21. Tätigkeitsbericht 2005-2006
Schaar: Staat muss Datenschutz stärken

Bonn, 24. April 2007

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Peter Schaar, hat heute (24.04.) dem Präsidenten des Deutschen Bundestages, Dr. Norbert Lammert, den 21. Tätigkeitsbericht für den Zeitraum 2005/2006 überreicht.

Hierzu weist er auf Folgendes hin:
„Für den Datenschutz hat die Arbeit deutlich zugenommen. Der vorliegende Bericht dokumentiert eine Vielzahl von Aktivitäten und Problemstellungen, von denen nur ein kleiner Teil von der breiten Öffentlichkeit wahrgenommen wird. Dass für die Bürgerinnen und Bürger der Schutz ihrer Daten von steigender Bedeutung ist, zeigt sich z.B. an den Eingaben, deren Zahl sich gegenüber der letzten Berichtsperiode um mehr als 28 % auf 5.516 erhöht hat. In den letzten beiden Jahren haben meine Mitarbeiterinnen und Mitarbeiter zahlreiche Informations- und Kontrollbesuche durchgeführt (Anl. 2, S. 160), bei denen häufig datenschutzrechtliche Mängel festgestellt wurden, denen in erfreulich vielen Fällen abgeholfen werden konnte. Allerdings kam ich nicht umhin, in sechs besonders gravierenden Fällen formelle Beanstandungen nach § 25 Bundesdatenschutzgesetz (BDSG) auszusprechen (Anl. 3, S. 162). Außerdem nahm die Beratung der Bundesregierung und des Deutschen Bundestages, insbesondere im Rahmen der Begleitung zahlreicher Gesetzgebungsvorhaben und IT-Projekte mit Datenschutzbezug, einen unverändert großen Raum ein.
Mit dem am 1. Januar 2006 in Kraft getretenen Informationsfreiheitsgesetz (IFG) wurden mir neue Aufgaben zugewiesen (Nr. 18.7), die meine Dienststelle erheblich in Anspruch nehmen, ohne dass die Zuweisung der hierfür erforderlichen neuen Stellen erfolgt ist. Über die Erfahrungen mit dem IFG werde ich Anfang des kommenden Jahres einen gesonderten Bericht vorlegen.

Zur **Lage des Datenschutzes** möchte ich folgendes bemerken:

Eine der wichtigsten Aufgaben des demokratischen Rechtsstaates ist es, die Freiheitsrechte seiner Bürger zu schützen. In der modernen Informationsgesellschaft ist das Recht auf informationelle Selbstbestimmung ein elementares Bürgerrecht, dessen Bedeutung vor allem angesichts des technologischen Fortschritts ständig zunimmt. Immer mehr personenbezogene Daten werden in immer mehr Lebensbereichen erfasst. Ob wir mit Kunden- und Kreditkarten einkaufen, im Internet surfen, telefonieren oder uns einfach nur in videoüberwachten Bereichen bewegen, die Datenflut ist so groß wie noch nie. Das Datenschutzrecht hat jedoch nicht mit dieser Entwicklung Schritt gehalten. Leider hat es die Bundesregierung in den letzten Jahren versäumt, hier initiativ zu werden. So stehen gesetzliche Regelungen zu Genomanalysen und zum Arbeitnehmerdatenschutz seit langem aus, obwohl der Deutsche Bundestag die Bundesregierung wiederholt und einstimmig aufgefordert hat, hierzu Entwürfe vorzulegen. Auch die dringend erforderliche Modernisierung des Datenschutzrechts und das Ausführungsgesetz zum Datenschutzaudit müssen endlich in Angriff genommen werden. Beides sollte schon im Anschluss an die Anpassung des Bundesdatenschutzgesetzes an die EG-Datenschutzrichtlinie im Jahr 2001 geregelt werden, ist aber dann auf der Strecke geblieben.
Umgekehrt wurde der Datenschutz auch im Berichtszeitraum zu Gunsten der Inneren Sicherheit immer mehr eingeschränkt. Das Gleichgewicht zwischen dem Schutz der Bürgerinnen und Bürger vor Terror und Kriminalität und dem Schutz ihrer Freiheit droht aus dem Lot zu geraten. Der Staat muss das Grundrecht auf informationelle Selbstbestimmung wieder stärker unter seinen Schutz stellen.

