

Jörg Tauss, MdB

(SPD- Fraktion)

Rede zur 2./3. Lesung des Entwurfes eines Gesetzes der Bundesregierung zur Änderung des Bundesdatenschutzgesetzes (BDSG) und anderer Gesetze am 06. April 2001

Sehr geehrte/r Frau/Herr Präsident/in,
sehr geehrte Damen und Herren,
liebe Kolleginnen und Kollegen,

der Datenschutz und das Grundrecht auf informationelle Selbstbestimmung sieht sich angesichts der technischen Entwicklungen in der Kommunikationstechnologie, aber auch beispielsweise in der Biotechnologie, in der medizinischen Forschung und angesichts eines wachsenden Missbrauchs personenbezogener Daten in den Neuen Medien vor enormen Herausforderungen. Mit der 2. und 3. Lesung zum Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze werden heute die Weichen zur Bewältigung dieser Probleme richtig gestellt.

Durch die Umsetzung der EG-Datenschutz-Richtlinie wird europaweit ein einheitliches Datenschutzniveau geschaffen und werden einheitliche Maßstäbe für die Erhebung und Verarbeitung von Daten in der Europäischen Union festgelegt. Die zentralen Ziele der EG-Datenschutzrichtlinie lauten zusammengefasst: Transparenz der Datenverarbeitung und Akzeptanz der Verbraucher und Nutzer.

Über Umsetzungspflicht der Richtlinie hinaus sind in diesem Gesetzentwurf bereits ein paar Elemente eines neuen und modernen Datenschutzrechtes aufgenommen, die auch für die zweite Stufe einer Gesamtreform von Bedeutung sind. Dazu zählen beispielsweise die Aufnahme der Prinzipien der Datenvermeidung und Datensparsamkeit, die Regelungen für mobilen Speichermedien (Chipkarten) und Regelungen zur Videoüberwachung, für die es – im privaten Bereich – bislang keine Regelungen gab.

Ein wesentliches Modernisierungselement stellt die künftige Möglichkeit eines freiwilligen Datenschutzaudits dar. Eine solche Auditierung trägt künftig mit dazu bei, die

Ergebnisse der Selbstregulierung transparent zu machen. Zugleich könnte sie die Wahrnehmung des Datenschutzes als Qualitäts- und Wettbewerbsfaktor stärken und damit deutlich machen, dass Datenschutz eben nicht nur als Kostenfaktor für Unternehmen anzusehen ist, sondern vor allem einen – wenn auch nicht kurz- so aber doch mittel- und längerfristig – entscheidenden Wettbewerbs- und Standortvorteil darstellen kann. Eine solche Zertifizierung, mit der die Unternehmen werben könnten, hätte nicht nur die unmittelbare Folge, dass aus Perspektive des Datenschutzes unbedenkliche Produkte auf den Markt kommen, sondern könnte ebenfalls das Bewusstsein um die Bedeutung des Datenschutzes in der Informationsgesellschaft erhöhen.

Seitens der Wirtschaft gab es hierzu sowohl unterstützende als auch kritische Anmerkungen. Natürlich gilt es, diese Bedenken ernst zu nehmen. Aufgabe der Politik ist es nun, gesetzliche Regelung zur Durchführung und Kontrolle eines solchen Auditierungsverfahrens zu entwickeln, die diesen Bedenken gerecht werden und mit denen bestimmte Verhaltensregeln und Mindeststandards vorgegeben werden.

Als letzter Redner der Koalition in dieser Debatte möchte ich nicht noch einmal auf die einzelnen Regelungen und die strittigen Punkte dieses Gesetzentwurfes im Detail eingehen, sondern vielmehr den Blick auf die sogenannte zweite Stufe der Modernisierung des Informationsrechtes lenken und Sie hierzu herzlich zur konstruktiven Mitarbeit einladen. Hierzu haben wir ja heute morgen auch ein Gespräch geführt.

Warum eigentlich eine zweite Stufe? Immer mehr Lebensbereiche in der sich entfaltenden Wissens- und Informationsgesellschaft werden von den neuen Informations- und Kommunikationstechniken durchdrungen. Damit wird eine dieser Gesellschaftsformationen angemessene neue Datenschutz-Politik notwendig, denn ohne einen besseren Schutz der Privatsphäre wird es keine demokratisch verantwortbare Informationsgesellschaft geben.

Ein paar Zahlen können dies belegen: 74 Prozent fühlen sich nach einer Umfrage von Opaschowski durch Datenmissbrauch betroffen und 55 Prozent sagen, Datenschutz sollte wieder einer größere Bedeutung haben. Nach einer Umfrage der Mannheimer Forschungsgruppe Wahlen aus dem Jahr 2000 haben 62 Prozent der Internetnutzer wegen des „nicht gewährleisteten Datenschutzes“ noch nicht online bestellt oder gekauft.

