



JÖRG TAUSS

MITGLIED DES DEUTSCHEN BUNDESTAGES

ABB-Datenschutzforum am 04. Mai 2001: „Wohin steuern Datenschutz und Datensicherheit - sind Sie und Ihre Unternehmen fit für das 21. Jahrhundert“?:¹

Zwischen Minimalismus und Modernisierung - Herausforderungen für ein zeitgemäßes Datenschutzrecht

Sehr geehrte Damen und Herren,

ich danke Ihnen herzlich für die Einladung zu dieser ABB-Datenschutzveranstaltung. Gern habe ich die Einladung der Veranstalter angenommen, auf dieser Veranstaltung ein Statement zu dem Thema „Wohin steuern Datenschutz und Datensicherheit in Deutschland – was ist Gegenstand der “ zu übernehmen.

Gestatten Sie mir zuvor jedoch eine kurze Bemerkung dazu, wie ein Forschungs- und Medienpolitiker zum Datenschutz kommt. In der letzten Legislaturperiode war ich für die SPD-Bundestagsfraktion Berichterstatter bei der Beratung des Informations- und Kommunikationsdienstegesetzes (luKDG - besser bekannt als Multimedia-Gesetz) und damit auch des Teledienstedatenschutzgesetz (TDDSG) im damaligen Ausschuss für Forschung, Bildung, Technologie und Technikfolgenabschätzung, in dessen federführender Zuständigkeit die Beratung dieses Gesetzesvorhaben lag. Im Nachhinein hat sich diese Federführung des BMBF und dieses Ausschusses als sehr positiv erwiesen, gelang es doch dadurch, innovative neue Denkansätze in die Datenschutzdebatte einzubringen. Gerade die mit dem TDDSG entwickelten neuen und innovativen Datenschutzansätze haben dazu beigetragen, daß mich das Thema Datenschutz seither nicht mehr losgelassen hat. Für die SPD-Bundestagsfraktion haben meine Kollegin Ute Vogt und ich mit großartiger Unterstützung namhafter Daten-

¹ Jörg Tauss, Mitglied des Deutschen Bundestages, stv. forschungspolitischer Sprecher der SPD-Bundestagsfraktion, Mitglied in den Bundestagsausschüssen für Bildung und Forschung sowie Kultur und Medien. Wahlkreis: Karlsruhe-Land. Korrespondenzanschrift: Jörg Tauss, MdB, Bundeshaus NHA 103, 53113 Bonn, joerg@tauss.de.

schutz-Experten Ende des vergangenen Jahre einen Entwurf für ein „Eckwerte-Papier“ mit dem Titel „Modernes Datenschutzrecht für die (globale) Wissens- und Informationsgesellschaft“ vorgelegt.² Ziel unserer Bemühungen war es vor allem, diese neuen Datenschutzkonzepte wie die Prinzipien Datenvermeidung und Datensparsamkeit in Ergänzung zum „traditionellen“ Datenschutz auch für die allgemeinen Datenschutzregelungen fruchtbar zu machen, um so zu einem der Informations- und Wissensgesellschaft angemessenen und wirksamen Datenschutz zu gelangen.

Doch genug der Vorrede. Das Thema meines Eröffnungsvortrages lautet: „Zwischen Minimalismus und Modernisierung - Herausforderungen für ein zeitgemäßes Datenschutzrecht“. Diesem Thema möchte ich mich in drei Schritten nähern:

So soll zunächst, in der gebotenen Kürze, auf die - kaum noch bestrittene - **dringende Notwendigkeit einer umfassenden Modernisierung des deutschen Datenschutzrechtes** angesichts der immensen Herausforderungen durch neuen Techniken aber auch angesichts der Herausforderungen durch die europäische Integration sowie die zunehmenden Globalisierungsprozesse eingegangen werden. Anschließend möchte ich mich der politischen Debatte, die wohl zu Recht mit den beiden Polen **Minimalismus vs. Modernisierung** beschrieben werden kann, widmen. Drittens schließlich möchte auf die **rechtspolitischen Vorhaben der neuen SPD-geführten Bundesregierung** im Bereich des Datenschutzes eingehen, die sich **der Herausforderung der Entwicklung eines modernen Datenschutzkonzeptes als zentrales Reform- und Modernisierungsprojekt stellen will** und stellen wird.

1. Herausforderungen an das Datenschutzrecht durch neue Technik und durch die europäische Integration

Gestatten Sie also zu Beginn einige Anmerkungen zu den immensen Herausforderungen an das lange Zeit bewährte deutsche Datenschutzrecht zu machen:

Immer mehr Lebensbereiche in der sich entfaltenden Wissens- und Informationsgesellschaft werden von den neuen Informations- und Kommunikationstechniken und -möglichkeiten durchdrungen. Mit der zunehmenden Bedeutung der neuen Informations- und Kommunikati-

² Abrufbar unter www.tauss.de (Suche: Arbeit in Bonn, 14. Legislaturperiode).

onstechniken und der zunehmenden Abhängigkeit vieler gesellschaftlicher Bereiche von diesen Techniken wächst auch das Bewußtsein um die damit einhergehenden Gefahren. In einer Gesellschaftsformation, die den Umgang und die Verarbeitung von Daten und Informationen als Markierung des gesellschaftlichen Wandels bereits im Namen trägt, wird die Sicherheit und der Schutz von Informationen und Daten von entscheidender Bedeutung sein.