Im Zeitraum des aktuellen Tätigkeitsberichts waren folgende Punkte von Bedeutung:

Gesetze zur Terrorismusbekämpfung – Tiefe Einschnitte in den Datenschutz (Nr. 5.1, 5.1.1, 5.1.2)

In der abgelaufenen Berichtsperiode wurde der umfassende Ausbau der Sicherheitsinfrastruktur von Bund und Ländern fortgesetzt. Von zentraler Bedeutung sind hier das Terrorismusbekämpfungsergänzungsgesetz sowie die Anti-Terror-Datei. Bei der Zusammenarbeit zwischen Polizei und Nachrichtendiensten ist das verfassungsrechtliche Trennungsgebot zu beachten. Ich habe Zweifel, dass dieser Vorgabe bei der Errichtung der Anti-Terror-Datei hinreichend Rechnung getragen wurde. Die Datei beschränkt sich nicht auf eine reine Indexfunktion, sondern führt umfangreiche polizeiliche und nachrichtendienstliche Erkenntnisse zusammen. Damit erhalten die Polizeibehörden Kenntnis von Daten, die sie ggf. nicht hätten selbst erheben dürfen. Bei der Aufnahme des Wirkbetriebs am 31. März 2007 wurden bereits Daten von mehr als 13.000 Betroffenen in der Anti-Terror-Datei erfasst, also nicht nur die in der Diskussion angeführten rund "hundert Gefährder".
Mit dem Terrorismusbekämpfungsergänzungsgesetz wurden die 2002 zur Terrorismusbekämpfung geschaffenen Befugnisse erneut ausgedehnt. Die Nachrichtendienste des Bundes können nunmehr unter wesentlich erleichterten Voraussetzungen umfängliche Auskünfte bei Kreditinstituten, Finanzdienstleistern, Luftverkehrsgesellschaften sowie Post- und Telekommunikationsunternehmen einholen. Auf der anderen Seite fehlt eine wissenschaftlich fundierte Evaluierung der Eingriffsbefugnisse durch eine unabhängige Stelle.
Ein Baustein der neuen Sicherheitsarchitektur ist das im Dezember 2004 in Berlin neu errichtete Terrorismusabwehrzentrum (GTAZ). Bei einer im Oktober 2005 durchgeführten Kontrolle des GTAZ habe ich schwerwiegende datenschutzrechtliche Verstöße festgestellt. Bundeskriminalamt und Bundespolizei haben eine Vielzahl personenbezogener Daten an das Bundesamt für Verfassungsschutz unzulässig übermittelt. Ich habe diese Verstöße gemäß § 25 Bundesdatenschutzgesetz beanstandet (Nr. 5.1.4).

Neue Befugnisse für die Sicherheitsbehörden – Verfassungsrechtliche Bedenken nicht ausgeräumt

Online-Durchsuchung (Nr. 5.1.3)
Online-Durchsuchungen von Computern können unverhältnismäßig tief in das Grundrecht nach Art. 13 GG und in das Recht auf informationelle Selbstbestimmung der Computer-Nutzer eingreifen. Durch die Maßnahme können auch höchst private Inhalte erfasst werden. Von diesen Maßnahmen wird zudem der Betroffene in der Regel nicht unterrichtet, was seine Rechtsschutzmöglichkeiten stark einschränkt. Angesichts der verfassungsrechtlichen Bedenken und aus meiner Sicht unlösbaren praktischen Fragen sollte das Projekt Online-Durchsuchungen aufgegeben werden.

Biometrische Daten in Reisepässen (Nr. 4.5.3)
Seit dem 1. November 2005 wird das digitalisierte Passfoto im Biometriechip des ePasses gespeichert. Inzwischen sind bereits knapp drei Millionen ePässe mit digitalisiertem Lichtbild im Chip ausgegeben worden. Zusätzlich sollen nun auch die digitalisierten

Abdrücke der Zeigefinger gespeichert werden. Besonders besorgt sehe ich den vorgesehenen Online-Zugriff der Polizei auf die digitalisierten Passbilder. Damit würden letztlich die über 5.000 kommunalen Register zusammengeschaltet, und es entstünde faktisch eine - virtuelle - Referenzdatei biometrischer Daten, die der Deutsche Bundestag ausdrücklich verhindern wollte. Für verfassungsrechtlich bedenklich hielte ich es auch, die Fingerabdrücke aller Pass- und Personalausweisinhaber in Dateien zu erfassen, denn dies käme der unterschiedslosen erkennungsdienstlichen Erfassung der gesamten Bevölkerung auf Vorrat gleich.