Auch die Tätigkeitsberichte dessen Bundesbeauftragten für den Datenschutz – auch diese stehen ja ebenfalls heute zur Beratung an – können als Beleg hierfür dienen. Dem 18. Tätigkeitsbericht Bericht zufolge müssen Bürgerinnen und Bürger in Deutschland immer häufiger mit Eingriffen in ihr Grundrecht auf informationelle Selbstbestimmung rechnen – sei es durch Überwachungsmaßnahmen, die immer häufigere Videoüberwachung im privaten Bereich oder das Ausspähen von Daten bei der Nutzung der neuen IuK-Möglichkeiten – beispielsweise des Internet. Der Bundesdatenschutzbeauftragte äußerte völlig zu Recht am Donnerstag große Sorge, dass zum Beispiel die Anordnungen von Telefonüberwachung seit 1995 um mehr 170 Prozent zugenommen hätten, ohne dass ein Grund dafür ersichtlich sei. In der Kriminalitätsentwicklung scheinen diese Gründe – wie die Zahlen belegen - nicht zu liegen, so dass wir hierüber einmal ruhig und sachlich reden müssen.

So ist und bleibt es ein wichtiges Ziel dieser rot-grünen Bundesregierung, die in den vergangenen Jahren eingeführten Regelungen, die eine Erweiterung der Eingriffsbefugnisse der Behörden zum Ziel hatten, hinsichtlich ihrer Notwendigkeit und Wirksamkeit zu evaluieren – wobei hier gerade seitens der Bundesländer eine größere Bereitschaft notwendig wäre. Dabei ist – wie gegenwärtig bei der Diskussion um den Entwurf für eine Telekommunikationsüberwachungsverordnung – besonders auch dem Umstand Rechnung zu tragen, dass Eingriffsmöglichkeiten in das Telekommunikationsgeheimnis durch "berechtigte" Stellen auch immer missbräuchliche Eingriffe durch unberechtigte Dritte zur Folge haben können.

Die Stuttgarter Nachrichten schreiben heute zum Thema „Datenschutz“: „In unserer vernetzten, indiskreten Gesellschaft bleibt wenig geheim, praktisch gar nichts. Nicht die Kreditbelastung, nicht das Konsumverhalten, auch nicht Adresse und Telefonnummer. Von Privatheit keine Spur, nicht mal der Gang durchs Museum ist noch unsere Sache: Wenn wir Pech haben, tauchen wir kurz darauf im Internet auf. Es gibt also viele ungute Gründe, wachsam zu sein. Wer finstere Mächte am Werk glaubt, wenn mitgehört und ausgeforscht wird, täuscht sich. Die Absichten sind lauter, stets geht es um die Aufklärung vermeintlicher Straftaten. Auch der Rechtsstaat ist nicht fehlerfrei. Fazit: Wer nichts verbirgt, hat viel zu befürchten.“ Soweit die Stuttgarter Nachrichten, denen ich an dieser Stelle zustimme.

Der Schutz der personenbezogenen Daten und die Transparenz der Datenverarbeitung werden – so können diese Überlegungen zusammengefasst werden – neben dem

Schutz von Persönlichkeitsrechten sowohl zu zentralen Akzeptanzvoraussetzungen als auch zu entscheidenden Wettbewerbsfaktoren.

Fazit: Will die Gesellschaft beim Übergang zur Wissens- und Informationsgesellschaft am Ziel eines freiheitlich-demokratischen Gemeinwesens festhalten und will sie auch die wirtschaftlichen und arbeitsmarktpolitischen Potentiale nicht gefährden, 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 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: 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 Verschlankung: Angesichts der Unübersichtlichkeit und Kompliziertheit des Datenschutzrechtes sollte im Interesse von datenverarbeitenden Stellen und Nutzern eine erhebliche Vereinfachung und Verschlankung des Datenschutzrechtes im Vordergrund stehen. Nur wenn der einzelne seine Rechte überhaupt kennt, kann er diese auch wahrnehmen! Vereinfachung und Verschlankung 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 Datenschutzrechtes. 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, Teledienststedatenschutzgesetz 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 Teledienststedatenschutzgesetzes (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 Sicherungsinfrastruktur 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 geschehen, 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 Selbst Datenschutzes 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.

Sehr geehrte Damen und Herren, liebe Kolleginnen und Kollegen,

auf Initiative der Koalitionsfraktionen hat der Unterausschuss Neue Medien beschlossen, diese 2. Stufe der Modernisierung des Informationsrechtes zugleich als Pilotprojekt einer elektronischen Demokratie zu begleiten. Hierzu werden in Abstimmung mit allen Fraktionen die letzten Detailfragen geklärt. Ich will als Vorsitzender des Unterausschusses und zugleich im Namen der Vorsitzenden des Innenausschusses, Ute Vogt, alle Fraktionen auch zur Mitarbeit an diesem e-Demokratie-Pilotprojekt herzlich einladen. 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.

Wenn wir dies jetzt auch mit diesem Zukunftsthema verbinden, haben wir für die bürgernahe Informationsgesellschaft einen weiteren Beitrag geleistet. Heute aber verabschieden wir zunächst die erste Stufe - dies ist ein wichtiger Schritt und wie ausgeführt ein Schritt zu weiteren interessanten Projekten.

Herzlichen Dank für die Aufmerksamkeit und – an die Opposition gerichtet- herzlichen Dank für die konstruktive Zusammenarbeit in der Schlussphase dieses Gesetzgebungsverfahrens.