Notwendig ist eine **dieser Gesellschaftsformation angemessene "neue Politik zum Schutz der Privatsphäre"**, wie dies zu Recht der Datenschutzbeauftragte von Schleswig-Holstein Helmut Bäumler feststellt, denn **"ohne einen besseren Schutz der Privatsphäre wird es keine demokratisch verantwortbare Informationsgesellschaft geben."**

Die Herausforderungen, mit denen das Datenschutzrecht konfrontiert wird, sind vielfältig. Zum einen muß das Datenschutzrecht auf ein **gänzlich entgegengesetztes Technikszenario**, reagieren, als es ursprünglich in den 70er und 80er Jahren konzipiert wurde. Die bestehenden Datenschutzgesetze, die vor dem Hintergrund eines inzwischen weitgehend überholten Technikszenarios entstanden sind, das von zentralen Großrechneranlagen ausging, geraten angesichts der rasanten technischen Entwicklung – Stichworte Dezentralisierung und Vernetzung – immer mehr an ihre Grenzen.

Zum anderen soll mit der EU-Datenschutzrichtlinie ein weiterer – und nicht zu unterschätzender – **Schritt in Richtung Harmonisierung des Rechts** gegangen werden, **der für die demokratische Verankerung der Europäischen Gemeinschaft von fundamentaler Bedeutung** ist: Für die europäische Integration ist die EU-Datenschutzrichtlinie ein wesentliches Element ihrer grundrechtlichen Fundierung. Damit ist jedoch nur ein erster Schritt getan, denn die weltweite Vernetzung macht weltweite Regelungen notwendig, die es zu entwickeln und zu formulieren gilt.

Die Weiterentwicklung des traditionellen Datenschutzes erweist sich jedoch nicht nur hinsichtlich der technischen und europäischen Herausforderungen als notwendig, sondern ist darüber hinaus Grundvoraussetzung zur Wahrung des Grundrechts auf informationelle Selbstbestimmung und damit Voraussetzung zur aktiven Teilhabe der Bürgerinnen und Bürger an der entstehenden Wissens- und Informationsgesellschaft. Die Weiterentwicklung des Datenschutzes ist gleichzeitig erforderlich, um die erheblichen Potentiale zur Modernisierung

von Staat und Verwaltung, zur Verwirklichung von Transparenz und zur Legitimierung staatlichen Handelns zu nutzen.

Schließlich kann die Modernisierung des Datenschutzrechtes auch einen wichtigen Beitrag zur Sicherung des Wirtschaftsstandortes Deutschland beitragen: Denn - und hierfür versuche ich von Anfang an zu werben - die Entwicklung eines angemessenen Datenschutzrechtes kann und darf unter ökonomischer Perspektive nicht allein unter Kostengesichtspunkten diskutiert werden, wie dies noch immer allzu häufig geschieht. Ein wirksamer und angemessener Datenschutz wird sich - vielleicht nicht unbedingt kurzfristig, auf alle Fälle jedoch auf mittelfristige Sicht - als ein wesentlicher Wettbewerbsvorteil erweisen. Wer das bezweifelt, der mag sich nur die neuen Gefährdungspotentiale, die die neuen Informations- und Kommunikationsmöglichkeiten eben auch mit sich bringen, vor Augen führen, dann hat er zugleich eine Antwort darauf, warum die vielen interessanten und lukrativen neuen Angebote eben noch sehr zögerlich angenommen werden.

Dadurch ausgelöste, objektiv nicht unbegründete, Befürchtungen könnten den weiteren Ausbau der Informationsgesellschaft und die Nutzung der durch die neuen Informations- und Kommunikationstechniken entstehenden Vorteile und Chancen ernsthaft behindern. **Ein angemessener und wirksamer Datenschutz wird zu den zu den zentralen Akzeptanzvoraussetzungen der Informationsgesellschaft zählen.** Eine aufgrund der Besorgnis um den Schutz der Privatsphäre ablehnende Haltung gegenüber den neuen Informations- und Kommunikationstechniken hätte mit großer Wahrscheinlichkeit auch erhebliche wirtschaftliche Konsequenzen: Bei fehlendem Vertrauen in die neuen Informations- und Kommunikationstechniken blieben die immensen ökonomischen Potentiale Makulatur – seien es Erwartungen in Milliardenhöhe beim electronic commerce, seien es Erwartungen für den Arbeitsmarkt durch Telearbeit oder seien es die erwarteten Umsätze der Informationswirtschaft.

Die technischen Innovationen im Bereich der Informations- und Kommunikationstechnik und die Vorgaben der EG-Richtlinie macht erhebliche Anpassungen und Änderungen des BDSG notwendig – über die Reichweite der Reform herrscht jedoch alles andere als Einigkeit. **Zwischen "Minimalismus" und "Modernisierung"** – so kann die politische Debatte über die Zukunft des Datenschutzes bis zur Bundestagswahl 1998 wohl zusammengefaßt werden, auf die ich im folgenden kurz eingehen möchte.

