zu diesen Grundsätzen gehört – wie sich zeigen wird – auch der der Transparenz der Verwaltung.

Ergeben die Untersuchungen des Bürgerbeauftragten, dass ein Missstand vorliegt, so bemüht sich der Bürgerbeauftragte soweit wie möglich, zusammen mit dem betroffenen Organ oder der betroffenen Institution, eine Lösung zu finden, durch die der Missstand beseitigt und der Beschwerde abgeholfen werden kann[5]. Ist eine solche gütliche Lösung nicht möglich, kann der Bürgerbeauftragte dem betroffenen Organ oder der betroffenen Institution Entwürfe für Empfehlungen vorlegen und anschließend – insbesondere falls diese nicht befolgt werden – dem Europäischen Parlament einen Bericht unterbreiten, in dem Empfehlungen ausgesprochen werden können[6]. Der Bürgerbeauftragte hält sich allerdings auch für berechtigt, es in geeigneten Fällen bei einer kritischen Anmerkung bewenden zu lassen, in der das Vorliegen eines Missstandes konstatiert wird.

Die Zahl der vom Europäischen Bürgerbeauftragten zu bearbeitenden Fälle ist stetig im Steigen begriffen[7]. Seit der Aufnahme seiner Tätigkeit im Jahre 1995 wurden bereits weit über 8000 Beschwerden an ihn herangetragen.

---

[3] Die englische und die französische Fassung ("maladministration") bringen deutlicher als die deutsche Fassung zum Ausdruck, dass es sich um einen Missstand in der *Verwaltung* handeln muss. Für die Untersuchung politischer Missstände (so es sie in der EU denn geben sollte) ist der Bürgerbeauftragte daher nicht zuständig.

[4] Jahresbericht des Europäischen Bürgerbeauftragten 1997, S. 26.

[5] Siehe Art. 3 Abs. 5 des auf der Grundlage von Art. 195 erlassenen Beschlusses des Europäischen Parlaments vom 9. März 1994 über die Regelungen und allgemeinen Bedingungen für die Ausübung der Aufgaben des Bürgerbeauftragten, ABl. 1994 Nr. L 113, S. 15 (im folgenden "Statut" genannt).

[6] Siehe Art. 3 Abs. 6 und 7 des Beschlusses vom 9. März 1994.

[7] Die Zahl der neuen Fälle für die jeweiligen Jahre betrug 298 (1995), 845 (1996), 1185 (1997), 1373 (1998), 1582 (1999) und 1733 (2000). Im laufenden Jahr wurden bis Ende August bereits knapp 1300 Beschwerden registriert.

II. Transparenz und Zugang zu Dokumenten in der EU

Der Grundsatz der Transparenz im allgemeinen und der Möglichkeit des Zugangs zu Dokumenten im besonderen hat sich auf der Ebene der EU erst im Laufe der letzten Jahre durchzusetzen begonnen. Seine erste Anerkennung findet sich in der Erklärung Nr. 17, die der Schlussakte des bereits erwähnten Vertrages über die Europäische Union von 1992 beigefügt wurde und folgenden Wortlaut hat: “Die Konferenz ist der Auffassung, dass die Transparenz des Beschlussverfahrens den demokratischen Charakter der Organe und das Vertrauen der Öffentlichkeit in die Verwaltung stärkt. Die Konferenz empfiehlt daher, dass die Kommission dem Rat spätestens 1993 einen Bericht über Maßnahmen vorlegt, mit denen die den Organen vorliegenden Informationen der Öffentlichkeit besser zugänglich gemacht werden sollen.” Die Notwendigkeit, die Gemeinschaft transparenter zu gestalten, wurde bei den Tagungen des Europäischen Rates in Birmingham im Oktober 1992 und in Edinburgh im Dezember 1992 bekräftigt[8]. Auf der Grundlage entsprechender Vorarbeiten der Kommission einigten sich der Rat und die Kommission am 6. Dezember 1993 auf einen Verhaltenskodex für den Zugang der Öffentlichkeit zu Rats- und Kommissionsdokumenten[9].

Dieser Verhaltenskodex stellt folgenden allgemeinen Grundsatz auf: “Die Öffentlichkeit erhält möglichst umfassenden Zugang zu den Dokumenten der Kommission und des Rates.” Der Ausdruck “Dokument” bezeichnet dabei “unabhängig vom Datenträger jedes im Besitz des Rates und der Kommission befindliche Schriftstück mit bereits vorhandenen Informationen”.

Der Verhaltenskodex sieht weiterhin vor, dass der Zugang zu Dokumenten verweigert *wird*, wenn ihre Verbreitung folgende Interessen beeinträchtigen könnte:

- “- den Schutz des öffentlichen Interesses (öffentliche Sicherheit, internationale Beziehungen, Währungsstabilität, Rechtspflege, Inspektionstätigkeiten);
- den Schutz des Einzelnen und der Privatsphäre;

---

8 Bull. EG 10-1992, S. 9 und 12-1992, S. 7.

9 ABl. 1993 Nr. L 340, S. 41.

- den Schutz des Geschäfts- und Industriegeheimnisses;
- den Schutz der finanziellen Interessen der Gemeinschaft;
- die Wahrung der Vertraulichkeit, wenn dies von der natürlichen oder juristischen Person, die die Information zur Verfügung gestellt hat, beantragt wurde oder aufgrund der Rechtsvorschriften des Mitgliedstaats, der die Information bereitgestellt hat, erforderlich ist."

Ferner *kann* der Zugang verweigert werden, um den Schutz des Interesses des Organs in bezug auf die Geheimhaltung seiner Beratungen zu gewährleisten.

Der Verhaltenskodex sieht ein zweistufiges Verfahren vor: Anträge auf Zugang sind von den zuständigen Dienststellen innerhalb eines Monats zu beantworten. Wird der Antrag abgelehnt, kann ein Zweitantrag gestellt werden, der ebenfalls innerhalb eines Monats zu bescheiden ist. Beharrt die Behörde auf der Ablehnung des Antrags, muss der Antragsteller darauf hingewiesen werden, dass gegen diese Entscheidung Klage beim Gericht erster Instanz erhoben oder Beschwerde beim Europäischen Bürgerbeauftragten eingelegt werden kann.

Schließlich sieht der Verhaltenskodex vor, dass der Rat und die Kommission die zur Durchführung dieser Grundsätze erforderlichen Maßnahmen zu treffen haben. Der Rat hat daraufhin am 20. Dezember 1993 den Beschluss 93/731/EG über den Zugang der Öffentlichkeit zu Ratsdokumenten[10] erlassen, der die Bestimmungen des Verhaltenskodex wiedergibt. Eine in der Form (wenn auch nicht in der Sache) abweichende Gestaltung wählte die Kommission in ihrem Beschluss 94/90/EGKS, EG, Euratom vom 8. Februar 1994 über den Zugang der Öffentlichkeit zu den der Kommission vorliegenden Dokumenten[11], der auf den diesem Beschluss beigefügten Verhaltenskodex verweist. Sowohl der Beschluss des Rates (in seinem Art. 7) wie der Beschluss der Kommission (in seinem Art. 2)

[10] ABl. 1993 Nr. L 340, S. 43; geändert durch den Beschluss 96/705/EG, EGKS, Euratom des Rates vom 6. Dezember 1996 (ABl. 1996 Nr. L 325, S. 19) und den Beschluss 2000/527/EG des Rates vom 14. August 2000 (ABl. 2000 Nr. L 132, S. 9).

[11] ABl. 1994 Nr. L 46, S. 58; geändert durch Beschluss 96/567/EG, EGKS, Euratom der Kommission vom 19. Februar 1996 (ABl. 1996 Nr. L 247, S. 45).

enthalten die wichtige Ergänzung, dass ein Antrag als abgelehnt gilt, wenn innerhalb der jeweiligen Monatsfrist keine Antwort ergeht.

Zwei Punkte sind in diesem Zusammenhang hervorzuheben: Erstens weist bereits der Verhaltenskodex darauf hin, dass die besonderen Bestimmungen über das Recht auf Akteneinsicht von Personen, die daran ein spezifisches Interesse haben, von den hier behandelten Bestimmungen nicht berührt werden. Dies gilt zum Beispiel für das Recht eines Unternehmens, gegen das die Kommission wegen eines Verstoßes gegen die Wettbewerbsvorschriften der Art. 81 oder 82 EG-Vertrag eine Geldbuße verhängen möchte, Einsicht in die Verfahrensakte zu nehmen. Zweitens bestimmen die genannten Vorschriften, dass im Falle von Dokumenten, die sich im Besitz von Rat oder Kommission befinden, deren Urheber jedoch eine andere Person oder Einrichtung ist, der Antrag direkt an den Urheber des Dokuments zu richten ist.

Die genannten Beschlüsse des Rates und der Kommission stützen sich auf die Vorschriften des EG-Vertrags (nunmehr Art. 207 und 218), die diesen Organen erlauben, sich eine Geschäftsordnung zu geben. Die Niederlande klagten gegen den Beschluss des Rates vor dem Europäischen Gerichtshof. Sie vertraten die Auffassung, die vom Rat gewählte Rechtsgrundlage sei unzutreffend gewesen, da der Beschluss sich nicht auf eine interne Organisationsmaßnahme beschränke, sondern Außenwirkungen entfalte. Der Gerichtshof hat diese Klage zurückgewiesen[12]. Die Ausführungen, die der Gerichtshof in diesem Zusammenhang machte, sind von allgemeinerem Interesse. Der Gerichtshof wies darauf hin, dass das Recht auf Zugang zu Dokumenten im Recht der meisten Mitgliedstaaten allgemein als Verfassungs- oder Rechtsgrundsatz anerkannt werde. Auch auf der Ebene der EU zeige die Entwicklung “eine immer stärkere Betonung des Rechts des Einzelnen auf Zugang zu den Dokumenten, die im Besitz der Regierung sind”. Solange der Gemeinschaftsgesetzgeber jedoch insoweit keine allgemeine Regelung erlassen habe, müssten die Gemeinschaftsorgane die Maßnahmen, welche die Behandlung von Anträgen auf Zugang zu Do-

[12] Rs. C-58/94, Niederlande/Rat, Slg. 1996, I-2169.

kumenten betreffen, aufgrund ihrer internen Organisationsgewalt erlassen[13].

Bereits dieses Urteil zeigt sehr deutlich, dass der Gerichtshof davon ausgeht, dass das Gemeinschaftsrecht der Öffentlichkeit ein Recht auf Zugang zu Dokumenten im Besitz der Gemeinschaftsbehörden gibt und dass die genannten Beschlüsse des Rates und der Kommission dieses Recht lediglich ausgestalten. Die weitere Rechtsprechung des Gerichtshofes und des Gerichts erster Instanz bestätigt dies und zeigt, dass bei der Auslegung der konkreten Vorschriften der “effet utile” dieses Rechtes im Mittelpunkt steht.

So hat das Gericht entschieden, dass der Beschluss 94/90 zwar eine interne Organisationsmaßnahme darstellt, aber gleichwohl Dritten Rechte verleiht, welche die Kommission beachten muss[14]. Gleiches hat natürlich für den Beschluss des Rates zu gelten. Mit diesen Beschlüssen soll der Grundsatz eines möglichst umfassenden Zugangs der Bürger zu Informationen verwirklicht werden[15]. Ausnahmen von diesem Grundsatz müssen daher eng ausgelegt und angewandt werden, um die Anwendung des allgemeinen Grundsatzes nicht zu beeinträchtigen[16]. Während eine Freigabe eines Dokuments verweigert werden *muss*, wenn bestimmte Interessen verletzt werden könnten, *kann* der Zugang verweigert werden, um die Geheimhaltung der Beratungen von Rat und Kommission zu schützen. Die Verwaltung verfügt insoweit also über einen Ermessenspielraum. Sie ist damit aber zugleich verpflichtet, dieses Ermessen auszuüben und die widerstreitenden Interessen sachgerecht abzuwägen[17]. Wird der Zugang verweigert, muss das Organ diese Entscheidung so klar und eindeutig begründen, dass sowohl der Antragsteller als auch das Gemeinschaftsgericht die tragenden Gründe erkennen können[18].

---

[13] A.a.O. (Fn. 12), Rdnr. 34-37.

[14] Rs. T-105/95, WWF UK/Kommission, Slg. 1997, II-313 Rdnr. 55; Rs. T-124/96, Interporc/Kommission, Slg. 1998, II-231 Rdnr. 46.

[15] Rs. T-309/97, Bavarian Lager Company/Kommission, Slg. 1999, II-3217 Rdnr. 36.

[16] Urteil WWF a.a.O. (Fn. 14), Rdnr. 56; Rs. T-174/95, Svenska Journalistförbundet/Rat, Slg. 1995, II-2289 Rdnr. 110.

[17] Rs. T-194/94, Carvel und Guardian Newspapers/Rat, Slg. 1995, II-2765 Rdnr. 65ff.

[18] Urteil Interporc (I) a.a.O. (Fn. 14), Rdnr. 53.

Der Schutz der Rechtspflege (im Rahmen des Schutzes des öffentlichen Interesses) rechtfertigt eine Verweigerung des Zugangs nur dann, wenn das betreffende Dokument speziell für ein bestimmtes Gerichtsverfahren erstellt wurde[19].

Der Verhältnismäßigkeitsgrundsatz verlangt, dass Ausnahmen nicht über das zur Erreichung des verfolgten Ziels angemessene und erforderliche Maß hinausgehen. Betreffen die Bedenken gegen den Zugang zu einem Dokument daher nur einen Teil desselben, muss das Organ prüfen, ob Zugang zu dem verbleibenden Teil des Dokuments zu gewähren ist[20].

Der 1997 geschlossene Vertrag von Amsterdam hat den Grundsätzen der Transparenz und des Zugangs zu Dokumenten Eingang in die Gründungsverträge verschafft. Art. 1 Abs. 2 des Vertrages über die Europäische Union in seiner geänderten Form bestimmt nun, dass in der EU Entscheidungen "möglichst offen und möglichst bürgernah getroffen werden". Dem neuen Art. 255 Abs. 1 EG-Vertrag zufolge haben die Unionsbürger sowie alle Personen mit Wohnsitz oder Sitz in der EU "das Recht auf Zugang zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission". Die allgemeinen Grundsätze und Bedingungen für diesen Zugang sind mittlerweile in der auf der Grundlage von Art. 255 Abs. 3 erlassenen Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission[21] festgelegt worden.