Mautdaten (Nr. 12.1)
Dem Konzept der Mauterhebung mit seiner umfangreichen Datenerfassung hat der Gesetzgeber seinerzeit unter der Voraussetzung einer strikten Zweckbindung dieser Daten nur für Mautzwecke zugestimmt. Nach mehreren Kapitalverbrechen, in die Fahrer schwerer Lastwagen verwickelt waren, wurde die gesetzliche Zweckbindung der Mautdaten in Frage gestellt. Ich habe hier eine sorgfältige Verhältnismäßigkeitsprüfung angemahnt. Nur wenn der Nachweis geführt werden kann, dass die Mautdaten überhaupt für Strafverfolgungszwecke geeignet sind, hielte ich eine Verwendung für bestimmte sehr schwere Delikte für vertretbar. Zudem wäre sicherzustellen, dass entsprechende Zugriffe nur nach einer richterlichen Anordnung erfolgen. Ein erster Entwurf der Bundesregierung sieht vor, die Verarbeitung und Nutzung der Mautdaten auch zur Verfolgung von "Straftaten von erheblicher Bedeutung" oder "zur Gefahrenabwehr" zuzulassen. Damit würde sich die Befürchtung bestätigen, dass die Lockerung der Zweckbindung letztlich zu einer unverhältnismäßigen Datennutzung führt.

Vorratsdatenspeicherung – Dammbruch zu Lasten des Datenschutzes (Nr. 10.1)

Die geplante generelle, verdachtlose Speicherung sämtlicher Verkehrsdaten der Telekommunikation und des Internet wird zu beispiellosen Sammlungen sensibler personenbezogener Daten ganz überwiegend unverdächtiger Personen führen. Schon jetzt sind Rufe nach einer Nutzung dieser grundrechtlich geschützten Fernmeldedaten zur Ermittlung von Teilnehmern sog. Musiktauschbörsen im Internet laut geworden. Die Preisgabe für zivilrechtliche Zwecke würde eine Entwicklung einleiten, an deren Ende diese Daten für kaum noch zu übersehende Zwecke und Empfänger zur Verfügung stehen könnten.

Immer mehr Videoüberwachung (Nr. 4.2)

Bei der Kontrolle der Videoüberwachung beim Deutschen Bundestag habe ich festgestellt, dass die gesetzlichen Anforderungen grundsätzlich erfüllt waren. Zudem wurden auf meinen Hinweis hin bereits während der Kontrolle kritische Kameraeinstellungen entsprechend abgeändert. Weiterhin wird der Deutsche Bundestag zukünftig Piktogramme nach der DIN-Norm zur Kennzeichnung der Kameras verwenden (Nr. 4.2.3).
Auch über die Videoüberwachung von Bahnhöfen durch die Bundespolizei habe ich mich informiert. Die Bundespolizei hat Zugriff auf die Aufzeichnungstechnik der Deutsche Bahn AG. Dabei standen bis Dezember 2006 3.092 Videokameras zur Verfügung, von denen bei 2.091 Kameras die Bildsignale bis zu 48 Stunden aufgezeichnet werden. Bilddaten der restlichen Kameras werden nicht aufgezeichnet; sie dienen der Überwachung in Realzeit (Nr. 4.2.2).
Ein in meinem Auftrag entwickeltes Schutzprofil zur Videoüberwachung stellt einen Prüfrahmen für die Datenschutzanforderungen an solche Systeme bereit. Ich erwarte, dass in Zukunft verstärkt Systeme eingesetzt werden, die den darin definierten Anforderungen entsprechen (Nr. 4.2.1).
Im Hinblick auf die rasante Entwicklung der Videotechnik kommt in Zukunft auch der Kombination von Videotechnik mit biometrischen Erkennungssystemen zentrale Bedeutung zu, wie sie z.B. bei dem vom Bundeskriminalamt im Mainzer Hauptbahnhof durchgeführten Projekt "Foto-Fahndung" getestet wurde (Nr. 5.2.6).