2. Politische Debatte in Deutschland: ‚Alter Wein in neuen Schläuchen‘ oder (Weiter-)Entwicklung eines zeitgemäßen Datenschutzrechts als gesellschaftliches Modernisierungsprojekt?

Diese Chancen des wichtigen "Zukunftsfaktors" Datenschutz zur Weiterentwicklung eines zentralen Grundrechts und zur Modernisierung der Gesellschaft - und zwar von Wirtschaft, Staat und Verwaltung - sind jedoch – zumindest in der politischen Diskussion – lange Zeit nicht hinreichend gewürdigt wurden. Auch eine konstruktiv-kritische Analyse der (neuen) Bedingungen moderner Datenverarbeitung und der damit einher gehenden Modernisierungspotentiale fand - mit Ausnahme vielleicht der Entwicklung und Beratung des Teledienstedatenschutzgesetzes (TDDSG) im Rahmen des Informations- und Kommunikationsdienstes-Gesetzes (IuKDG - besser bekannt als Multimedia-Gesetz) - ebenso lange nicht statt.

Zwar hat ein Beratungsgremium der vorherigen Bundesregierung, der Rat für Forschung, Technologie und Innovation, **bereits 1995** festgestellt, daß es notwendig sei, **das traditionell normativ ausgerichtete Datenschutzrecht um Datenschutztechnologie zu ergänzen** und **Bestimmungen, die einen Grundstandard an organisatorischen und technischen Sicherheitsmaßnahmen gewährleisten, zu erarbeiten**. Außerdem sei es erforderlich, das Datenschutzrecht mehr und mehr darauf auszurichten, den **Selbstschutz der Nutzer** und den **Systemdatenschutz** zu unterstützen, **indem es etwa datensparende und datenvermeidende Technik privilegiert**. All dies fand in den Entwürfen der alten Bundesregierung keinen Eingang, vielmehr zeigen diese das Bestreben, das deutsche Datenschutzrecht möglichst wenig zu verändern und möglichst gar nicht mit neuen Regelungen bzw. Regelungen anderer Datenschutzsysteme zu konfrontieren.

Die Frist für die Anpassung des deutschen Datenschutzrechts an die EU-Richtlinie 95/46/EU ("Datenschutzrichtlinie") lief am 24. Oktober 1998 ab. Zwar kursierte bereits im Frühsommer 1997 ein erster Arbeitsentwurf aus dem zuständigen Referat des BMI, über den Anfang 1998 vorgelegten Referentenentwurf (Stand: 08.12.1997) zur Novellierung des Bundesdatenschutzgesetzes konnte jedoch innerhalb der alten Bundesregierung nicht einmal mehr Einigkeit erzielt werden.

Hinzu kam, daß dieser Entwurf **angesichts der mangelnden Bereitschaft, innovative und wirksame Instrumente in das Datenschutzrecht einzubauen**, bereits im Vorfeld auf heftige Kritik gestoßen ist. Die Novellierung des Datenschutzrechts wurde somit kurzerhand von der Tagesordnung gestrichen und auf die Zeit nach die Bundestagswahl im Herbst 1998 vertagt. Die **Entwicklung eines zeitgemäßen und der entstehenden Informationsgesellschaft angemessenen Datenschutzkonzeptes** ist damit offensichtlich im oft genannten "Reformstau" steckengeblieben. Gleiches gilt für den noch immer fehlenden **Arbeitnehmerdatenschutz**. Zwar wurden auch hier gesetzliche und außergesetzliche Regelungen immer wieder angekündigt, jedoch ist es bei den Ankündigungen geblieben.

Einem modernen und wirksamen Datenschutz kommt jedoch – und nicht nur im Hinblick auf den überfällige Umsetzungsfrist, wie ich mit diesen kurzen Ausführungen deutlich machen wollte – in der sich entfaltenden Wissens- und Informationsgesellschaft eine herausragende Bedeutung zu. Will die moderne Gesellschaft beim Übergang zur Wissens- und Informationsgesellschaft am Ziel eines freiheitlich-demokratischen Gemeinwesens festhalten, kommt sie nicht umhin, auch in einer vernetzten und digitalisierten Welt das Grundrecht auf informationelle und kommunikative Selbstbestimmung zu bewahren. Die Entwicklung eines modernen Datenschutzkonzeptes ist damit ein zentrales Reform- und Modernisierungsprojekt der nächsten Jahre und hat von daher auch Eingang in die Koalitionsvereinbarung zwischen der SPD und Bündnis 90/Die Grünen gefunden.

3. Rechtspolitische Vorhaben der neuen Bundesregierung im Bereich des Datenschutzes und des Informationsrechtes

Die Veranstalter dieser Veranstaltung baten mich, auf aktuelle Entwicklungen im Datenschutzrecht und auf die rechtspolitischen Vorhaben der neuen Bundesregierung einzugehen – gerade auch auf die sogenannte 2. Stufe der Modernisierung des Informationsrechtes. Dieser Bitte komme ich gerne nach, nicht zuletzt deshalb, weil ich auch dazu einladen möchte, bei dem wichtigen gesellschaftlichen Reformprojekt „Modernisierung des Informationsrechtes“ mitzuarbeiten.