Das Recht auf Zugang zu Dokumenten hat auch in die im Jahre 2000 aufgestellte Charta der Grundrechte der Europäischen Union[22] Eingang gefunden (Art. 42).

---

[19] T-92/98, Interporc/Kommission, Slg. 1999, II-3521 Rdnr. 40.

[20] Rs. T-14/98, Hautala/Rat, Slg. 1999,II-2489 Rdnr. 85 ff.; Rs. T-188/98, Kuijer/Rat, Slg. 2000, II-1959 Rdnr. 54 ff. Vgl. aber Rs. T-204/99, Mattila/Rat und Kommission, Urteil vom 12. Juli 2001, noch nicht in Slg., wonach das Recht auf teilweisen Zugang in besonderen Fällen verweigert werden kann, wenn seine Gewährung zu einem unangemessenen Verwaltungsaufwand führen würde (a.a.O., Rdnr. 68 ff.).

[21] ABl. 2001 Nr. L 145, S. 43.

[22] ABl. 2000 Nr. C 364, S. 1.

Es war nicht zuletzt dieser Umstand, der einen der Generalanwälte des Gerichtshofes bewogen hat, in seinen kürzlich verkündeten Schlussanträgen die Auffassung zu vertreten, das Recht auf Zugang zu Dokumenten stelle nunmehr ein Grundrecht dar[23].

III. Die Tätigkeit des Bürgerbeauftragten auf dem Gebiet des Zugangs zu Dokumenten

Zu den Grundsätzen, deren Einhaltung der Bürgerbeauftragte überprüfen kann, gehört somit auch jener der Transparenz. Der Europäische Bürgerbeauftragte hat denn auch mit einer Fülle von Fällen zu tun gehabt, in denen es um Transparenz im allgemeinen und den Zugang zu Dokumenten im besonderen ging. Nur die zuletzt genannten Fälle sollen hier erörtert werden.

Ich werde mich dabei auf Fälle beschränken, die anhand der Beschlüsse 93/731 des Rates und 94/90 der Kommission zu beurteilen waren. Eine wichtige Fallgestaltung des Zugangs zu Dokumenten, in der diese Normen keine Rolle spielten, soll aber gleichwohl kurz vorgestellt werden. Die Organe und Institutionen der EU rekrutieren ihre Beamten gewöhnlich durch Auswahlverfahren, die schriftliche Prüfungen umfassen. Viele Kandidaten, die an diesen Prüfungen scheitern, haben den verständlichen Wunsch, Einsicht in ihre korrigierte Prüfungsarbeit zu nehmen. Dieser Wunsch wurde von den Organen und Institutionen der EU jedoch in der Vergangenheit stets mit der lapidaren Begründung abgewiesen, die anzuwendenden Vorschriften[24] sähen vor, dass die Arbeiten des Prüfungsausschusses geheim seien. Es konnte daher nicht überraschen, dass dem Bürgerbeauftragten eine Vielzahl von Beschwerden gegen diese Praxis vorgelegt wurden. Die meisten dieser Beschwerden betrafen die Kommission. Der Bürgerbeauftragte leitete daraufhin eine Initiativuntersuchung[25] ein, in deren Verlauf er der Kommission vier Vorschläge zur Verbesserung der Transparenz ihrer Einstellungsverfahren unterbreitete. Die Kommission akzeptierte schließlich drei dieser Vorschläge, nicht aber den vierten, wonach Zugang zu den korrigierten Prüfungsarbeiten gewährt werden sollte. Der Bürgerbe-

---

[23] Siehe die Schlussanträge von Generalanwalt Léger in der Rs. T-353/99 P, Rat/Hautala, noch nicht in Slg., Ziff. 77 und 84.

[24] Art. 6 des Anhangs III des EU-Beamtenstatuts.

[25] Untersuchung 1004/97/(PD)/GG.

auftragte legte daher dem Europäischen Parlament am 18. Oktober 1999 einen Sonderbericht vor, in dem er auf seiner Forderung beharrte[26]. Anfang Dezember 1999 teilte die Kommission dem Bürgerbeauftragten mit, dass sie nunmehr auch diesen Vorschlag akzeptiere, so dass der Bürgerbeauftragte diesen Fall erfolgreich abschließen konnte.

Betrachtet man die bisher vom Bürgerbeauftragten behandelten Fälle, kann man vereinfachend feststellen, dass dort insbesondere drei Fragen geprüft wurden. Bereits sehr früh ging der Bürgerbeauftragte der Frage nach, ob überhaupt Vorschriften über den Zugang zu Dokumenten existierten. Sodann widmete er sein Augenmerk der Frage, ob die existierenden Vorschriften korrekt angewandt wurden. Schließlich prüfte der Bürgerbeauftragte, ob die Voraussetzungen für eine sinnvolle Ausübung des Rechts auf Zugang zu Dokumenten gegeben waren.

Vorschriften über den Zugang zu Dokumenten

Die bereits erörterten Beschlüsse 93/731 und 94/90 betreffen den Zugang zu Dokumenten des Rates und der Kommission. Der Bürgerbeauftragte leitete daher im Juli 1996 eine Initiativuntersuchung ein, durch die geklärt werden sollte, ob auch die anderen Organe und Institutionen der Gemeinschaft über entsprechende Vorschriften verfügten[27]. Er wies dabei darauf hin, dass es ihm nicht um die Prüfung der Frage ging, "ob die Vorschriften selbst die richtigen sind, um den Grad der Transparenz zu gewährleisten, den die europäischen Bürger zunehmend von der Union erwarten"[28]. Dieser beschränkte Ansatz könnte auf den ersten Blick verwundern und Fragen nach seiner Nützlichkeit aufwerfen[29]. Allerdings war zu beachten, dass der Inhalt der von Rat und Kommission erlassenen Vorschriften beschränkt war. Hätte der Bürgerbeauftragte daher die anderen Organe und Institutionen dazu angehalten, weitergehende

---

[26] Der Text ist abgedruckt im ABl. 1999 Nr. C 371, S. 12.
[27] Untersuchung 616/PUBAC/IJH.
[28] Jahresbericht der Europäischen Bürgerbeauftragten ("Jahresbericht") 1996, S. 86.
[29] So ist denn auch der Vorwurf erhoben worden, der Bürgerbeauftragte beschränke sich auf eine minimalistische und legalistische Betrachtungsweise (*Adam Tomkins*, Transparency and the Emergence of a European Administrative Law, Yearbook of European Law 2000, S. 237).

Vorschriften zu erlassen, wären damit implizit die von Rat und Kommission erlassenen Regelungen in Frage gestellt worden. Ob der Bürgerbeauftragte dazu berechtigt gewesen wäre, ist durchaus fraglich.

Die Untersuchung des Bürgerbeauftragten betraf insgesamt 15 Organe und Institutionen der Gemeinschaft. Der Bürgerbeauftragte kam in seiner im Dezember 1996 erlassenen Entscheidung zu dem Schluss, dass die Weigerung, Regeln über den Zugang zu Dokumenten zu gewähren, einen Missstand darstellte. Er empfahl daher diesen Organen und Institutionen, binnen dreier Monate Regeln über den Zugang zu Dokumenten aufzustellen und diese Regeln der Öffentlichkeit zugänglich zu machen[30]. Er empfahl dabei zudem, dass diese Regeln für alle Dokumente gelten sollten, für die noch keine besonderen Vorschriften galten[31]. Auf der Grundlage der daraufhin eingegangenen Stellungnahmen der betroffenen Organe und Institutionen erstellte der Bürgerbeauftragte einen Sonderbericht, der dem Europäischen Parlament im Dezember 1997 unterbreitet wurde[32]. Der Bürgerbeauftragte konstatierte in diesem Bericht, dass fast alle Organe und Institutionen inzwischen Vorschriften über den Zugang zu Dokumenten erlassen hatten, und stellte es dem Parlament anheim, zu prüfen, ob diese Vorschriften einen ausreichenden Grad an Transparenz gewährleisteten. Lediglich der Europäische Gerichtshof hatte sich noch nicht in der Lage gesehen, solche Vorschriften aufzustellen. Der Bürgerbeauftragte vertrat jedoch die Auffassung, dass er nicht befugt sei, gegenüber dem Gerichtshof insoweit eine Empfehlung auszusprechen. Er begründete dies damit, dass nach Art. 195 EG-Vertrag die Ausübung der Rechtsprechungsbefugnisse des Gerichtshofes aus seinem Mandat ausgeklammert sei. Dies ist in der Tat der Fall. Gleichwohl überrascht das Ergebnis, hatte der Bürgerbeauftragte den Gerichtshof zunächst doch nur aufgefordert, Vorschriften über den Zugang zu seinen *Verwaltungs*dokumenten (und nicht zu den Dokumenten, welche die Rechtsprechungstätigkeit betrafen) aufzustellen. Die vom Bürgerbeauftragten vertretene Ansicht ist auch schwerlich mit dem (noch

---

[30] Siehe Jahresbericht 1996, S. 85 ff. (S. 91).

[31] Diese Empfehlung zeigt übrigens, dass sich der Bürgerbeauftragte nicht auf eine bloß formale Prüfung beschränkte.

[32] Veröffentlicht im ABl. 1998 Nr. C 44, S. 9.

zu erörternden) Grundsatz zu vereinbaren, wonach Ausnahmen vom Recht auf Zugang zu Dokumenten eng auszulegen seien.

Da nach dem Abschluss dieses Verfahrens vier weitere Einrichtungen geschaffen worden waren – die Europäische Agentur für Sicherheit und Gesundheitsschutz am Arbeitsplatz, die Europäische Zentralbank, das Gemeinschaftliche Sortenamt und das Europäische Polizeiamt (Europol) - , leitete der Bürgerbeauftragte im April 1999 eine weitere Initiativuntersuchung über den Zugang zu Dokumenten dieser Institutionen ein[33]. Diese Untersuchung führte hinsichtlich der drei erstgenannten Institutionen zu einem zufriedenstellenden Ergebnis[34]. Lediglich gegenüber Europol sah sich der Bürgerbeauftragte veranlasst, die im Rahmen der ersten Untersuchung ausgesprochenen Empfehlungen zu bekräftigen[35]. Europol hat in der Folgezeit Vorschriften über den Zugang zu seinen Dokumenten angenommen[36]. Bemerkenswert ist in diesem Zusammenhang, dass der Bürgerbeauftragte die von den betroffenen Institutionen aufgestellten Regeln auch einer inhaltlichen Prüfung unterzog[37].

Auslegung der Vorschriften über den Zugang zu Dokumenten

Wie nicht anders zu erwarten, stellt die Frage nach der korrekten Auslegung der Vorschriften über den Zugang zu Dokumenten den zweiten – und zahlenmäßig wichtigsten – Schwerpunkt der Tätigkeit des Bürgerbeauftragten in diesem Bereich dar. Die “entscheidende Frage” lautet hier, ob die betroffene Institution “ihre eigenen Regeln über den Zugang der Öffentlichkeit korrekt angewandt hat und ob sie sich innerhalb des ihrer Amtsgewalt entsprechenden Ermessensspielraums bewegt hat”[38].

Da die Vorschriften von Rat und Kommission Dokumente Dritter ausnehmen, vermag es nicht zu überraschen, dass der Bürgerbeauftragte keinen Missstand feststellen konnte, wo der Zugang zu

---

[33] Untersuchung OI/1/99/IJH.
[34] Jahresbericht 1999, S. 285, 288 und 292.
[35] Jahresbericht 1999, S. 296.
[36] Siehe Jahresbericht 2000, S. 216.
[37] Vgl. etwa die Ausführungen des Bürgerbeauftragten zu den Vorschriften der EZB, denen zufolge diese Vorschriften auch auf bestimmte dort nicht genannte Dokumente Anwendung finden sollte (Jahresbericht 1999, S. 291 f.).
[38] Jahresbericht 1998, S. 32.

Dokumenten Dritter verweigert wurde[39]. Der Bürgerbeauftragte ist jedoch ersichtlich bestrebt, die daraus resultierende Beschränkung des Zugangsrechts der Bürger so gering wie möglich zu halten. In einem 1998 entschiedenen Fall[40] ging es um ein Dokument aus dem Bereich der Sozialpolitik, das auf Informationen beruhte, welche die Mitgliedstaaten zur Verfügung gestellt hatten. Die Kommission hatte zuvor den Mitgliedstaaten einen Fragebogen zugesandt und sich dann darauf beschränkt, die eingegangenen Informationen zusammenzustellen. Sie vertrat daher die Ansicht, dass es sich hier nicht um ein *Kommissions*dokument handele. Der Antrag auf Zugang zu dem Dokument solle vielmehr bei dessen Urhebern, den Mitgliedstaaten, gestellt werden. Der Bürgerbeauftragte verwies demgegenüber auf die Rolle, welche die Kommission bei der Vorbereitung des Dokuments gespielt hatte und stellte sich auf den Standpunkt, die Verweigerung des Zugangs untergrabe das Vertrauen in die Gemeinschaftsverwaltung. Er wies außerdem darauf hin, dass der Beschwerdeführer, nachdem er sich an einen Mitgliedstaat gewandt hatte, von diesem an die Kommission verwiesen worden war, und zwar mit der Begründung, dass es sich um ein Kommissionsdokument handele. Der Bürgerbeauftragte schlug daher eine einvernehmliche Lösung des Falles vor, nach der die Kommission Zugang zu dem Dokument gewähren sollte. Die Kommission nahm diesen Vorschlag an.

Ebenso verfuhr der Bürgerbeauftragte in einem kürzlich entschiedenen Fall, der zwei Gutachten betraf, die die Kommission bei Dritten in Auftrag gegeben hatte. Der Bürgerbeauftragte befand, dass diese Dokumente im Hinblick auf ihre Natur und auf die Rolle, welche die Kommission bei ihrer Herstellung gespielt habe, als Dokumente der Kommission anzusehen seien[41]. Die Kommission war damit einverstanden.