Geltendes Datenschutzrecht - Weit hinter der technischen Entwicklung zurück (Nr. 2.1, 2.4, 2.7, 9.1)

Die seit vielen Jahren angekündigte und vom Deutschen Bundestag gerade wieder in seiner Entschließung zu meinem letzten Tätigkeitsbericht angemahnte grundlegende Reform des Datenschutzrechts ist auch im Berichtszeitraum nicht in Angriff genommen worden, obwohl hier ein erhebliches Potenzial für Verwaltungsmodernisierung, Entbürokratisierung und Stärkung von Bürger- und Verbraucherrechten festzustellen ist. Ohne entsprechende Reformschritte wird die Lücke zwischen technologischem Fortschritt und dem Einsatz elektronischer Datenverarbeitung in immer neuen Lebensbereichen auf der einen Seite und den geltenden datenschutzrechtlichen Bestimmungen sowie dem System der Kontrollmöglichkeiten auf der anderen Seite immer größer. Deswegen ist es dringend geboten, endlich die gesetzlichen Voraussetzungen für ein Datenschutzaudit zu schaffen. Zum Schutz der Bürgerinnen und Bürger vor negativen Konsequenzen des Einsatzes moderner Technologien sind auch Regelungen zum Arbeitnehmerdatenschutz und zur umfassenden Profilbildung in der Wirtschaft – etwa beim Scoring oder zentralen Auskunftssystemen – überfällig. Wir erleben gerade in diesen Bereichen heute die Entwicklung, die das Bundesverfassungsgericht mit seinem Volkszählungsurteil verhindern wollte, nämlich den gläsernen Bürger, der in seinem Verhalten für Dritte berechenbar und manipulierbar wird und damit in seiner Handlungsfreiheit und in der freien Entwicklung seiner Persönlichkeit eingeschränkt ist.

Genetische Daten – Heimliche Gentests verhindern (Nr. 13.2)

Genanalysen ermöglichen einen immer tieferen Einblick in unsere Erbanlagen. So erlauben sie Vorhersagen über die Eintrittswahrscheinlichkeit einer Krankheit bereits lange vor dem tatsächlichen Ausbruch. Daher ist es dringend erforderlich, diese Materie umfassend zu regeln. Heimliche Gentests müssen ebenso verhindert werden wie die missbräuchliche Nutzung genetischer Erkenntnisse im Arbeitsleben und im Versichertenverhältnis. Auch das Bundesverfassungsgericht hat am 13. Februar 2007 (1 BvR 421/05) festgestellt, dass die Verwertung von heimlichen genetischen Abstammungsuntersuchungen als Beweismittel abzulehnen ist. Obwohl der Deutsche Bundestag die Vorlage eines Gendiagnostikgesetzes schon seit längerem angemahnt hat, liegt bis heute kein Gesetzentwurf vor.

Kontenabruf durch die Finanzämter und andere Behörden – Keine Standardabfrage (Nr. 8.2)

Nach wie vor ist die seit dem 1. April 2005 durchgeführte staatliche Kontenabfrage Gegenstand von Kontroversen. Dieses Beispiel macht deutlich, wie staatliche Stellen zunehmend Zugriff auf Datenbestände der privaten Wirtschaft nehmen. Über die Ende 2004 eingelegten Verfassungsbeschwerden ist bisher noch nicht entschieden worden. In dem Entwurf des Unternehmenssteuerreformgesetzes sind einige meiner Forderungen aufgenommen worden, etwa Informationsverpflichtungen der Behörden, die Dokumentation der Abrufe und die Benennung der Leistungen, die andere Behörden außerhalb der Finanzverwaltung zur Kontenabfrage berechtigen. Kritisch sehe ich, dass die Kapazität der täglichen Kontenabrufe von jetzt 100 auf demnächst 5.000 gesteigert werden soll. Die Kontenabfrage darf nicht zu einer Standardmaßnahme werden.