SPD und Bündnis 90/Die Grünen haben die Bedeutung, die diesem wichtigen Reformprojekt zukommt, erkannt. In ihrer Koalitionsvereinbarung heißt es - ZITAT: „Effektiver Datenschutz

im öffentlichen und im privaten Bereich gehört zu den unverzichtbaren Voraussetzungen für eine demokratische und verantwortbare Informationsgesellschaft.“ - ZITAT-Ende.

Dabei ging es **zunächst, aber nicht nur** um die **Umsetzung der Datenschutzrichtlinie der EG in das deutsche Datenschutzrecht**. Wie soeben angesprochen, hat sich die vorherige Bundesregierung nicht auf einen entsprechenden Gesetzentwurf einigen können und damit ihre europarechtliche Pflicht, die Richtlinie bis Ende Oktober 1998 umzusetzen, verletzt. Die neue Bundesregierung hat daher in ihrer Koalitionsvereinbarung verabredet, die - ZITAT - „notwendige Anpassung des deutschen Datenschutzrechtes an die Richtlinie der Europäischen Union **kurzfristig** umzusetzen“ - ZITAT-Ende.

Aufgrund des enormen Zeitdrucks, der durch versäumte fristgerechten Umsetzung der Richtlinie entstanden ist, haben wir uns für ein zweistufiges Verfahren entschieden. So sollte in einem ersten Schritt mit der Novellierung des BDSG die EG-Datenschutz-Richtlinie schnellstmöglich umgesetzt werden. Jedoch schon mit der parlamentarischen Beratung der Bundesdatenschutzgesetznovelle soll - als fest vereinbarter zweiter Schritt - das gesamte deutsche Datenschutzrecht auf den Prüfstand gestellt werden. Für die ersten Stufe hat das Innenministerium Anfang letzten Jahres einen entsprechenden Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze erarbeitet. Der Gesetzentwurf der Bundesregierung zur Änderung des Bundesdatenschutzgesetzes (und anderer Gesetze) wurde am 06. April 2001 in zweiter und dritter Lesung beraten und – um einige Änderungsanträge der Koalitionsfraktionen ergänzt – verabschiedet.

Zunächst ging es in dieser ersten Stufe jedoch vor allem darum, Irritationen und Mißverständnisse abzubauen, die u.a. dadurch entstanden, daß in den beteiligten Ressorts und den Regierungsfractionen zunächst große Uneinigkeit über die Reichweite der notwendigen Anpassungen im Datenschutzrecht herrschte. So war das federführende BMI zunächst der Auffassung, daß grundsätzlich nur die Richtlinie umgesetzt werden sollte und daß hierfür nur einige wenige Änderungen notwendig seien. Dies sei mit dem Entwurf der vorherigen Bundesregierung erfüllt. Die SPD-Bundestagsfraction und auch das BMJ sowie der BfD waren dagegen der Auffassung, daß zum einen ein erheblich größerer Anpassungsbedarf - beispielsweise bei der Frage der Datenschutzkontrolle - besteht und daß bereits in dem ersten Schritt wichtige technologische Neuerungen (z.B. Chipkarte und Videoüberwachung) als auch datenschutzrechtliche Innovationen - ich erinnere an die Neuerungen des TDDSG -

aufgenommen werden sollten. Daß daneben eine Reihe von Irritationen vor allem daraus resultierten, daß in manchen Abteilungen einiger Ministerien der 27. September 1998 scheinbar spurenlos vorbeigegangen ist, sei hier nur der Vollständigkeit und im Sinne eines „Anekdotchens“ erwähnt.

Hinzu kam - für mich als Forschungs- und Medienpolitiker - die bemerkenswerte Tatsache, daß zu nahezu alle Fragen, die im Zusammenhang mit der Modernisierung des Datenschutzes zu tun hatten - beispielsweise die Frage der Selbstregulation und das Datenschutzaudit - in diesen Abstimmungsgesprächen relativ schnell Konsens zu erreichen war. Anders dagegen, wenn es sich um die Frage des Sicherheitsbereiches handelte. Ähnlich wie in der Krypto-Debatte wurde hier - und dies beinahe schon irrational und in einer für mich nicht nachvollziehbaren Form - „mit Rücksicht auf den Sicherheitsbereich“ nahezu jeglicher Änderungswunsch geblockt. Eine weitere Begründung erfolgte zunächst nicht. Erst nach schwierigen Verhandlungen gelang es, die neuen Regelungen Punkt-für-Punkt dahingehend zu durchforsten, wo denn tatsächlich Probleme für den Sicherheitsbereich auftreten könnten, beispielsweise bei Benachrichtungspflichten.