Eine Beschwerde von Statewatch – einer britischen Einrichtung, von der hier noch mehrmals die Rede sein wird – gab dem Bürger-

---

[39] Vgl. Untersuchung 532/28.3.96/UTEC/B/KT (Jahresbericht 1997, S. 98) und Untersuchung 709/9.7.96/TC/IRL/KT (Jahresbericht 1997, S. 269).

[40] Untersuchung 1045/21.11.96/BH/IRL/JMA (Jahresbericht 1998, S. 173).

[41] Verbundene Untersuchungen 271/2000/(IJH)/JMA und 272/2000/(IJH)/JMA. Die englische Fassung der Entscheidung vom 31. Mai 2001 ist auf der Webseite des Bürgerbeauftragten verfügbar.

beauftragten Gelegenheit, weitere wichtige Fragen hinsichtlich der Identität des Urhebers eines Dokuments zu klären[42]. Dort begehrte der Beschwerdeführer vom Rat unter anderem Zugang zu Tagesordnungen für bestimmte Treffen zwischen EU-Stellen und amerikanischen Behörden. Diese Tagesordnungen wurden gemeinsam vom Rat, von der Kommission und von den amerikanischen Behörden festgelegt. Es wurde daher geltend gemacht, es handele sich nicht um Dokumente des Rates. Der Bürgerbeauftragte widersprach dem. Er befand, dass auch Dokumente, die vom Rat gemeinsam mit anderen Personen verfasst worden waren, in den Anwendungsbereich des Beschlusses 93/731 fielen. Dies entspreche dem Grundsatz größtmöglichen Zugangs zu Dokumenten, den dieser Beschluss verwirklichen solle. Der Rat hatte im übrigen zunächst die Auffassung vertreten, es handele sich hier um Dokumente der Präsidentschaft, nicht um solche des Rates. Von dieser merkwürdigen Einschätzung ist der Rat allerdings noch im Laufe des Verfahrens abgerückt.

Wer allerdings geglaubt hatte, der Rat würde nunmehr – wie der Bürgerbeauftragte ihm in der kritischen Bemerkung, mit der er diesen Fall abgeschlossen hatte, nahegelegt hatte – Zugang zu den genannten Dokumenten zu gewähren, sah sich getäuscht. In einer weiteren Beschwerde wies Statewatch den Bürgerbeauftragten darauf hin, dass der Rat sich nunmehr auf den Standpunkt gestellt habe, die fraglichen Dokumente befänden sich nicht im Besitz des Rates, sondern von dessen Generalsekretariat. Aus diesem Grunde sei der Rat nicht verpflichtet (oder nicht einmal in der Lage), Zugang zu diesen Dokumenten zu gewähren. Der Bürgerbeauftragte befand, dass die auf diese Begründung gestützte Verweigerung des Zugangs einen Missstand darstelle. Der Rat lenkte daraufhin ein und gewährte dem Beschwerdeführer Zugang zu den Dokumenten, so dass der Bürgerbeauftragte den Fall abschließen konnte[43].

In dem soeben genannten Fall machte der Rat in dem Verfahren vor dem Bürgerbeauftragten geltend, dass die Frage, ob das Generalsekretariat für die Zwecke des Zugangs zu Dokumenten als Teil

---

[42] Untersuchung 1056/25.11.96/STATEWATCH/UK/IJH (Jahresbericht 1998, S. 194).

[43] Untersuchung 916/2000/GG. Die englische Fassung der Entscheidung vom 16. Juli 2001 ist auf der Webseite des Bürgerbeauftragten abrufbar.

des Rates anzusehen sei, auch in einem vor dem Gericht erster Instanz anhängigen Verfahren aufgeworfen worden sei. Der Bürgerbeauftragte ließ sich durch diesen Hinweis jedoch – zu Recht[44] – nicht davon abhalten, über die Beschwerde zu entscheiden. Wesentlich vorsichtiger ging der Bürgerbeauftragte hingegen in einem anderen Fall[45] vor. Dort ging es um die Frage, ob der Beschluss 94/90 der Kommission auch für Dokumente der sogenannten Komitologie-Ausschüsse[46] gilt. Der Bürgerbeauftragte ließ diese Frage zunächst offen, bis das Gericht erster Instanz sie in einem anderen Verfahren bejaht hatte[47].

Auch für den Bereich der Ausnahmen vom Recht auf Zugang zu Dokumenten lassen sich der Entscheidungspraxis des Bürgerbeauftragten nützliche Hinweise entnehmen.

Dies gilt zunächst für die Frage, wann zum Schutz des öffentlichen Interesses der Zugang zu einem Dokument verweigert werden *muss*. Auch der Bürgerbeauftragte betont die Bedeutung, die in einem solchen Fall der Begründung der ablehnenden Entscheidung zukommt. Ein bloßer Verweis auf die Notwendigkeit der "Bekämpfung des organisierten Verbrechens" ohne nähere Erläuterungen wurde vom Bürgerbeauftragten zu Recht als nicht ausreichend angesehen[48].

In einem 1999 entschiedenen Fall[49] ging es um die Festsetzung der obligatorischen Destillation durch die Erzeuger von Tafelwein – eines der Instrumente, mit denen die Gemeinschaft der Weinflut Herr zu werden versucht. Die Beschwerdeführer, italienische Winzer, wa-

---

[44] Der Bürgerbeauftragte kann gemäß Art. 195 Abs. 1 EG-Vertrag keine Untersuchung durchführen (oder muss eine solche einstellen, vgl. Art. 2 Abs. 7 seines Statuts), "wenn die behaupteten Sachverhalte Gegenstand eines Gerichtsverfahrens sind oder waren". Dies war hier nicht der Fall, da die - übrigens später zurückgenommene – Klage vor dem Gericht zwar möglicherweise die gleiche Rechtsfrage, aber einen anderen "Sachverhalt" betraf.

[45] Untersuchung 633/97/PD (Jahresbericht 1999, S. 270).

[46] Diese Ausschüsse unterstützen die Kommission, wenn sie Maßnahmen zur Durchführung der ihr nach dem einschlägigen Beschluss des Rates (Beschluss 87/373 vom 13. Juli 1987, ABl. 1987 Nr. L 197, S. 33; sog. "Komitologie-Beschluss") übertragenen Befugnisse erlässt.

[47] Rs. T-188/97 Rothmans International/Kommission, Slg. 1999, II-2463 Rn. 62.

[48] Untersuchung 105725.11.96/STATEWATCH/UK/IJH (Jahresbericht 1998, S. 200).

[49] Untersuchung 506/97/JMA (Jahrsbericht 1999, S. 182).

ren der Ansicht, dass die Berechnung der von den einzelnen Staaten zu destillierenden Mengen auf diskriminierende Weise vorgenommen und Italien im Ergebnis eine erhebliche Geldbuße auferlegt worden sei. Sie beantragten daher, in verschiedene Unterlagen Einsicht nehmen zu dürfen, auf welche die Kommission sich bei der Festsetzung der relevanten Mengen gestützt hatte. Die Kommission lehnte dies mit der Begründung ab, dass beim Gerichtshof ein Verfahren anhängig sei, das die Rechtmäßigkeit ihrer Entscheidung betreffe. Anträge auf Zugang zu den betroffenen Dokumenten müssten daher direkt beim Gerichtshof gestellt werden. Die Kommission machte somit geltend, dass sie den Zugang zum Zwecke des Schutzes der Rechtspflege versagen müsse. Der Bürgerbeauftragte hielt diese Haltung für falsch. Er wies darauf hin, dass die fraglichen Dokumente erarbeitet worden seien, um die Entscheidung der Kommission über die Zwangsdestillation vorzubereiten, nicht aber, um im Rahmen eines Gerichtsverfahrens einem bestimmten Zweck zu dienen. Diese einschränkende Auslegung verdient Zustimmung.

Auch in einem neueren Fall hat der Bürgerbeauftragte den Grundsatz betont, dass Ausnahmen vom Recht auf Zugang eng auszulegen seien. In diesem Fall – der bereits kurz erwähnt wurde – ging es um den Zugang zu Gutachten, welche die Kommission bei Dritten in Auftrag gegeben hatte. Durch diese Gutachten sollte geklärt werden, ob ein Mitgliedstaat seine Verpflichtungen aus bestimmten Richtlinien im Bereich des Umweltschutzes erfüllt hatte. Die Kommission machte geltend, diese Gutachten seien erstellt worden, um eine mögliche Klage gegen diesen Mitgliedstaat vor dem Gerichtshof vorzubereiten. Der Bürgerbeauftragte stellte sich hingegen auf den Standpunkt, dass die Gutachten vor der Entscheidung über die Einleitung einer Untersuchung entstanden seien. Die Verweigerung des Zugangs zu ihnen könne daher nicht mit der Begründung gerechtfertigt werden, es handele sich dabei um die Ergebnisse der Inspektions- oder Untersuchungstätigkeiten der Kommission. Die Kommission hat daraufhin Zugang zu den fraglichen Dokumenten gewährt[50].

[50] Verbundene Untersuchungen 271/2000/(IJH)/JMA und 272/2000/(IJH)/JMA. Die englische Fassung der Entscheidung vom 31. Mai 2001 ist auf der Webseite des Bürgerbeauftragten verfügbar.

Soweit das Gemeinschaftsorgan bei der Frage der Gewährung des Zugangs über ein Ermessen verfügt, muss sie dieses effektiv und korrekt ausüben[51]. Interessant ist in diesem Zusammenhang eine Untersuchung, in der es um den Zugang zu Tagesordnungen von Ausschüssen des Rates und anderen Dokumenten ging. Der Rat war der Auffassung, dass der Zugang zu versagen sei, da die Beratung des betreffenden Gegenstandes im Rat noch nicht abgeschlossen sei und der künftige Informationsaustausch zwischen Rat und Mitgliedstaaten durch die Veröffentlichung gefährdet werden könne. Der Bürgerbeauftragte befand, dass eine solche Erwägung angesichts des Zieles der Zugangsregeln – der Stärkung des demokratischen Charakters der Gemeinschaftsorgane und des öffentlichen Vertrauens in sie – mit Vorsicht gehandhabt werden müsse. Er hielt daher einen Missstand für gegeben, da es im konkreten Fall an genaueren Erläuterungen fehlte[52].

Wie bereits dargelegt wurde, ist das Gericht der Ansicht, dass grundsätzlich auch die Möglichkeit eines teilweisen Zugangs zu Dokumenten in Betracht gezogen werden müsse, wenn kein vollständiger Zugang gewährt werden kann. Interessanterweise scheint der Bürgerbeauftragte diesen Grundsatz bereits vor dem Urteil des Gerichts angewandt zu haben. In einer 1997 eingereichten Beschwerde ging es um den Zugang zu einem Bericht, der von einem Beratungsunternehmen für die Kommission angefertigt worden war. Der Bürgerbeauftragte kam zu dem Ergebnis, dass der überwiegende Teil dieses Berichts zugänglich gemacht werden konnte. Er unterbreitete der Kommission einen entsprechenden Vorschlag, den diese annahm[53].

<u>Voraussetzungen für wirksames Gebrauchmachen vom Recht auf Zugang</u>

Das Recht auf Zugang zu Dokumenten im Besitz von Rat oder Kommission wird zwar von der Gemeinschaftsrechtsordnung geschützt. Seine wirksame Ausübung hängt jedoch von verschiede-

---

[51] Vgl. Untersuchung 709/9.7.96/TC/IRL/KT (Jahresbericht 1997, S. 269); Untersuchung 1057/25.11.96/STATEWATCH/UK/IJH (Jahresbericht 1998, S. 210).

[52] Untersuchung 634/97/PD (Jahresbericht 1998, S. 210).

[53] Verbundene Untersuchungen 620/97/PD und 306/98/PD (Jahresbericht 1999, S. 74).

nen Voraussetzungen ab, die in den Beschlüssen 93/731 und 94/90 nicht näher dargelegt werden.

Eine dieser Voraussetzungen besteht darin, dass die fraglichen Dokumente von dem betroffenen Organ oder der betroffenen Institution aufbewahrt werden. Dass dies nicht selbstverständlich ist, zeigte eine Beschwerde von Statewatch aus dem Jahre 1996, der zufolge der Rat bestimmte Tagesordnungen nach einem Jahr vernichtete. In seiner Stellungnahme zu der Beschwerde teilte der Rat mit, dass nunmehr Vorsorge dafür getroffen worden sei, diese Dokumente systematisch aufzubewahren[54].

Ein Bürger wird sein Recht auf Zugang zu Dokumenten erst dann ausüben können, wenn er von der Existenz dieser Dokumente erfahren hat. Ein Register oder Verzeichnis der vorhandenen Dokumente ist daher unverzichtbar.

Das Fehlen einer aktuellen Liste der im Bereich Justiz und Inneres verabschiedeten Maßnahmen wurde in einer Beschwerde von Statewatch im Jahre 1996 moniert. Der Bürgerbeauftragte empfahl daraufhin dem Rat, “in Übereinstimmung mit den Bestimmungen des Beschlusses Nr. 93/731” ein solches Verzeichnis zugänglich zu machen. Der Rat folgte dieser Empfehlung, so dass der Bürgerbeauftragte die Untersuchung Anfang 1999 abschließen konnte[55].

Bereits in einer gegen den Rat gerichteten Beschwerde im Jahre 1997 wurde das Fehlen eines Dokumentenregisters hervorgehoben. Der Bürgerbeauftragte stellte seine Untersuchung jedoch insoweit ein, da sich ergab, dass der Rat im Begriffe war, ein solches Register einzurichten[56]. Allerdings dauerte es noch eine Weile, bis dieses Register tatsächlich funktionsfähig war[57].

---

[54] Untersuchung 1054/25.11.96/STATEWATCH/UK/IJH (Jahresbericht 1997, S. 199).

[55] Untersuchung 1055/25.11.96/STATEWATCH/UK/IJH (Jahresbericht 1998, S. 291 und Jahresbericht 1999, S. 268).

[56] Untersuchung 634/97/PD (Jahresbericht 1998, S. 210).