Steuer-Identifikationsnummer – Datenpool für neue Begehrlichkeiten? (Nr. 8.1)

Die Einführung der "Identifikationsnummer für steuerliche Zwecke" in der Abgabenordnung und damit die Einrichtung eines zentralen Registers aller in Deutschland steuerpflichtigen Personen wurde mit dem Steueränderungsgesetz 2003 beschlossen. Beim Bundeszentralamt für Steuern (BZSt) wird 2008 in Zusammenarbeit mit den kommunalen Meldebehörden erstmals ein zentrales Register der gesamten Bevölkerung geschaffen – unter Einschluss von Neugeborene, da sie potenziell steuerpflichtig sind. Dies sehe ich sehr kritisch. Die Erfahrung zeigt, dass Datensammlungen, die für einen bestimmten Zweck angelegt wurden, schnell weitere Begehrlichkeiten wecken.

Einsatz von RFID-Chips – Nicht auf Kosten der Privatsphäre (Nr. 4.3)

Angesichts der besonderen Risiken, die mit dem Einsatz der per Funk auslesbaren RFID-Chips verbunden sind, muss sichergestellt werden, dass das Verhalten von Personen nicht heimlich überwacht oder registriert wird. Hier ist es dringend geboten, dass sich Handel und Hersteller umfassend, nachprüfbar und verbindlich dazu verpflichten, den Daten- und Verbraucherschutz bei RFID sicherzustellen. Hierzu gehören umfassende Informationen für die Betroffenen und die Möglichkeit, die im Handel verwendeten RFID nach der Zahlung an der Kasse zu deaktivieren.

Speicherung von EU-Bürgern im AZR – Neues Vertragsverletzungsverfahren? (Nr. 7.1.1)

Für problematisch halte ich die generelle Speicherung personenbezogener Daten ausländischer Unionsbürger im Ausländerzentralregister (AZR), die nach einem Gesetzentwurf zur Umsetzung von EU-Recht zukünftig auch Lichtbilder umfassen soll.
Bislang ist nicht substantiiert begründet worden, warum es einer solchen unterschiedslosen Datenspeicherung bedarf. Die von mir vorgeschlagene Begrenzung auf bestimmte Speicheranlässe (z.B. Ausweisungen, Abschiebungen, Einreisebedenken) wurde vom BMI nicht übernommen. In der generellen Speicherung von Daten ausländischer Unionsbürger sehe ich zudem einen Verstoß gegen das Europarecht. Ich gehe davon aus, dass die Europäische Kommission Deutschland in dieser Sache vor dem EuGH verklagen wird.

Offene datenschutzrechtliche Fragen im internationalen Bereich

Fluggastdatenübermittlung (Nr. 3.3.2, 3.3.3)

Das Ende Juli 2007 auslaufende Interimsabkommen der Europäischen Union mit den USA zur Übermittlung von Fluggastdaten muss durch eine langfristige Vereinbarung ersetzt werden, welche die Rechte und Freiheiten der Passagiere garantiert und den Umfang der Datenübermittlung auf ein angemessenes Maß reduziert. Der Datentransfer muss endlich auf ein aktives Übermittlungsverfahren umgestellt werden, denn es ist nicht hinzunehmen, dass sich die US-Behörden weiterhin mittels Online-Zugriffs der Daten der Fluggesellschaften bedienen können.

SWIFT (Nr. 9.4)

Seit 2001 haben US-Behörden Zugang zu den Zahlungsverkehrsdaten von SWIFT (Society for Worldwide Interbank Financial Telecommunication), um sie im Rahmen der Bekämpfung des Terrorismus auszuwerten. Alle grenzüberschreitenden Überweisungen und nationalen Eilzahlungen werden über SWIFT abgewickelt, das die Überweisungsdaten in Rechenzentren in Europa und in den USA speichert. Hierzu gehören auch Überweisungsdaten innerhalb Europas. Die deutschen und europäischen Datenschutzgremien haben die Praxis von SWIFT für unzulässig erklärt und sowohl SWIFT als auch die Banken aufgefordert, die Datenschutzmängel abzustellen. Ferner müssen Banken ihre Kunden über die Zugriffsmöglichkeiten informieren. In Deutschland wird nach den mir vorliegenden Kenntnissen zumindest die Kundeninformation sichergestellt. Weitere Maßnahmen zur Gewährleistung des Datenschutzes werden vorbereitet.

Nummer: 14/2007

Erscheinungsdatum: 24.04.2007