Während die alte Bundesregierung - und das BMI hielt auch nach der Bundestagswahl zunächst daran fest - dafür plädierte, den Sicherheitsbereich gänzlich aus der Umsetzung der EG-Richtlinie herauszunehmen, da für diesen Bereich keine Umsetzungspflicht bestünde, hat sich die SPD-Fraktion und das BMJ dafür eingesetzt, daß die Umsetzung der EU-Richtlinie - von einigen notwendigen terminologischen Ausnahmen als Übergangsregelung abgesehen - auch für die Sicherheitsbehörden gelten soll. Wie soll man den sonst legitimieren können, daß eine kleine Arztpraxis, in der mehrere Personen personenbezogenen Daten verarbeiten, einen Datenschutzbeauftragten stellen müssen, die Sicherheitsbehörden jedoch - zumindest per Gesetz - nicht? Und dies, obwohl diese alle bereits einen solchen haben, der durch dessen gesetzliche Verankerung natürlich gestärkt würde!

Ganz generell konnten wir - wie sich dies auch in den manchmal etwas schwierigen Abstimmungsgesprächen zwischen den beteiligten Ressorts, also vor zwischen dem federführenden BMI und dem BMJ sowie den Koalitionsfraktionen, immer wieder zeigte - nicht ohne weiteres an den Entwurf der vorherigen Bundesregierung anknüpfen, da dieser die Richtlinie

nur unzureichend umgesetzt und in wichtigen Punkten nicht den politischen Vorstellungen der neuen Bundesregierung entsprochen hätte.

Der Entwurf der vorherigen Bundesregierung bedurfte also einer grundlegenden Überarbeitung. Zu diesen Änderungen und zu der inzwischen abgeschlossenen ersten Stufe will ich – in aller Kürze - 4 Punkte ansprechen. Der SPD-Bundestagsfraktion und der SPD-geführten neuen Bundesregierung ging es **erstens** um den **Abbau** der nach der Richtlinie unzulässigen **Beschränkungen der Kontrollbefugnisse des Bundesbeauftragten für den Datenschutz** und um die Gewährleistung einer **wirklich unabhängigen Datenschutzkontrolle im nicht-öffentlichen Bereich**, also vor allem der Datenverarbeitung in der Wirtschaft. Anders als die vorherige Bundesregierung wollte sich die neue Bundesregierung **zweitens** nicht auf die bloße Umsetzung der EG-Richtlinie beschränken, sondern darüber hinaus **das deutsche Datenschutzrecht auch schon** in der ersten Stufe mit kleinen Schritten **modernisieren**. Modernisierung des BDSG meint Zusammenhang mit der 1. Stufe die Übernahme der neuen datenschutzrechtlichen Instrumente aus dem Multimediarecht, also aus dem Teledienste-Datenschutzgesetz und dem Medienstaatsvertrag der Länder in das Bundesdatenschutzgesetz. Ein Grundgedanke, der den neuen datenschutzrechtlichen Instrumenten zugrunde liegt – und der in der zweiten Stufe noch von weitaus größerer Bedeutung sein wird, ist „**Datenschutz durch Technikgestaltung**“.

Die neuen technischen Möglichkeiten stellen nicht nur eine Gefährdung für die Grundrechte dar, sondern können auch im Dienste der Grundrechte eingesetzt werden. Hierzu müssen Anforderungen zur datenschutzfreundlichen Ausgestaltung von Informations- und Kommunikationstechnik entwickelt werden. Dazu gehören vor allem die Prinzipien Datensparsamkeit und Datenvermeidung. Das bedeutet konkret, daß die Datenverarbeitungstechnik so auszugestalten ist, daß keine oder möglichst wenige personenbezogene Daten anfallen und daß eine anonyme Nutzung oder eine Nutzung unter Pseudonym ermöglicht wird. Vorgesehen ist außerdem das so genannte Datenschutz-Audit. Unternehmen könnten mit einem solchen Zertifikat für ihre datenschutzfreundlichen Dienste werben - Datenschutz als Wettbewerbsfaktor - in meinen Augen eine ebenso interessante wie vielversprechende Vorstellung. Ich freue mich sehr, daß die anfängliche Skepsis der Wirtschaft der zunehmenden Bereitschaft weicht, die Chancen eines solchen freiwilligen Datenschutzaudits zu erkennen.

Wir haben uns **drittens** mit den beteiligten Ressorts und auch dem BfD auf die Aufnahme von Regelungen zum Datenschutz bei mobilen Speichermedien, den **Chipkarten**, und erstmals auch Regelungen von **Videoüberwachungen** verständigt.

Viertens besteht inzwischen Einigkeit darüber, daß die neuen Regelungen des Bundesdatenschutzgesetzes - ob richtlinienbedingt oder nicht - grundsätzlich **auch für die Sicherheitsbehörden** gelten sollen, eine wichtige Entscheidung, die in der vorherigen Bundesregierung bis zuletzt höchst streitig blieb.

All diese angesprochenen Punkte sind mit der 1. BDSG-Novelle in einem **ersten gesetzgeberischen** Schritt im April diesen Jahres verabschiedet worden.