[57] Vgl. den Beschluss 2000/23/EG des Rates vom 6. Dezember 1999 zur Verbesserung der Information über die Gesetzgebungstätigkeit des Rates und das öffentliche Register der Ratsdokumente (ABl. 2000 Nr. L 9, S. 22).

In seiner 1999 ergangenen Entscheidung zu einer Beschwerde gegen die Kommission befand der Bürgerbeauftragte, ein grundlegendes Prinzip guter Verwaltungspraxis bestehe darin, dass eine Behörde ein Dokumentenverzeichnis führen solle, in dem ein- und ausgehende Dokumente aufzuführen seien. Das Fehlen eines solchen Verzeichnisses behindere den Bürger dabei, sein Recht auf Zugang zu Dokumenten auszuüben. Der Bürgerbeauftragte empfahl daher der Kommission, ein solches, der Öffentlichkeit zugängliches Verzeichnis anzulegen. In ihrer Antwort machte die Kommission geltend, dass diese Frage im Rahmen der Durchführung von Art. 255 EG-Vertrag geprüft werden müsse. Obwohl die Kommission auch insoweit jedoch keine feste Zusage abgegeben hatte, erachtete der Bürgerbeauftragte die Antwort der Kommission für zufriedenstellend[58]. Diese Entscheidung ist nicht leicht zu verstehen. Vielleicht spielten die internen Schwierigkeiten, mit denen die Kommission zu der fraglichen Zeit konfrontiert war – 1999 war bekanntlich das Jahr, in dem die Kommission kollektiv zurückgetreten war und eine neue Kommission bestimmt werden musste – eine gewisse Rolle.

Eine wichtige Frage wurde in diesem Zusammenhang durch eine im Jahre 2000 eingereichte Beschwerde von Statewatch aufgeworfen[59]. Der Beschwerdeführer war in den Besitz einiger Vermerke über Treffen des Rates oder seiner Ausschüsse im Bereich Justiz und Inneres gelangt. Er bemerkte, dass in diesen Vermerken auf bestimmte Dokumente verwiesen wurde, die in den Tagesordnungen der jeweiligen Treffen nicht erwähnt wurden. Diese Dokumente wurden als “room documents”, “non-papers”, “meetings documents” oder “SN” (“sans numéro”, d.h. Dokumente ohne Nummer) bezeichnet. Der Beschwerdeführer rügte, dass der Rat es unterlassen habe, diese Dokumente in einem Verzeichnis aufzulisten. Der Rat machte in seiner Stellungnahme zu der Beschwerde geltend, es handele sich bei diesen Unterlagen um Dokumente, die einen lediglich vorübergehenden und vorläufigen Charakter aufwiesen. Müssten auch alle diese Dokumente in ein Verzeichnis aufgenommen werden, würde man dem Generalsekretariat des Rates eine schwere administrative Last aufbürden. Der Bürgerbeauftragte befand,

---

[58] Untersuchung 633/97/PD (Jahresbericht 1999, S. 270).
[59] Untersuchung 917/2000/GG.

dass das Recht auf Zugang zu Dokumenten ernstlich gefährdet oder gar zunichte gemacht werden könnte, wenn der Bürger nicht wisse, welche Dokumente sich im Besitz des Organs befinden. Er kam daher zu dem Ergebnis, dass die Grundsätze guter Verwaltungspraxis es geböten, *alle* Dokumente, die dem Rat vorgelegt werden, in einem Verzeichnis aufzuführen. Die daraus resultierende zusätzliche Arbeitsbelastung der Verwaltung des Rates müsse im Hinblick auf die grundlegende Bedeutung des Rechts auf Zugang hingenommen werden. Der Bürgerbeauftragte empfahl daher dem Rat im März dieses Jahres, ein solches Verzeichnis anzulegen und der Öffentlichkeit zugänglich zu machen[60]. Ende Mai 2001 teilte der Rat dem Bürgerbeauftragten mit, dass er diese Empfehlung annehme. Zugleich machte er aber geltend, dass nicht jedwedes Dokument in das Verzeichnis aufgenommen werden müsse, sondern nur Dokumente, die den Beratungen des Rates zugrunde lagen, die den Entscheidungsfindungsprozess beeinflussten oder die den erreichten Sachstand widerspiegelten. Der Bürgerbeauftragte wird nun zu entscheiden haben, ob dies als ausreichend zu erachten ist[61].

Es versteht sich von selbst, dass der Europäische Bürgerbeauftragte auch selbst Zugang zu den in seinen Händen befindlichen Dokumenten gewährt[62]. Angesichts der umfassenden Transparenz, die der Bürgerbeauftragte bei seiner Tätigkeit walten lässt – so werden sämtliche Entscheidungen und eine Vielzahl weiterer Informationen auf seiner Webseite[63] veröffentlicht – hat dieser Zugang allerdings bislang keine besondere Bedeutung erlangt.

IV. Zugang zu Dokumenten und Datenschutz

Dem Datenschutz wird auch auf der Ebene der EU immer mehr der ihm gebührende Raum eingeräumt. Hier sind insbesondere zwei wichtige Rechtsakte zu nennen. Die Richtlinie 95/46/EG des Euro-

---

[60] Die englische Fassung des Empfehlungsentwurfs vom 1. März 2001 ist auf der Webseite des Bürgerbeauftragten verfügbar.

[61] Der Beschwerdeführer hat insoweit beachtliche Bedenken vorgetragen.

[62] Siehe Art. 13 der vom Europäischen Bürgerbeauftragten am 16. Oktober 1997 erlassenen Durchführungsbestimmungen (veröffentlicht auf der Webseite des Bürgerbeauftragten).

[63] http://www-ombudsman.eu.int

päischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[64] sieht in ihrem Art. 7 vor, dass die Verarbeitung personenbezogener Daten nur erfolgen darf, wenn eine der folgenden Voraussetzungen erfüllt ist:

(a) Die betroffene Person hat ohne jeden Zweifel ihre Einwilligung gegeben;

(b) die Verarbeitung ist erforderlich für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung vorvertraglicher Maßnahmen, die auf Antrag der betroffenen Person erfolgen;

(c) die Verarbeitung ist für die Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;

(d) die Verarbeitung ist erforderlich für die Wahrung lebenswichtiger Interessen der betroffenen Person;

(e) die Verarbeitung ist erforderlich für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt und dem für die Verarbeitung Verantwortlichen oder dem Dritten, dem die Daten übermittelt werden, übertragen wurde;

(f) die Verarbeitung ist erforderlich zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt sind, überwiegen.

Unter “personenbezogenen Daten” sind dabei “alle Informationen über eine bestimmte oder bestimmbare natürliche Person” zu verstehen (Art. 2 Buchstabe a der Richtlinie).

---

[64] ABl. 1995 Nr. L 281, S. 31.

Nach Art. 286 EG-Vertrag waren die Bestimmungen dieser – an die Mitgliedstaaten der EU gerichteten – Richtlinie vom 1. Januar 1999 an auch von den Organen und Institutionen der EU zu beachten.

Inzwischen ist – auf der Grundlage des genannten Art. 286 EG-Vertrag – eine eigene Verordnung erlassen worden, die speziell für die Verarbeitung personenbezogener Daten durch die Organe und Institutionen der Gemeinschaft gilt. Die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr[65] sieht im übrigen die Einrichtung einer unabhängigen Kontrollbehörde, des Europäischen Datenschutzbeauftragten, vor (siehe Art. 41 der Verordnung).

Das Recht auf Zugang zu Dokumenten kann offensichtlich mit den Belangen des Datenschutzes in Konflikt geraten. Bereits der Verhaltenskodex von Rat und Kommission hatte, wie wir gesehen haben, den Zugang zu Dokumenten ausgeschlossen, wenn dadurch “der Schutz des Einzelnen und der Privatsphäre” gefährdet würde. Die Probleme, die sich aus diesem Gegensatz zwischen dem Prinzip der Transparenz einerseits und dem Datenschutz andererseits ergeben können, werden – wenn auch auf eine eher überraschende Art und Weise - durch eine Beschwerde verdeutlicht, mit dem sich der Bürgerbeauftragte zu befassen hatte[66].

Der Beschwerdeführer, ein britischer Staatsangehöriger, importierte deutsches Bier, das zum Verbrauch in Gaststätten in England bestimmt war. Er sah sich in dieser Geschäftstätigkeit jedoch durch den Umstand behindert, dass im Vereinigten Königreich viele Gastwirte durch Bierlieferungsverträge gebunden sind, die sie zum ausschließlichen Bezug des Biers einer bestimmten Brauerei verpflichten. Der britische Gesetzgeber hatte diese Verpflichtung zwar durch eine Verordnung aufgelockert, wonach britische Brauereien mit einer großen Zahl gebundener Gastwirte es diesen erlauben müssen, auch von einer anderen Brauerei Bier zu beziehen. Es musste sich dabei jedoch um Fassbier mit einem bestimmten Alkoholgehalt

---

[65] ABl. 2001 Nr. L 8, S. 1.
[66] Untersuchung 713/98/IJH.

handeln. Diese Regelung wird gemeinhin als “Guest Beer Provision” bezeichnet. Als “Fassbier” gilt nach dieser Regelung Bier, “das in dem Behältnis, dem es zum Verzehr entnommen wird, weiter gärt”. Die meisten der außerhalb des Vereinigten Königreichs erzeugten Biere werden jedoch vor dem Abfüllen gefiltert und gären deshalb nicht weiter. Sie sind demnach nicht als “Fassbier” im Sinne der genannten Regelung zu betrachten.

Der Beschwerdeführer hielt die britische Regelung für unvereinbar mit der durch Art. 28 EG-Vertrag geschützten Warenverkehrsfreiheit und wandte sich daher mit einer Beschwerde an die Kommission. Diese leitete daraufhin eine Untersuchung ein. Im Sommer 1996 beschloss die Kommission, eine mit Gründen versehene Stellungnahme an das Vereinigte Königreich zu richten[67]. Dazu kam es jedoch nicht mehr. Im Oktober 1996 fand in Brüssel ein Treffen zwischen der Kommission, den britischen Behörden und einem Brauerverband (der Confédération des Brasseurs du Marché commun) statt. Der Beschwerdeführer war nicht geladen worden. Im März 1997 schlugen die britischen Behörden eine Änderung der Guest Beer Provision vor[68]. Die Kommission hielt diese Änderung für zufriedenstellend und stellte das Vertragsverletzungsverfahren ein.

Der Beschwerdeführer wandte sich daraufhin an die Kommission, um herauszufinden, welche Vertreter des Brauerverbandes[69] an dem genannten Treffen teilgenommen und welche Personen der Kommission im Laufe des Verfahrens Stellungnahmen unterbreitet hatten. Da die Kommission dies ablehnte, wandte sich der Beschwerdeführer an den Bürgerbeauftragten.

Die Kommission berief sich darauf, dass die Richtlinie 95/46 es ihr nicht erlaube, die Identität der betroffenen Personen ohne deren ausdrückliche Einwilligung preiszugeben. Sie erklärte sich jedoch bereit, eine Ad-hoc-Lösung für diese Beschwerde zu suchen, indem sie die betroffenen Personen bitten würde, zu erlauben, dass ihre

---

[67] Es handelt sich dabei um den Verfahrensschritt, der gemäß Art. 226 EG-Vertrag einer Klage beim Gerichtshof vorausgehen muß.

[68] Dieser Änderung zufolge sollte nun neben Fassbier auch Flaschenbier einer anderen Brauerei verkauft werden dürfen.

[69] Der Beschwerdeführer hatte sich auch an diesen Verband selbst gewandt, der ihm jedoch mitteilte, dass keine Unterlagen mehr vorhanden seien.

Namen dem Beschwerdeführer mitgeteilt würden. Die Kommission teilte in der Folge mit, dass sie an insgesamt 45 Personen geschrieben habe, von denen 14 zustimmend und 6 ablehnend reagiert hatten. Die Namen der 14 Personen, die zugestimmt hatten, wurden dem Beschwerdeführer mitgeteilt. Auf ein weiteres Schreiben des Bürgerbeauftragten hin stellte sich die Kommission auf den Standpunkt, dass sie die entsprechenden Namen nur offenlegen könne, wenn die betroffene Person „ohne jeden Zweifel ihre Einwilligung gegeben hat".

Der Bürgerbeauftragte hielt dies nicht für ausreichend und empfahl der Kommission, alle Namen offenzulegen. Er vertrat die Ansicht, dass es sich bei der Mitteilung von Informationen an eine Verwaltungsbehörde durch eine Person, die an einem Verwaltungsverfahren beteiligt ist, nicht um „personenbezogene Daten" handeln dürfte. Andernfalls würde man akzeptieren, dass es ein Grundrecht auf die geheime Überlassung von Informationen an eine Verwaltungsbehörde gäbe, was nicht der Fall sei. Der Bürgerbeauftragte verwies insoweit auf die Bedeutung der Transparenz im Gemeinschaftsrecht. Er machte zudem geltend, dass zudem – wenn man die Anwendbarkeit der Datenschutzrichtlinie bejahe – einige der in ihrem Art. 7 genannten Ausnahmen erfüllt seien. Auf der Grundlage dieser Erwägungen gelangte der Bürgerbeauftragte zu der Schlussfolgerung, dass die Kommission ihre aus der Richtlinie folgenden Verpflichtungen missverstanden und daher das Prinzip der Offenheit verletzt habe. Er empfahl daher der Kommission, dem Beschwerdeführer die fraglichen Namen mitzuteilen.

In ihrer Stellungnahme beharrte die Kommission auf ihrem Standpunkt. Sie merkte aber an, dass im vorliegenden Fall in Anbetracht von dessen Besonderheiten die Rechte und Interessen derjenigen Personen, die auf das Schreiben der Kommission nicht reagiert hatten, nicht überwögen. Die Kommission teilte dem Beschwerdeführer daher auch die Namen der 25 Personen mit, welche die Anfrage der Kommission, ob sie mit der Weitergabe ihres Namens einverstanden seien, nicht beantwortet hatten.