Diesem ersten Schritt folgen soll aber - und vorgesehen ist hierfür das Ende der Legislaturperiode – auch wenn wir dies realistischerweise kaum noch schaffen können -, ein **zweiter gesetzgeberischer Schritt**, ein weiteres Artikel-Gesetz. Mit diesem zweiten Gesetzgebungsvorhaben soll die Datenschutzrichtlinie flächendeckend auch im bereichsspezifischen Datenschutzrecht umgesetzt werden (so es denn bereichsspezifischer Regelungenbedarf – und auch das wird zunächst zu prüfen sein) und zwar auch insoweit, als keine europarechtliche Umsetzungspflicht besteht, weil die Materie nicht dem ersten Pfeiler der Europäischen Union zuzuordnen ist. Durch diese Grundsatzentscheidung wird vermieden, daß es künftig zweierlei Datenschutzrecht gibt: Datenschutzrecht auf dem Niveau der Richtlinie und Datenschutzrecht unterhalb dieses Niveaus. Nur so können Wertungswidersprüche und sachlich nicht gerechtfertigte unterschiedlich hohe Datenschutzstandards im bereichsspezifischen Datenschutzrecht vermieden werden. Die Entwicklung eines modernen Datenschutzkonzeptes ist und bleibt damit ein zentrales Reform- und Modernisierungsprojekt der nächsten Jahre. Schwerpunkte der 2. Stufe der Modernisierung des Datenschutzrechtes werden insbesondere sein:

1. Datenschutz durch Technik: Diese Frage wurde ja bereits im Zusammenhang mit der ersten Stufe angesprochen: Die Möglichkeiten der informationstechnischen Sicherheit müssen als ein zentrales Instrument zur Umsetzung eines „neuen Datenschutzes“ verstanden werden. Um zu einem wirklich effektiven Datenschutz zu kommen, muss das Zusammenwirken zwischen Datenschutz und Datensicherheit intensiviert werden.

2. Vereinfachung und Verschlankeung: Angesichts der Unübersichtlichkeit und Kompliziertheit des Datenschutzrechts sollte im Interesse von datenverarbeitenden Stellen und Nutzern eine erhebliche Vereinfachung und Verschlankeung des Datenschutzrechts im Vordergrund stehen. Nur wenn der einzelne seine Rechte überhaupt kennt, kann er diese auch wahrnehmen! Vereinfachung und Verschlankeung dürfen natürlich nicht zu einer Aufweichung der verfassungsrechtlich garantierten Rechte oder zur Einschränkung oder Abschwächung bewährter Verfahren des Datenschutzes führen. Diese Ziele erweisen sich aber vor allem deshalb als notwendig, um zu widerspruchsfreien, einheitlichen, praktikablen und vor allem auch verständlichen Regelungen zu gelangen. Selbst die Datenschutzexperten klagen über eine kaum noch zu überblickende Normenflut auf dem Gebiet des Datenschutzrechts. Das allgemeine und das bereichsspezifische Datenschutzrecht bedarf daher einer Durchforstung und Überprüfung. So hat in den vergangenen Jahren die Bedeutung des Bundesdatenschutzgesetzes durch immer neue bereichsspezifische Regelungen tendenziell abgenommen. Mit der Umsetzung der zweiten Stufe ergibt sich die Möglichkeit, durch eine Aufwertung des BDSG die Menge der bereichsspezifischen Regelungen deutlich zu reduzieren. Dazu zählt – gerade bei den neuen IuK-Möglichkeiten – beispielsweise auch die Frage, wie sich Abgrenzungsprobleme zwischen Telekommunikationsgesetz, Teledienstedatenschutzgesetz und den Datenschutzregelungen des Mediendienste-Staatsvertrages vermeiden lassen und ob hier gegebenenfalls Anpassungsbedarf besteht. Dazu zählt auch die meiner Meinung nach dringend notwendige Anpassung von Teil 11 des Telekommunikationsgesetzes (TKG) an die neuen datenschutzrechtlichen Instrumente des Teledienstedatenschutzgesetzes (TDDSG).

3. Stärkung des Selbstschutzes: Eine große Bedeutung kommt in einem neuen Datenschutzrecht den Möglichkeiten des Selbstschutzes für den einzelnen Nutzer zu. Dazu bedarf es insbesondere der weiteren Entwicklung von Selbstschutzinstrumenten (z.B. Digitale Signatur, Verschlüsselungssoftware), was zugleich eine Herausforderung an eine zukunftsgerichtete Forschungsförderpolitik ist. Außerdem ist der Aufbau einer Sicherheitsinfrastruktur für die Nutzung dieser Selbstschutzmechanismen unabdingbar, wofür die Politik Rahmenbedingungen formulieren muß. Notwendig ist darüber hinaus die Förderung des Bewußtseins um die Möglichkeiten des Selbstdatenschutzes und des Systemdatenschutzes. Dies kann zum einen durch Maßnahmen zur Aufklärung über die Chancen und Risiken der neuen Informations- und Kommunikationstechniken gesche-

hen, zum anderen aber auch dadurch, daß die öffentliche Verwaltung entsprechende Techniken einsetzt und Ansätze zu „electronic government“ gezielt gefördert werden.