Der Bürgerbeauftragte vertrat die Auffassung, dass die Zugeständnisse der Kommission den von ihm konstatierten Missstand nicht ausgeräumt hatten. Er erkannte zwar die Bedeutung des Interesses

an, das an dem Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere ihres Privatlebens besteht. Der Bürgerbeauftragte beharrte jedoch auf seiner Überzeugung, dass die Belange des Datenschutzes es nicht verlangten, die Namen von Personen geheimzuhalten, die der Kommission „Standpunkte oder Informationen in Zusammenhang mit der Ausübung ihrer Funktionen unterbreiten". Er legte daher dem Europäischen Parlament im November 2000 einen Sonderbericht zu diesem Fall vor[70].

Der Petitionsausschuss des Europäischen Parlaments hat in der Zwischenzeit zwei Anhörungen veranstaltet, bei denen der Bürgerbeauftragte und das zuständige Mitglied der Kommission gehört wurden. Eine Stellungnahme des Ausschusses und des Parlaments steht noch aus.

Die Haltung der Kommission begegnet großen Bedenken. Dies gilt insbesondere für die Identität der Teilnehmer des ominösen Treffens in Brüssel. Die Personen, um die es hier geht, nahmen an diesem Treffen nicht zu ihrem Privatvergnügen teil, sondern in ihrer Rolle als Vertreter des Brauerverbandes. Es ist daher nicht ersichtlich, welche Rolle hier der Schutz der Privatsphäre spielen könnte. Die von der Kommission vertretene extensive Auslegung beschwört die Gefahr herauf, die legitimen Belange des Datenschutzes ad absurdum zu führen. „Vernunft wird Unsinn, Wohltat Plage". Eine konsequente Verfolgung dieses Ansatzes würde auch die vom Gemeinschaftsrecht gewollte Transparenz des Verwaltungshandelns in Frage stellen. Nebenbei bemerkt vermag die Haltung der Kommission in diesem Fall schon aus dem Grunde nicht zu überzeugen, dass sie selbst die Vorschriften missachtet, die sie zu schützen behauptet. Wenn nämlich tatsächlich die Namen nur dann mitgeteilt werden durften, wenn die betroffene Person „ohne jeden Zweifel ihre Einwilligung gegeben hat", so verstieß die Nennung der Namen der 25 Personen, die auf das Schreiben der Kommission nicht reagiert hatten, gegen das Gemeinschaftsrecht.

[70] Der Sonderbericht ist auf der Webseite des Bürgerbeauftragten verfügbar.

V. Verordnung (EG) Nr. 1049/2001

Wie bereits erwähnt, haben der Rat und das Europäische Parlament nunmehr die in Art. 255 Abs. 3 EG-Vertrag vorgesehene Verordnung über die Ausgestaltung des Rechts auf Zugang zu Dokumenten erlassen. Diese Verordnung bringt eine Reihe von Neuerungen und Verbesserungen mit sich. Die Qualität dieses Rechtsaktes wird besonders deutlich, wenn man ihn mit dem Entwurf[71] vergleicht, auf dem er beruht. In diesem Entwurf, den die Kommission ohne vorherige Konsultation vorgelegt hatte, war der Begriff "Dokument" dergestalt definiert, dass er Dokumente zum internen Gebrauch ausschloss. Diese Einschränkung ist nicht in die Verordnung aufgenommen worden.

Die Verordnung gilt – wie es ihrer Grundlage, dem Art. 255 EG-Vertrag entspricht – nur für den Zugang zu Dokumenten im Besitz von Rat, Kommission oder Parlament. In einer gemeinsamen Erklärung zu dieser Verordnung haben diese drei Organe jedoch zum Ausdruck gebracht, dass auch die anderen Organe und Institutionen der EU über entsprechende Vorschriften verfügen sollten[72].

Die erste große Neuerung ergibt sich aus Art. 2 Abs. 3 der Verordnung. Dieser Bestimmung zufolge erfasst das Recht auf Zugang nicht nur die Dokumente, die von dem jeweiligen Organ erstellt worden sind, sondern auch die bei ihm eingegangenen Dokumente Dritter (Art. 2 Abs. 3). Dies stellt eine wichtige und eindeutig positiv zu bewertende Änderung dar. Die Interessen der Urheber der bei dem Organ eingegangenen Dokumente bleiben dabei gewahrt. Das Organ hat diese Personen nämlich zu konsultieren, bevor es über die Freigabe entscheidet, es sei denn, es wäre klar, dass das Dokument freigegeben oder aber nicht freigegeben werden darf (Art. 4 Abs. 4).

Die Regelung der Ausnahmen hat ebenfalls eine Verbesserung erfahren.

---

[71] KOM(2000) 30 endg. (ABl. 2000 Nr. C 177 E, S. 70).
[72] ABl. 2001 Nr. L 173, S. 5.

Art. 4 Abs. 1 bestimmt, dass der Zugang verweigert werden *muss*, wenn folgende Interessen beeinträchtigt würden:

"(a) der Schutz der öffentlichen Interessen im Hinblick auf
- die öffentliche Sicherheit,
- die Verteidigung und militärische Belange,
- die internationalen Beziehungen,
- die Finanz-, Währungs- oder Wirtschaftspolitik der Gemeinschaft oder eines Mitgliedstaats;

(b) der Schutz der Privatsphäre und der Integrität des Einzelnen, insbesondere gemäß den Rechtsvorschriften der Gemeinschaft über den Schutz personenbezogener Daten."

Ebenfalls verweigert werden *muss* der Zugang zu einem Dokument, wenn dadurch (a) der Schutz der geschäftlichen Interessen einer natürlichen oder juristischen Person, einschließlich des geistigen Eigentums, (b) der Schutz von Gerichtsverfahren und der Rechtsberatung oder (c) der Schutz des Zwecks von Inspektions-, Untersuchungs- und Audittätigkeiten beeinträchtigt würde, *es sei denn*, es bestehe ein "überwiegendes öffentliches Interesse" an der Verbreitung.

Schließlich regelt die Verordnung den Schutz der internen Meinungsbildung des Organs, wobei danach unterschieden wird, ob bereits ein Beschluss gefasst worden ist oder nicht. Ist dies noch nicht der Fall, wird der Zugang zu internen Dokumenten und zu Dokumenten Dritter, die bei dem Organ eingegangen sind, verweigert, *es sei denn*, es bestehe ein "überwiegendes öffentliches Interesse" an der Verbreitung. Ist hingegen bereits ein Beschluss gefasst worden, so wird nur der Zugang zu internen Dokumenten verweigert, *es sei denn*, es bestehe ein "überwiegendes öffentliches Interesse" an der Verbreitung. Bei den internen Dokumenten, deren Offenlegung versagt werden kann, muss es sich im letztgenannten Fall um "Stellungnahmen zum internen Gebrauch im Rahmen von Beratungen und Vorgesprächen innerhalb des betreffenden Organs" handeln (Art. 3 Abs. 3).

Eine besonders heikle Frage ist in Art. 5 geregelt. Manche Dokumente der Organe der Gemeinschaft werden den Mitgliedstaaten

übermittelt. Dadurch eröffnet sich Bürgern die Möglichkeit, auf der Grundlage nationaler Vorschriften Zugang zu Dokumenten zu erhalten, die ihnen von den Gemeinschaftsorganen vorenthalten werden. Art. 5 verpflichtet die Mitgliedstaaten in einem solchen Fall (es sei denn, es wäre klar, ob das Dokument weitergegeben werden darf oder nicht), das betreffende Organ zu konsultieren, um eine Entscheidung zu treffen, "die die Verwirklichung der Ziele dieser Verordnung nicht beeinträchtigt".

Die Verordnung dürfte auch für eine gewisse Beschleunigung der Verfahren sorgen, da nunmehr sowohl über den Erstantrag wie über Zweitantrag binnen 15 Arbeitstagen zu entscheiden ist (Art. 7 Abs. 1 und Art. 8 Abs. 1)[73].

Eine besondere Behandlung ist für sogenannte "sensible" Dokumente vorgesehen (Art. 9). Es handelt sich dabei um Dokumente, die zum Schutz fundamentaler Interessen der EU oder eines oder mehrerer Mitgliedstaaten als geheimhaltungsbedürftig eingestuft worden sind[74]. Hier ist insbesondere an Dokumente aus dem militärischen Bereich zu denken. Auch für diese Dokumente gilt, dass der Zugang nur verweigert werden kann, wenn eine der in Art. 4 genannten Ausnahmen vorliegt. Allerdings sind dabei bestimmte Maßgaben zu beachten, die dem Schutz der in diesem Artikel genannten Interessen dienen. So leuchtet es unmittelbar ein, dass Anträge auf Zugang zu 'sensiblen' Dokumenten nur von Personen bearbeitet werden dürfen, die berechtigt sind, Einblick in diese Dokumente zu nehmen (Art. 9 Abs. 2).

Die zweite große Neuerung enthält Art. 11, der die Organe verpflichtet, ein Dokumentenregister einzurichten, das öffentlich zugänglich sein muss. Diese Maßgabe wird damit begründet, dass dem Bürger die wirksame Ausübung seiner Rechte erleichtert wer-

---

[73] Die Vorschriften des Bürgerbeauftragten über den Zugang zu seinen Dokumenten hatten bereits vorher diese kürzere Frist festgelegt, vgl. Art. 13 Abs. 5 seiner Durchführungsbestimmungen (s. oben Fn. 62).

[74] Vgl. hierzu den Beschluss des Generalsekretärs des Rates/Hohen Vertreters für die Gemeinsame Aussen- und Sicherheitspolitik vom 27. Juli 2000 über die im Generalsekretariat des Rates anzuwendenden Maßnahmen zum Schutz der als Verschlusssachen einzustufenden Informationen (ABl. 2000 Nr. C 239, S. 1).

den soll[75]. In der Tat kann der Bürger sein Recht auf Zugang zu einem Dokument in der Regel nur dann sinnvoll ausüben, wenn er von dessen Existenz Kenntnis hat. Art. 11 Abs. 3 zufolge müssen diese Register spätestens am 3. Juni 2002 funktionsfähig sein.

Die Verordnung 1049/2001 trat am 3. Juni 2001 in Kraft, gilt aber erst vom 3. Dezember 2001 an (Art. 19). Dadurch wird es den Organen ermöglicht, ihre bestehenden Vorschriften über den Zugang zu Dokumenten an die Bestimmungen der Verordnung anzupassen[76].

VI. Ausblick

Die Entscheidungen des Europäischen Bürgerbeauftragten haben bei der Bestimmung des Umfangs wie auch bei der Durchsetzung des Rechts auf Zugang zu Dokumenten eine bedeutende Rolle gespielt. Die Zukunft dieses Rechtes wird nicht zuletzt davon abhängen, wie die Grenzen zu bestimmen sind, welche ihm durch die Belange des Datenschutzes gezogen werden. Man darf auf die weitere Entwicklung – auch der Praxis des Bürgerbeauftragten - gespannt sein.

---

[75] Vgl. die 14. Begründungserwägung der Verordnung und den Wortlaut von Art. 11 Abs. 1.

[76] Vgl. die 17 Begründungserwägung der Verordnung.

Dr. Otto Ulrich
Europäische Akademie zur Erforschung von Folgen wissenschaftlich-technischer Entwicklungen

Das Internet – Chance und Risiko für die Demokratie: Kann der Globalisierung eine demokratische Richtung gegeben werden?

„Während die nationalstaatlich
gebundene Gesellschaft zum
sozialen Problem wird,
eröffnet der Horizont der
Weltzivilisation eine
neue Epoche der Kultur."
Rüdiger Altmann

Lässt sich die Technologie des Internet mit demokratischen Prinzipien synchronisieren? Sind wir jetzt, mit dem Internet, auf dem Weg in eine kosmopolitische Demokratie? Die virtuelle globale Zivilgesellschaft – als Trägerin eines „Internet-Parlaments" – kann ein notwendiges Gegengewicht zum unkontrollierten globalen Zugriff auf die Privatheit der Bürger werden.

„Das Internet verhält sich zur Privatheit der Bürger wie einst das Gewehr zum Büffel."
Eindeutig erkennbarer wird, dass die globale Revolution zu einer vollständigen Veränderung der sozialen Verhältnisse der Welt führt. Darf diese Entwicklung an der Demokratie, an der sich nun mit Hilfe des Internets bietenden Chance zur Weiterentwicklung der Demokratie, vorbeigehen – zumal die Glaubwürdigkeit der Parteiendemokratie sich weiter auflöst? Die Internet-Ökonomie blüht im globalen Maßstab auf – und was ist mit der Globalisierung der Demokratie? Hat es nicht darum zu gehen, den von technischen und ökonomischen Funktionseliten vorangetriebenen neoliberalen Prozess ihres globalen einseitigen Zugriffs auf die Welt zu demokratisieren? Dabei hat die Sorge zunächst nicht der Zukunft der politischen Parteien zu gelten. Die von diesen jahrelang betriebene Aufrüstung hat sie zu Machtkampfverbänden gewandelt, in Konkurrenz miteinander um

Machterhalt und Machtgewinnung kämpfend, um damit aber das, was ihnen anvertraut wurde, die Demokratie, zu einer vom Volk abgeschotteten Konkurrenzdemokratie verkommen zu lassen. Der Bürger wendet sich ab und den Infotainments im „Web“ zu, auch wenn die aktuell aufgebrochene Demokratie-Krise im Sinne seiner Bürgerrechte durchaus und endlich die Chance formulierbar macht, die unter der parteienstaatlich gesteuerten „demokratischen“ Eliteherrschaft steckengebliebene Demokratie – nun in globalem, kosmopolitischem Maßstab – weiter zu entwickeln. Die aktuelle Diskussion um eine „elektronische Demokratie“ muss in Dimensionen hineingestellt werden, die den neuen technologischen Möglichkeiten des Internets angemessen sind.

Wie sonst soll es gelingen,

- dem umfassenden Handelsregime der World Trade Organisation seine Grenzen zu setzen,
- die globale Ausbeutung von Mensch und Natur durch soziale und ökologische Leitplanken zu begrenzen und einzustellen,
- ohne internationale Wettbewerbsordnung die internationalen „feindlichen Übernahmen“ an soziale Standards zu knüpfen, um sie damit zu verhindern, damit endlich die zerstörende Konkurrenzwirtschaft in eine globale „Kooperationswirtschaft“ hineinwachsen kann,
- ohne internationale Währungsordnung den spektakulären „Casino-Kapitalismus“ zu bändigen,
- das totale Durchlöchern der im „Web“ repräsentierten „elektronischen Privatheit“ zu verhindern

wenn es auch weiterhin keine globale Demokratie gibt, die etwa den Umweltschutz, den Schutz der Kinder, den Generationenzusammenhalt, die wachsende weltweite Armut, den Analphabetismus, den Datenschutz, also dass der bürgerlichen Gesellschaft konstitutive Recht auf Privatheit an eine human-sozial, ökologisch und demokratisch ausgerichtete Globalisierung anbindet? Die Zeit rückt näher und erkennbarer wird, was unabdingbar kommt, nämlich dem von mächtigen Nationalstaaten und multinationalen Konzernen vorangetriebenen Prozess der Globalisierung sowohl eine demokratische Richtung zu geben als auch ein kosmopolitisch-zivilgesellschaftliches Gegengewicht entgegen zu stellen.

Glänzender, aber unausgewogener Start ins Internet-Zeitalter

Wer über die Zukunft spricht, spricht heute von der „Informationsgesellschaft“; es wird davon gesprochen, wir seien gar auf dem Weg in eine „elektronische Dienstleistungsgesellschaft“, von einer neuartigen „digitalen Online-Ökonomie“ ist zu hören – und das Internet, soviel steht fest, ist der Schlüssel zur Entwicklung in globale Dimensionen. Wird das Internet nur Gewinner kennen? Auf den ersten Blick sieht es so aus: Das Internet wächst mit phänomenaler Geschwindigkeit. Geschätzt wird, dass bis zum Jahr 2004 allein in Westeuropa die Zahl der Erwachsenen mit Internet-Zugang von derzeit 50 Millionen auf schätzungsweise 121 Millionen steigen wird. Das Internet verbreitet sich auch rascher und in größerem Umfang als jede Kommunikationstechnologie zuvor. So dauerte es beispielsweise 35 Jahre, bis das Medium Radio 50 Millionen Zuhörer zählte, und was das Fernsehen angeht, verstrichen immer noch 13 Jahre, bis die gleiche Zahl an Zuschauern erreicht war. Demgegenüber wies das Internet nach gerade einmal 4 Jahren schon die gleiche Nutzerzahl auf. Dieses rapide Wachstum und die hohe Akzeptanz legen die Vermutung nahe, dass sich das Internet anschickt die Gesellschaften in ähnlich dramatischer Weise zu verändern, wie dies die im 18. Jahrhundert aufkommenden Manufakturen als Wegbereiter der industriellen Revolution taten.

Die andere Seite – und das gehört auch zur Bestandsaufnahme – ist aus UNESCO-Quellen ablesbar: Der Erwerb eines Computers entspricht in den USA einem Monatseinkommen, in Bangladesh muss dagegen das Einkommen von 8 Jahren aufgebracht werden; 74 Prozent der Telefonleitungen in der Welt werden von dem reichsten Fünftel der Weltbevölkerung genutzt, 1,5 Prozent dagegen von dem ärmsten Fünftel und insgesamt nur 55 Länder tätigen 99 Prozent der gesamten Ausgaben für Informationstechnologie.

Um so berechtigter ist es zu fragen: Wo steht, dass nicht auch Rechtsstaatlichkeit, Demokratie und universalistische Prinzipien der Menschenrechte unter die Räder dieser großen, die „Welt“ als Cyberspace umfassenden Entwicklung kommen? Anzunehmen ist, dass mit einer „wie von selbst“ aus der Internet-Technologie kommenden *Berücksichtigung* von „Demokratie“ und entsprechenden demokratiefördernden Strukturen nicht zu rechnen ist.

Schon immer mussten technische Neuerungen, bevor sie tragende Stützen der weiteren Demokratisierung werden konnten, erst als solche vom Volk ergriffen werden – was bei der Internet-Technologie momentan auf dem Wege zu sein scheint. Aber von einem sich selbst erfüllenden Automatismus hin zu mehr Demokratie – jetzt im globalen Maßstab – kann überhaupt keine Rede sein. Wie stets, so auch hier, wenn nicht mitgehalten wird, liefert die neue Technologie auch neue Waffen um anti-universalistische Affekte zu schüren, also Tendenzen zu verstärken, die latent vorhandene Demokratieverachtung strukturell zu zementieren – etwa durch neuartige Abhörmethoden oder durch fehlende Aufklärung über die Risiken der Nutzung des elektronischen Handels für die informationelle Selbstbestimmung.

Wer ist das „Volk“ im Cyberspace?

Schon immer standen Technik und Demokratie in einem spannungsreichen Verhältnis. Jetzt, mit dem anscheinend unaufhaltbaren Siegeszug des Internets, entgleitet diese Technologie aber vollends der Politik, wie der Moral – und der nationalstaatlichen wie territorialen Gebundenheit von Rechtsstaatlichkeit und Demokratie. Deshalb: Sind wir wirklich mit all unserem neuen Reichtum an Internet-vermittelten Informationen auf dem Weg in eine dem Menschen gemäße, also in eine dem Wesen der Demokratie gemäßen Entwicklung – und das in kosmopolitischer Perspektive? Reicht es aus, technologische Metaphern – wie die „Informationsgesellschaft“, den „virtuellen Raum“, den „Cyberspace“ – zur Beschreibung von gesellschaftlicher Zukunft zu bemühen? Wird da nicht zu kurz gedacht? Welche Türen schließen sich, welche Gestaltungsansätze werden erst gar nicht sichtbar – geeignet, die unabdingbar notwendige Globalisierung zu demokratisieren? Wächst nicht die Erkenntnis, dass wir, wenn wir nur auf die Faszination der immer neu sich gebärenden technischen Möglichkeiten starren, steckenbleiben?

Vergewissern wir uns wo wir stehen: *Arnold Toynbee*, der große englische Historiker, hat in seinen Studien über die Gesetze des Niedergangs einst blühender Gemeinwesen ein für allemal auf die „versteckten Kosten“ einseitiger sozialer Entwicklungen aufmerksam gemacht: Schon immer, durch alle Zeiten hindurch, war es so, dass hochentwickelte Gesellschaften sich nicht davon befreien

konnten, spätestens dann auf dem Weg des Niederganges zu sein, wenn *Wirtschaft und technologische Entwicklung* einerseits, *Staat und Politik* andererseits, und die *kulturell-geistige Entwicklung der Menschen* zum Dritten nicht mehr in einem sich ausbalancierenden Gleichgewicht standen.

Das zivilgesellschaftliche „Internet-Volk“

„Ein Volk als Ganzes gibt es nicht“ sagte Karl Jaspers, aber das Volk als Erfahrungsgemeinschaft vielleicht doch, denn was ist mit jener Gemeinschaft von Menschen im Cyberspace, die, verteilt über den Globus, sich im Netz „trifft“, um sich – jetzt als virtuelle Gemeinschaft – per E-Mail, per Websites, im „Chat-Room“ (und demnächst ergänzt um Telekonferenzen) im Internet digital über Erfahrungen auszutauschen? Wächst da nicht millionenhaft rund um den Globus (neben all dem Schwachsinn, der da „kommuniziert“ wird) eine neue Identitätsgemeinschaft, also eine neue weltweit vernetzte Erfahrungsgemeinschaft heran, die es ohne die technischen Möglichkeiten des Internets nicht geben würde? Daraus müssen sich doch Folgerungen für eine Globalisierung der Demokratie ableiten lassen. Jene Millionen Internet-Nutzer, die via „Web“ gemeinsam in Fragen aktiv sind, die als Schicksalsfragen der Menschheit rund um den Globus zu verstehen sind, also alle angehen, – muss diese virtuelle Netzgemeinde, dieses „Internet-Volk“, nicht als virtuelle Repräsentanz der längst existierenden globalen wie lokalen Zivilgesellschaft verstanden werden?

Entscheidende Fragen einer auf der Erkenntnis der Natur und des Menschen basierenden Weltsozialordnung bedürfen Antworten auf globale Umweltfragen, Menschenrechtsfragen, Entwicklungsfragen, Gesundheits- oder Friedens- wie Bürgerrechtsfragen. Aber unter den Bedingungen einer parteigesteuerten Zustimmungserzeugung, einer eliteorientierten (Themen-)Filterung bestehen keine Chancen, dass diese politischen Handlungsfelder – zum Zwecke der Herstellung von *Gleichheit der Teilhabe,* von *Generationenverantwortlichkeit* wie *lebbarem multikulturalistischem Pluralismus* – eine ihnen wesengemäße Gewichtung bekämen. Antiquiert ist, weiterhin diese Themen aus der Perspektive der herrschenden Praxis des Ökonomismus wie der parteienstaatlich gesteuerten Selektivitäten zu instrumentalisieren. Denn: die neuen, schon erkennbaren Signaturen

einer sich wandelnden Welt – wozu sicherlich die neue Qualität der Internet-Technologie und offenbar auch die offen gelegte und zu wendende Demokratie-Krise gehört – sollten sie nicht, wie Rüdiger Altmann vorschlug, als „Horizonte einer neuen Epoche der (politischen) Kultur“ auf dem Weg zu einer Weltzivilisation gesehen werden?

Die Filtermechanismen der Parteiendemokratie

Die pluralistische Konkurrenzdemokratie ignoriert systematisch extrasoziale Interessen und nachweltorientierte Verpflichtungen. Als Kompetenzverwalter von *langfristigen*, von *neuen,* von *allgemeinübergreifenden* sowie von *Werte-Verwirklichungsinteressen* fällt das etablierte Institutionenarrangement „demokratischer“ Elitenherrschaft aus – öffentlicher Raum für zivilgesellschaftliche Aktivitäten. Aus dieser Perspektive findet die neue virtuelle Netzgemeinschaft – also das an zivilgesellschaftlichen Fragen arbeitende und in elektronischem interaktiven Austausch befindliche „Internet-Volk“ – als „Weltbürgergemeinschaft“ – im Cyberspace ihren gemäßen neuen „öffentlichen Raum“, geeignet – blitzschnell, unzensiert und millionenfach – Informationen über Erfahrungen, Ideen und Intentionen bis hin zu programmatischen wie aktionistischen Aktivitäten auszutauschen – was, zwar „nur“ netzbasiert, aber immerhin auch, „soziale“ Identitäten wachsen lässt.

Das „Volk“ im Cyberspace ist jene virtuelle Netzgemeinschaft, die ihre soziale, gemeinschaftsbildende Identität aus der Tatsache zieht, als „Wächter der Menschheit“, sowohl Ohr wie Sprachrohr zu sein. Eine „Weltgewissensgemeinschaft“, sensibel und wach, die das Web als virtuelles Vereinslokal nutzt, um Verletzungen wie Versäumnisse gegenüber der „kulturellen Sphäre“ anzuprangern: *„Wenn diese neue globale kulturelle Macht aktiviert wird – und das Netz ist die technologische Basis dazu – arbeitet sie als virtuelle Netzgemeinde nicht in den alten Kategorien von Abstimmung und Wahl. Eher enthüllt sie Themen, die mit Bedeutung, Wahrheit, Ethik, Moral, Glaubwürdigkeit und Legitimität verbunden sind“,* so Nicanor Perlas in seinem Buch: *Shaping Globalisation: Civil Society, Cultural Power and Threefolding*. Jeder Versuch, die Weiterentwicklung der Demokratie im Zeitalter des Internet zu formulieren, tut gut daran, sich hieran zu orientieren.

Wird die typologische Struktur des Internet verkannt?

Weiterhin mit alten Denkformen, etwa mit Rechtsnormen, auf die Informationstechnik zu reagieren, heißt, die typologische Struktur dieser neuen Technologie zu verkennen – diese ist dynamisch, virtuell, (global) vernetzt und „offen“ – im wahrsten Sinne des Wortes! Sie konstituiert eine "neue Wirklichkeit", in der Dienstleistungen zur elektronischen Ladung werden; die Netztopologie des Internet konstituiert jenen „Cyberspace“, in dem neben millionenfachen normalen Nutzern aber auch Cyberterroristen, private Datensammler wie Internet-Warrior und Hacker ihren unkontrollierbaren Machenschaften nachgehen: jede ungeschützt über das „Netz“ laufende Information, also jeder Surf-Schritt, jede E-Mail hinterlässt elektronische Spuren, die von diesen finsteren unbekannten Demokratieverächtern unbeobachtet mitgelesen, manipuliert oder kopiert werden können.

Richtig bleibt; im Internet hat das Menschenrecht auf informationelle Selbstbestimmung keine Heimat: krypthographische Verschlüsselungsverfahren *(„Krypthographie für Alle!“)* können demokratiefördernden Schutz bieten. Eine demokratisch-zivilgesellschaftliche Weltbürgergesellschaft, die das Internet als technologische Basis ihrer sicheren und geschützten Kommunikation nutzt, wird es nur dann geben, wenn der „User“ als Weltstaatsbürger in seinen Rechten, Chancen und Pflichten gegenüber der globalen Mitweltgesellschaft aufgeklärt wird, auch darüber, was Internationalisierung und Wahrnehmung seiner global zu geltenden Weltstaatsbürgerrechte eigentlich heißt.

Daraus folgt wiederum: Die vertrauten Grenzen von Raum, Zeit, Territorium und Nationalstaat wie die vertraute Rolle des Staates werden aus globaler Perspektive aufgehoben – aber dann doch wiederum in spezifisch neuer Form gebraucht, wie noch zu zeigen sein wird. Jedenfalls, mit vertrauten Regelungsprinzipien – wie etwa dem allein rechtlich operierenden Bundesdatenschutzgesetz – kann das "Neue" offenbar direkt nicht gestaltet werden.

Wo stehen wir heute? Die Lage ist schlimm, zumal die Politik – beobachtbar etwa am Beispiel Deutschlands – nicht als starker Partner auf Seiten jener steht, die an einer Zukunft der Demokratie im

Zeitalter des Internet interessiert sind. Eher geht es darum, wie aus den momentanen Antworten der rot-grünen Bundesregierung – etwa dem Aktionsprogramm „Innovation und Arbeitsplätze in der Informationsgesellschaft des 21. Jahrhunderts“ – ablesbar ist, nationale Gestaltungsspielräume so zu nutzen, dass man sich als funktionierender Bestandteil der sich heraus kristallisierenden Mega-Maschinerie ausweisen kann – um damit die schon bestehende eindimensionale Form der Globalisierung zu verstärken.