4. Systemdatenschutz: Um die nun festgeschriebenen Gebote der Datensparsamkeit und der Datenvermeidung „mit Leben“ zu füllen, sollten die Systeme der Diensteanbieter nach dem Prinzip des Systemdatenschutzes organisiert werden. Die informationsverarbeitenden Systeme sollten so konstruiert werden, daß sie möglichst wenig personenbezogene Daten verarbeiten müssen (und können), um ihre jeweilige Aufgabe zu erfüllen.
5. Neue Technologien: In den vergangenen Tagen wurde in den Medien die Frage von „heimlichen Gentests“ thematisiert. Natürlich stellt sich die Frage eines modernen Datenschutzrechtes also nicht nur im Zusammenhang mit den neuen Möglichkeiten der Informations- und Kommunikationstechnik. Auch andere neue Technologien bergen erhebliche Gefährdungspotenziale für das Recht auf informationelle Selbstbestimmung. Das gilt beispielsweise für diese heimlichen Genomanalysen und für die Nutzung dieser Informationen, beispielsweise durch Versicherungen. Auch diese Gefährdungspotentiale gilt es auszuloten und – wo nötig – gesetzlich zu regeln.
6. Anonyme und pseudonyme Nutzung: Grundlegende Bedeutung kommt gerade bei der Nutzung der neuen Informations- und Kommunikationsmöglichkeiten der pseudonymen Nutzungsmöglichkeit als Mittel des Selbstdatenschutzes zu, die gefördert werden sollte. Mit einer pseudonymen Nutzungsmöglichkeit werden die personenbezogenen Daten zwar nicht reduziert, jedoch wird damit die Zurückverfolgung der gespeicherten und verarbeiteten Daten zu einer tatsächlichen Person wirksam verhindert – außer im Streitfall.
7. Schutz der Kommunikation am Arbeitsplatz: Nach jahrelangen Ankündigungen müssen im Rahmen dieser 2. Stufe – unter Einbeziehung aller Beteiligten – Regelungen zum Schutz der Kommunikationsprozesse am Arbeitsplatz entwickelt werden. Rechtssicherheit in diesem Bereich ist übrigens sowohl im Interesse der Arbeitgeber als auch der Beschäftigten: Bei der Entwicklung zu computergestützter Arbeit im Betrieb und im Rahmen von Telearbeit wachsen die Daten in Umfang und Qualität stark an, ohne daß sie in angemessener Weise geschützt sind und einer angemessenen Kontrolle unterliegen. Lediglich die Ausweitung des Fernmeldegeheimnisses auch auf innerbetriebliche Kommunikation hat in den letzten Jahren zu einem Zuwachs an Schutz geführt.

8. Regulierte Selbstregulierung: Die in der EU-Datenschutzrichtlinie enthaltene Verpflichtung, im nationalen Datenschutzrecht ergänzende Möglichkeiten der Selbstregulierung vorzusehen, sollte nicht als unvereinbare „Systemwidrigkeit“, sondern als Chance begriffen werden, dieses Instrument für den Schutz des Rechts auf informationelle Selbstbestimmung fruchtbar zu machen. Es kann nicht mehr Regelungen für jedes Detail in jedem Prozess geben – und erst recht nicht durchgesetzt werden. Entsprechende Regelungen sollten sich an den Erfahrungen von Staaten orientieren, die bereits Erfahrungen mit Selbstregulierung im Bereich des Datenschutzes gesammelt haben. So können auch mögliche Schwächen im Hinblick auf Repräsentativität und Umsetzung in den jeweiligen Branchen, die diese „codes of conduct“ haben, erkannt und vermieden werden. Selbstregulierungsmechanismen setzen jedoch gesetzliche Rahmenbedingungen voraus, für den Fall, daß diese versagen – die Betroffenen dürfen in einem solchen Fall nicht schutzlos sein.

9. Verbesserung der Kontrolle: Wirksame und unabhängige Kontrolle ist die Voraussetzung eines erfolgreichen Datenschutzes. Wenn man Datenschutz zunehmend als Querschnittsaufgabe begreifen will, muss dies auch institutionelle Folgen haben. Zu fragen und abzuwägen sein wird in dieser zweiten Stufe auch die Stellung des Bundesbeauftragten für den Datenschutz.

10. Informationsfreiheitsgesetz: Als Kehrseite derselben Medaille müssen wir auch über den Zugang zu Informationen reden. Die Koalition hat in ihrem Koalitionsvertrag angekündigt, ein Informationsfreiheitsgesetz vorzulegen. Im Sommer soll dieser Entwurf vorliegen und beraten werden.

Gestatten Sie mir bitte – auch wenn dies auch nicht in unmittelbarem Zusammenhang mit der Novellierung des deutschen Datenschutzrechtes steht, **diese jedoch konterkarieren** könnte - eine ganz kurze Anmerkung zu einem brisanten Thema machen, das in den vergangenen Wochen die Öffentlichkeit zu Recht erregte: die Cybercrime-Konvention. In diesem Kontext gesehen werden muß diese Debatte vor allem deshalb, weil sie zugleich eine wichtige Begründung für die gegenwärtig in Deutschland erarbeitete Telekommunikationsüberwachungsverordnung (TKÜV) darstellt.