Demokratie als Anhängsel der Internet-Gesellschaft?

Wer die Förderung der Online-Ökonomie zur Orientierung politischen Handelns macht, um aus dieser Perspektive nach Maßstäben zur Anpassung der „Demokratie“ zu suchen – elektronische Wahlen, virtuelle Parteizentralen – entlarvt sich selbst, nämlich die Zukunft der Demokratie nur aus der Perspektive eines „Anhängsels“ an globale technologische Trends zu verstehen. Damit da keine Missverständnisse aufkommen: Alles was heute als Versuch diskutiert wird, zu einer „direkten elektronischen Demokratie“ zu kommen, ist aufregende Spielwiese, getragen von dem Gedanken „die Praxis des alten Athen zum Vorbild zu nehmen“ (Lawrence K. Grossmann), so, als wenn die alten Griechen schon das Neue des heutigen Internet-Zeitalters gekannt hätten. Das kann es doch wohl nicht sein!

Wer prioritär, allein und gewichtig erst die Stärkung technologischer Trends zum Thema seiner Politik macht, arbeitet den kommerzialisierten und privatisierten Interessen der Global Player zu – wie dies im Aktionsprogramm der Bundesregierung zu besichtigen ist, und zu schwachen Absichtserklärungen zum Thema „Internet für Alle“ führen muss. Aus dieser Perspektive kann nicht ins Visier kommen, worum es zu gehen hätte, nämlich nach einer Weiterentwicklung der Demokratie im Zeichen der neuen Parameter der Internet-Technologie zu suchen, also nach einer Zukunft der globalen Demokratie *mit* Hilfe des Internets zu fragen – und nicht umgekehrt!

Lässt sich Internet und Demokratie synchronisieren?

Vielleicht formuliert die rot-grüne Bundesregierung deshalb so unverbindlich, weil es bislang keine schlüssig formulierte Vision gibt,

wie der von den politischen Parteien heruntergewirtschaftete und ausgelebte „demokratische Zirkus“ am Laufen gehalten werden kann, zumal auch völlig unklar ist, ob sich das Werkzeug Internet überhaupt mit Vorstellungen zum Thema Demokratie und dessen notwendigen Weiterentwicklung synchronisieren lässt?

Die Geschichte zeigt es: Stets waren es technologische Stützen, die zu einer Stärkung und Prägung demokratischer Anforderungen sowie Möglichkeiten zur Teilhabe an öffentlichen Belangen der *res publica* geführt haben. Ob es sich um den *Buchdruck* (Demokratisierung des Lesens), um das *Schießpulver* (Ritterrüstung taugte nicht mehr gegen Musketen) oder um den *Kompaß*, den *Rundfunk*, das *Fernsehen* und heute um den sich massenhaft vernetzenden *Computer* handelt: stets ist der Siegeszug der Demokratisierung des Wissens mit einer wachsenden Ausprägung – wie wir heute sagen würden – globalen Urteilsvermögens und weltweiten Gestaltungswillens einhergegangen – was zu einer heute klar erkennbaren individuell und bewusstseinsmäßig gewollten Ablösung und Herauslösung von obrigkeitlichen und traditionellen Autoritäten führt.

In diesem Sinne will das Internet in seinem Werkzeugcharakter verstanden werden: es muss als potentieller, noch *gestaltungsbedürftiger* Träger verstanden werden. Erst aus dieser Perspektive lassen sich überhaupt *demokratiefördernde* Strukturen definieren, mit denen eine technologische Unterstützung einer wesensgemäßen Entwicklung der Demokratie *mit* dem Internet möglicher wird – beispielsweise durch "freeware" für Alle und Schutz durch technologische Anonymisierung im Netz.

„Freie Software für Alle!“

Grundsätzlich repräsentieren moderne Technologien – und die darauf setzenden Märkte – stets den Geist und die Denkform jener technischen und ökonomischen Eliten, die auf ihren Hochschulen nicht lernen konnten, was es heißt, neben technischen Machbarkeits- wie wirtschaftlichen Marktabwägungsstudien auch den Maßstab einer demokratieverträglichen Gestaltung – etwa von elektronischen Dienstleistungen – kennen zu lernen. Deshalb kann die gegenwärtige Form der Globalisierung auch als ein eindimensionales

Produkt neoliberalen Marktdenkens verstanden werden, denn kaum oder gar nicht wird systematisch gelehrt,

- dass es nicht automatisch im Trend hin zur totalen Digitalisierung liegt, dass dieser aus sich heraus bürgerrechtsfreundliche Strukturen zum Schutz der Privatsphäre generieren wird,
- was es heißen könnte, die Offenlegung des Quellcodes einer Software als essentielle Basis für eine paradigmatisch andere Richtung gesellschaftlicher, mithin also auch demokratischer Entwicklung zu verstehen.

Wer also die Gesellschaft und dessen lebensweltliche Zusammenhänge als System, als Maschine und nicht als lebendigen Organismus versteht, der spiegelt nur das herrschende Weltbild einer im Niedergang, aber gleichwohl noch in voller Blüte stehenden Epoche wieder. Der Mensch ist zum Objekt einer Zweckbestimmung, dem der Mechanisierung, geworden. Der demokratische Zynismus liegt darin, dass im Namen des Souveräns, des Wahlbürgers, also „des Volkes“, die digitale Durchdringung der Gesellschaft weiterhin beschleunigt wird. Damit aber wird genau jenen ohnehin schwach entwickelten Verfahren und rechtsstaatlichen (Verfassungs-)Institutionen – etwa den Einrichtungen des Daten- und Verbraucherschutzes – entgegengearbeitet, zumal gerade diese sich als verbliebende „Bollwerke“ zum Schutz von Bürger- und Verbraucherrechten verstehen. Der öffentliche Raum – Wesenselement einer bürgerlich-demokratischen Gesellschaft – droht unter den zersetzenden Bedingungen globalisierter Märkte weiter zu schrumpfen, und die Politik forciert als nicht-intendierte Folge ihres Handelns diesen Prozess.

Wird Demoskopie mit Demokratie verwechselt?

Es wird versucht, aus der Realwelt entlehnte demokratische Beteiligungsformen – jetzt als virtuelle Parteizentralen, als digitale Wahlkämpfe, als Bürgernetze oder virtuelle Partizipation – mit einer Netztopologie wie dem Internet voranzutreiben. Jeder Versuch, innerhalb der vorgegebenen Logik des Netzes nach einer adäquaten, dieser globalen Technologie angemessenen, Weiterentwicklung der Demokratie zu suchen, greift zu kurz. Verständlich ist der Enthusiasmus, sich mit den Gegebenheiten des Internets zu arrangieren

– dies aber darf nicht mit einer wesensgemäßen, kosmopolitisch angesagten Zukunft einer globalen Demokratie verwechselt werden. Der erkennbare Versuch *Demokratie auf Demoskopie* zu reduzieren, wird in dem lauter werdenden Ruf nach „Fernbedienung für Alle!“ einmünden; dies wird dann gar für eine Strategie gehalten werden, zumal, wenn dies, was absehbar ist, mit dem Trend hin zum WebTV begründet wird. Wer die Weiterentwicklung der Demokratie als Teledemokratie versteht, meint *Zuschauerdemokratie*, meint, dass im zustimmenden oder ablehnenden Zappen per Fernbedienung über vorgegebene Alternativen der angemessene Ansatz liege, um den neuen Medien gerecht zu werden. Die Trends laufen hin zur Zapper-Demokratie. Nur, dies hat nichts mit Demokratie, mit dem Ringen um Argumente, mit Verständigung über Grenzen, mit dem Mündig-werden, mit der Kunst der Begegnung mit anderen, zur Mündigkeit strebenden Menschen, kurz mit einer wesensgemäßen (Weiter-)Entwicklung der demokratischen Idee unter den sich wandelnden Bedingungen einer selbstbewusster werden Bürgergesellschaft zu tun. Die Bürger wissen mit parteienstaatlich zementierten „demokratischen“ Abstimmungsritualen immer weniger anzufangen – und wollen es offensichtlich auch nicht.

„Demokratie ist kein Universalrezept für eine besonders bemerkenswerte Staatsform, sondern die ständige Mahnung an Menschen, auf eine bestimmte Art zu leben: verantwortlich, autonom, in selbstbestimmten Gemeinwesen, die dennoch für Fremde offenbleiben, in Toleranz und gegenseitiger Achtung, aber mit einem guten Gespür für eigene Werte“, wie dies Benjamin Barber in seinem Buch: *Demokratie im Würgegriff* formuliert. Und dies ist anschlussfähig an ein Verständnis von *wesensmäßiger Entwicklung,* das an dem aus der ökologischen Debatte her bekannten Konzept einer *nachhaltigen Entwicklung* anknüpft, aber entscheidend weitergeht, in dem es nämlich zurückführt und wieder in den Blick nimmt, was zwar in den Herrschaftszeiten der Parteiendemokratien verloren gegangen ist, aber weiterhin Demokratie ihrem Wesen nach ist, nämlich soziale Ausdrucksform menschlicher Gemeinschaft.

Auf dem Weg in eine kosmopolitische Demokratie?

Das wäre der Maßstab, so lässt sich das Demokratie-Ideal formulieren, wie aber lässt es sich in einen, als Weltbürgergesellschaft formierenden Alltag zur wesengemäßen Entfaltung bringen?

Als Tatsache kann wohl gelten: Das heutige globale Laissez-faire muss als Durchgangsstadium in der noch jungen Geschichte der sich nunmehr deutlicher herausbildenden Weltwirtschaft und nicht als ihr Endpunkt verstanden werden: „Es bringt nichts, dem herrschenden Marktfundamentalismus auf lokaler Ebene entgegen zu steuern und ihm auf der globalen Ebene die Herrschaft zu überlassen“, schreibt Anthony Giddens in seinem Buch über die *Erneuerung der sozialen Demokratie*, um dann in der Verbreitung der kosmopolitischen Demokratie eine (kommende) Bedingung zu sehen, um das demokratisch unkontrollierte Zusammenwirken von Regierungsvertretern und Managern der Großkonzerne zu beseitigen und einzudämmen.

Aber wie geht das? Wie müsste eine Netzpolitik aussehen – wer wären die Akteure? – um demokratische Prinzipien mit Unterstützung des Internet zu globalisieren? Stichworte wie „globales Regieren“, „Regieren ohne Regierung“ verweisen darauf, wie Bernd Lutterbeck feststellt, „dass die globale Ökonomie(!) als ein Gebilde zu verstehen ist, in dem neue internationale Regimes und nationale Regimes zusammen wirken müssen, um verbindliche Entscheidungen zu treffen.“ Ist dieses hierarchielose Steuerungsprinzip übertragbar auf die Herausstellung von „virtuellen Strukturen“, die als „Basis“ eines zivilgesellschaftlich orientierten „Internet-Parlaments“ – mit sicheren Zugangsbedingungen, eigener Website, mit Logo und „hoheitlichen“ Symbolen und Entscheidungsfindungsverfahren ausgestattet – dienen können, oder ist das alles zu wenig aus dem Geist der im Virtuellen herrschenden binären Logik der Digitalisierung und der eigenen Logik des globalen Netzwerkes gedacht?

Mag sein. Aber Tatsache bleibt, eine Weltinnenpolitik – die sich den Namen verdienen will – kommt nicht daran vorbei, die Technologie des Internet als ihr Organ zu nutzen, auch, aber nicht nur, um den Kosmopolitismus „von unten“ abzubilden: Jene, nicht-hierarchisch organisierten nicht-staatlichen Organisationen – die *„Nicht-Regie-*

rungs-Organisationen“ – die Ziele verfolgen, die sich auf die Lebensbedingungen der Menschheit und ihrer Mitwelt richten, sind längst klar zu identifizieren: Sie bilden – wie beispielsweise Greenpeace oder Amnesty International oder Privacy International – den Kern der ins Virtuelle wachsenden globalen Zivilgesellschaft. Vom virtuellen Vereinslokal zum globalen „Internet-Parlament“? Warum nicht? Bricht eine neue Zeit des utopischen Denkens an? Vielleicht ist es aber auch gar nicht so utopisch für den, der auf die Trends achtet, die die Diskussion um „Internet Governance“ – also das „Regieren ohne Regierung“ – immer weiter nach vorne rücken:

- mehr globale Strukturen und Institutionen,
- transkulturelle Verständigung über universelle Grundwerte,
- einen globalen Rechtsrahmen,
- eine Weltsozialordnung,
- neue global-national-lokale parlamentarische Kooperationsbündnisse zwischen „Internet-Parlament“ und nationalstaatlichen Parlamenten zum Zwecke der Herstellung demokratischer Legitimation und Handlungsverbindlichkeit,
- sichere und geschützte Infomationszugangsrechte für Alle,
- die politischen Parteien im Wandel, hin zu Innovationsmotoren gegenüber den Bürgern in Sachen Internationalismus und Weltstaatsbürgerschaft.

Globales Regieren und globale Zivilgesellschaft gibt es längst – und das Internet steht für eine neue Qualität des globalen Konzertierens und Bündelns von zivilgesellschaftlichen Interessensaspekten. Die absehbare Herausbildung einer netzgestützten kosmopolitischen Demokratie in „Form“ des „Internet-Parlaments“ ist – gemessen an den heute schon „im Netz“ laufenden „Abstimmungen“ – vielleicht auch nur noch eine Zeitfrage, denn eine Erneuerung der Demokratie als deren Weiterentwicklung im globalem Maßstab ist angesagt.

Verwendete Literatur:

Altmann, R.: *Abschied vom Staat.* Frankfurt 1998
Banse, G.: *Nachhaltigkeit ohne Technik?* In: technica didactica. Zeitschrift für Allgemeine Techniklehre. 1.jg. 1997, Bd.1. 5 – 30
Barber, B. R.: *Demokratie im Würgegriff.* Frankfurt 1999
Beck, U.: *Was ist Globalisierung?* Frankfurt 1998

Fricke, W., (Hrsg.): *Was die Gesellschaft bewegt.* Jahrbuch Arbeit und Technik 1999/2000. Bonn 1999
Giddens, A.: *Der dritte Weg.* Die Erneuerung der sozialen Demokratie. Frankfurt 1999
Grossmann, L. K.: *Der Traum des Nebukadnezar*. In: Leggewie/Maar (Hrsg.): *Internetpolitik*. Von der Zuschauer- zur Beteiligtendemokratie. Köln 1998
Held, D.: *Global Transformation: Politics, Economy and Culture.* Cambridge 1999
Lutterbeck, B.: *Globalisierung des Rechts – am Beginn einer neuen Rechtskultur?* In: Computer und Recht, Heft 1, 2000, 52 – 60.
Nuscheler, F.: (Hrsg.): Entwicklung und Frieden im 21. Jahrhundert. Zur Wirkungsgeschichte des Brandt-Berichts. Bonn 2000
Perlas, N.: *Shaping Globalisation: Civil Society, Cultural Power and Treefolding.* Stuttgart 2000

Ewa Kulesza
The Inspector General of Poland for the Protection of Personal Data

Protection of Personal Data in Poland – First Experiences.

The Polish Act on the Protection of Personal Data, was adopted on 29th September 1997. Earlier, in Poland, there were no legal rules providing for citizens' data protection. Even on the contrary, in the communistic system the legal provisions and public authority activity imposed upon citizens the obligation of providing public bodies with any information, regardless of whether those data were adequate to the purpose for which they had been collected, and whether there was a basis of requesting for such data. Filling all forms without questioning the purpose and legal basis of requested data became a habit which also affected relations between citizens and the private sector.

The idea of introducing the data protection regulation in Poland arose at the moment when the new Constitution was created in 1997. Citizens' right to protection of their personal data is guaranteed under article 51 of the Polish Constitution and developed in the Act on the Protection of Personal Data. This right is still not clear for citizens. However an understanding of regulations and a consciousness of vested rights comes together with the experience gained both by the bodies obliged to guarantee the rights and by the citizens themselves. Judicial decisions and literature influences upon this right as well. That is why there is a need to explain the provisions of the Act on the Protection of Personal Data and the constitutional right to protection of such data and a need to undertake the activities which will be the guidelines for citizens. The Act on the Protection of Personal Data was the basis of appointment the independent body (the Inspector General for the Protection of Personal Data) which may exercise wide powers. This lecture presents exercising of some tasks and experiences gained during the first three years of functioning of the Act.

Educational activity

The entering into force of the Polish Act on the protection of personal data has caused some additional, negative and unexpected effect. Many people recognised that the provisions of the Act, despite the legislator's intentions, prohibit providing any information containing personal data without the data subjects' consent. According to this, referring to the Act, citizens refused to provide information even when the regulations were the basis of the requesting of data. Even public bodies refused to provide information necessary for the conduct of matters by other bodies.

Consequently, immediately after the Act became the law, data protection authority had to initiate an educational activity addressed to both citizens and public institution officials and private sectors.

As a part of this educational activity, the widest range of media were employed. Citizens rights providing for personal data protection and the controllers; obligations linked to it were explained in television and radio interviews given by the Inspector General and the employees of the Bureau and during press conferences. The provision of the Act on the Protection of Personal Data were also widely explained and commented on in both the daily and professional press. Although three years have passed since the Act was passed, in the legal section of one of the leading Polish newspapers - "Rzeczpospolita", a special column devoted personal data protection is published regularly. It offers explanations regarding the application of the Act on the Protection of Personal Data and it has to be admitted that it is very popular. The national press has twice been used to publish the Inspector's announcement reminding the controllers of the necessity of fulfilling the registration obligation. It has to be admitted that these announcements, published on the front pages of all national newspapers produced an effect in the form of considerable increase of the number of file registrations.

After the organisation the Bureau of the Inspector General frequently updated web site was created which contains the binding legislation (the Act and law enforcement provisions) regarding personal data protection, up-to-date jurisdiction by the Inspector General and explanations of the provisions of the Act, the Inspector

General's annual reports of her activity submitted to the Parliament (Sejm), Supreme Administrative Court jurisdiction and Supreme Court jurisdiction, bibliography regarding data protection, reports from conferences and meetings the Inspector's employees have participated, international legal acts and the documents adopted by European institutions.

Within the framework of popularising the idea of personal data protection both the Inspector General and the employees of the Bureau participated in the lectures and thematic seminars, meetings (e.g. in 1999 training meetings for self-government employees regarding the Act on the Protection of Personal Data were held).

The most interesting experiences have come form contacts with the private sector. Unfortunately not all of them. Large insurance companies which have their mother company in Western Europe, reacted the most rapidly to the entering into force the Act on the Protection of Personal Data. These companies were the first to ask questions e.g. concerning the possibility of transferring personal data abroad to their mother companies to notify of the files to be registered. Contact was established with one of the first economic self-government – the Polish Chamber of Insurance in order to discuss some questions (e.g. the content of the clause concerning the consent of the insurance company's clients to the processing of their medical data). It has to be admitted that these contacts were very interesting for both sides and also were beneficial for the insurance company's clients. At present I am not in receipt of any complaints from citizens regarding insurance companies' activity.

Contacts with the banks were finally also very positive. Citizens bring many complaints concerning banking activity. These complaints concerned mainly questioning bank practices of using clients' personal data without their consent. Finally, as a result of many meetings and discussions both with the banking economic representative body, as well as of meetings with wide circles of every bank's representatives (such meetings took place repeatedly), the banks have conformed to determined rules (regarding e.g. the adequacy of the processing data) and some satisfactory forms of co-operation have been established. At present for example, the complaints about banks' activity are examined by the Inspector

General, who handles them on the basis of the Act on the Protection of Personal Data, but also are sent to for the attention of and for the examining, according to internal procedures by the banks economic representative organisation.

On the other hand contacts are difficult with public sector institutions and bodies, especially with central administration bodies which do not fulfil the obligations stipulated by the Act on the Protection of Personal Data and are not inclined to co-operate with the Bureau of the Inspector General.

Citizens' complaints

More then 700 complaints concerning the public and private sector controllers are brought to the Inspector General per year (761 complaints were brought in 2000). Generally these complaints concern too broad scope of requested data and lack of basis to collect data or using data incompatible with the purpose for which data were collected. However only 40 percent of complaints is justified. The rest of them results form lack of appropriate legal knowledge or lack of understanding of law. Therefore there were complaints on e.g. collecting data by social assistance institution while the provision of the Act on Social Insurance System precisely determine the scope of data and the procedure of collecting data (including sensitive data). Similarly, the complaints on collecting data using for domicile recording purposes can not be justified because the Act on Population Record enumerates in detail data which may be requested by authority during registration of domicile.

However in some cases the complaint which is not justified may be the basis of the official address to competent authority (a signalling), with indicating doubts concerning the scope of personal data. For example there was a signalling addressed to the Minister of Internal Affairs and Administration because the Act on Population Record requires giving as many as 15 personal data for domicile registration purpose.

On the other hand some complaints concerning e.g. the scope of data collected by insurance companies, telecom companies or

banks were fully justified.[1] These subjects very often require at the moment of entering into a contract with clients not only wider scope of data than it is provided by law (e.g. Telecommunications Act) but also various testimonials for checking clients' liability.

In many cases the complaints concern using data for the purpose other than they were collected for. These complaints were lodged both by private and public sector. For example the complaints concerned: using bank clients data to promote an open pension fund's offer; using data from address bureau for the marketing purposes by private companies and private schools; using by the police the picture of the person being the subject of checking proceeding which was later discontinued. These pictures were placed in the album of "presumptive suspects" which is shown to the victims of the offences. There were also signalled unjustified practices of administrative bodies, public prosecutor's office and the police consisted in the notification made by one copied document included all private addresses, which was sent to all participants in legal proceeding (also injured persons) informing of the closure of the proceeding.

Relatively considerable quantities of complaints concerned disclosure of data to the journalists who were using exact information about persons (including their private addresses) in publications and television information. On this occasion the Inspector General questioned judge's practice of making files of a criminal or civil cases available to the journalists before passing the judgement.

The complaints on processing sensitive data were in a category by itself. The provision of Polish Act provides that sensitive data are data revealing racial or ethnic origin, political opinions, religious, party or trade-union membership, as well as data concerning health, genetic code, addictions or sex life and data regarding criminal convictions. These data may be processed on the basis of data subject's written consent or the provision of other law provide for the processing of such data or processing is required for the purposes of preventive medicine, the provision of care or treatment or processing is necessary for the purposes of carrying out statutory objectives of churches or other religious unions, associations, founda-

[1] In this lecture, for the sake of it's volume, are given only some examples of justified complaints.

tions and other non-profit-seeking organisations or institutions with a political, scientific, religious, philosophical or trade-union aim and the processing relates solely to the members of those organisations or institutions. This is why the complaints on employers illegitimately requested employees data concerning his/her confession were fully justified. The labour law provisions do not provide for collecting such data by employer and in fact there is no reasonable grounds for it. The same concerns the complaints on employers requested lists of trade-unions members. The complaints on the clauses of consent to collect medical data inserted in a insurance companies contracts without clear indicating from whom data are collected and without determining the scope of medical data to be collected, were justified. The complaints on judicial practice putting on the envelopes information of character of written statements of claim or defence in a court action (e.g. “indictment act”).

Separate group of complaints constitute the complaints on coping identity cards by both private and public sector. The Inspector General questioned this practice and indicated that in this case copying of Polish identity cards is leading to collecting data not adequate to the purpose (e.g. image of the person, description of outstanding features, information about children or former places of residence). This legal issue will be the subject of Supreme Administrative Court’s judgement.

At the same time it is to be stressed that in many cases the complaints concern the refusal of providing information e.g. community authorities (making reference to the Act on the Protection of Personal Data) refused to provide information on malfeasants addresses (necessary to bring a case in competent body) on request of the city guard or the police. Also the police refused providing of the perpetrator of the accident address in case when the victim want to sue for damages to civil court. The Social Insurance Institution being asked by social assistance body refused providing information concerning the right to cash benefits and the amount of these benefits paid given person by The Social Insurance Institution.

Inspection activity

The Inspector General and inspectors authorised by him/her are empowered under the Act to carry out the inspection of the controllers. The inspection comprises the compliance of data processing with the provision on the protection of personal data (the compliance of the purpose, the scope and premises of data processing with the provisions of the Act, technical and organisational safeguards). Technical and organisational conditions which should be fulfilled by the controllers are provided in general by the Act on the Protection of Personal Data and in more detailed way by law enforcement provision to the Act –The Regulation of June 3, 1998 by the Minister of Internal Affairs and Administration as regards establishing basic, technical and organisational conditions which should be fulfilled by devices and information systems used for the personal data processing.

The inspectors authorised by the Inspector General are empowered, in particular: to enter any premises where the registered data filing systems are being kept and to perform necessary examination of devices, demand written or oral explanations and presentation of documents. In case of revealing any breach of the provision on personal data protection, the Inspector General is authorised to order the controller by means of an administrative decision to restore the proper legal state, and in particular: to remedy the negligence; to complete, update, correct, disclose or not to disclose personal data; to apply additional measures protecting personal data; to safeguard the data or to transfer them to other parties, to erase personal data.

From the beginning of the Inspector General's activity, the inspection activities were carried out according to the annual inspection's plan and as a result of complaints brought to the Inspector General. More than 100 inspections are carried out a year (127 inspections were carried out in 2000), in public and private sector. For example: 19 inspections were carried out in marketing companies, 9 in banks, 7 in insurance companies, 6 in central and local administration bodies (e.g. the Prime Minister's Chancellery and the Supreme Chamber of Control)

In general it was found that large companies such as banks, insurance companies, which have on it's disposal both proper equipment and reacquired documentation, are prepare best to safeguard their data filing systems. Whereas private sector companies have breached the provisions on personal data protection in the context of the scope of requested data and insufficient processing premises most often.

The public sector fulfils definite obligation much worse. In most cases inspections revealed: lack of appropriate technical safeguards of the information systems, lack of person responsible for the protection of personal data and authorised to data processing, lack of instructions or instructions fulfilled the minimal requirements regarding the procedure in case of breach of personal data safety.

The positive result of the inspections was in many cases eliminating the incompatibilities just when the inspection was under way, because very often these breaches were caused by incomprehension of law. It also happened that as the result of inspection, the controller carried out the activities in view of putting the information system in order. This is why relatively not many decisions ordered to eliminate the incompatibilities have been issued (22 decisions in 2000).

Registration of Personal Data Filing Systems

Under the Act the controller shall be obliged to register a data filing system. According to article 43 of the Act, this obligation shall not apply to the controllers of such data which: constitute a state secret, were collected by e.g. the police during it's operational-investigation activities, are processed by relevant bodies for the purpose of court proceedings, refer to the persons employed by them, their members or trainees, are being publicised, refer to persons availing themselves of their health care services, notarial or legal advice. The release from this obligation does not release form other controller obligations provided by the Act.

The registry proceeding does not mean only taking of cognisance of the fact that such filing system is conducted. The notification is only the basis of checking whether legal basis of processing exists or

whether the scope of data is in compliance with law and the data filing systems are properly protected.

From the beginning of our activity 75 thousand data filing systems were notified to registration. 50,000 of them were registered by the end of 2000. Approximately 3000 new data filing systems are notified a year(2801 files notified in 2000). In 2000, in 880 cases the registration was refused or the notification was made by unauthorised subject. The explanatory proceeding in connection with incomplete documentation were led in 4500 cases.

Summary

The above lecture presents experiences of the Inspector General's activity from the first three years of functioning of the Act. First experiences show that at this moment, thanks to introducing the Act on the Protection of Personal Data, the rules concerning processing personal data have been ordered. The controllers obligations have been clearly determined and illegitimate, wide using of personal data without the knowledge and the consent of data subject has been stopped.

However taking into consideration the experience of the countries introduced personal data legislation long before now, the change of citizens and controllers awareness calls for much more time.