Die zunehmende Bedeutung der neuen Informations- und Kommunikationsmöglichkeiten in allen gesellschaftlichen Bereichen bringt – und das ist unumstritten - auch eine Reihe neuer Gefährdungen und Bedrohungen mit sich. Vor allem die zunehmende Digitalisierung und Vernetzung sowie die neuen Möglichkeiten des „Spurenverwischens“, beispielsweise durch die Nutzung kryptographischer und steganographischer Verfahren, stellt die Sicherheitsbehörden vor grundsätzlich neue Herausforderungen. **Das kann aber nicht zur Folge haben, daß die Eingriffsbefugnisse der Sicherheitsbehörden – und noch dazu geradezu konspirativ unter Ausschluß der Öffentlichkeit – immer weiter und über das Ziel hinaus ausgeweitet werden.**

Natürlich ist es **notwendig**, um auch dies klar zu sagen, die Sicherheitsbehörden in die Lage zu versetzen, **Kriminalität auch in den Datennetzen effektiv zu verfolgen**. Eine Übertragung der für die Überwachung des „klassischen“ Telefonverkehrs entwickelten Konzepte auf globale Datennetze, wie dies derzeit auf europäischer Ebene vorbereitet wird, hätte jedoch fatale Folgen. Damit stünde nicht nur die umfassende Überwachung der Datenkommunikation auf der Tagesordnung, vielmehr werden mit diesen Überwachungsschnittstellen Sollbruchstellen erst aufgebaut, die zu (Computer-) Kriminalität und Wirtschaftsspionage geradezu einladen.

Doch zurück zur Reform des Datenschutzrechtes in Deutschland: Es ist beabsichtigt, die auf der Grundlage des Expertenvotums vorgelegten Entwürfe der Bundesregierung nicht nur im Kreis der Ausschüsse und innerhalb des Begleitausschusses zu diskutieren, sondern die dabei entstehenden Papiere und Stellungnahmen auch im Internet unter den Adressen www.moderner-datenschutz.de bzw. www.modernes-datenrecht.de, möglichst unter einer Startseite des Deutschen Bundestages www.bundestag.de/e-Demokratie, zu veröffentlichen und zur Diskussion zu stellen. Damit wäre in Deutschland zum ersten Mal mit Hilfe des Internet das Entstehen eines neuen Gesetzes, die Beratung mit den Interessenverbänden und im parlamentarischen Raum nahezu umfassend transparent. Dies ist daher als wichtiger Versuch anzusehen, weitgehende Schritte in Richtung einer e-Demokratie zu gehen. Die Modernisierung des Datenschutzrechtes als ein wesentlicher Baustein der sich entfaltenden Informations- und Wissensgesellschaft eignet sich besonders für ein solches

Projekt, da von den Normen dieses Rechtsgebietes nahezu jeder betroffen sein kann. Da zugleich die „Grabenkämpfe„ der 70er Jahre (erinnert sei nur an die Parole: Datenschutz gleich Täterschutz) zu einem großen Teil obsolet geworden sind bzw. sein sollten, bietet sich insbesondere in diesem Bereich ein solch transparentes Verfahren mittels eines neuen Kommunikationsmediums Internet an, gilt es doch wichtige Fundamente einer demokratisch verfaßten und offenen Gesellschaft – das Recht auf informationelle Selbstbestimmung - neu zu definieren. Dieses e-Demokratie-Pilotprojekt bietet eine hervorragende Gelegenheit, die immensen Chancen der neuen Informations- und Kommunikationsmöglichkeiten auch für den politischen Prozess als auch zur Ermöglichung von mehr Partizipation zu erkennen und zu nutzen – im Interesse eines modernen und angemessenen Informationsrechtes der Bürgerinnen und Bürger und im Dialog mit ihnen und der Fachszene. Eine demokratische und verantwortbare Informations- und Wissensgesellschaft darf wie ausgeführt die neuen Möglichkeiten des Dialoges nicht verstreichen lassen.

Damit möchte ich zum Schluß kommen. Die aufgrund der Umsetzung der EU-Datenschutzrichtlinie notwendige Novellierung oder Neuformulierung datenschutzrechtlicher Rahmenbedingungen sollte als Chance erkannt werden, auch auf neue Technikrisiken zu reagieren, wie dies auch die Datenschutzbeauftragten des Bundes und der Länder gefordert haben. Dabei darf jedoch auch bei der Debatte um eine umfangreiche Novellierung die Gefahr einer Verengung auf die Ebene rechtlicher Regulierung nicht unterschätzt werden. Es gilt, und dazu wird das e-Demokratie-Projekt einen erheblichen Beitrag leisten können, zu vermeiden, daß - um es mit den Worten des Datenschutzbeauftragten der Freien Hansestadt Bremen zu formulieren - "juristische Sandkastenspiele" stattfinden, die ohne nennenswerten Einfluß auf die Zukunft der Informationsgesellschaft bleiben.

Ich danke Ihnen für Ihre Aufmerksamkeit!