Humanistische Union

Datenschutz – ein bedrohtes Grundrecht

Mitteilungen Nr. 189, S.1-3

Der Datenschutz, also das Grundrecht auf informationelle Selbstbestimmung, bindet - wie jedes Grundrecht - Gesetzgeber, Verwaltung und Rechtsprechung. Zum Grundrechtsschutz gehören die unabhängigen Datenschutzbeauftragten als Beratungs- und Kontrollorgane, die über ihre Tätigkeit den Parlamenten regelmäßig Bericht erstatten, um frühzeitig auf Gefahren und Fehlentwicklungen hinzuweisen. Als Bundesbeauftragter für den Datenschutz habe ich nach § 26 Abs. 1 Satz 2 des Bundesdatenschutzgesetzes den Deutschen Bundestag und die Öffentlichkeit über wesentliche Entwicklungen des Datenschutzes zu unterrichten. Diesen Auftrag habe ich in der Vergangenheit wahrgenommen und werde mich nicht davon abbringen lassen, dies auch in Zukunft zu tun.
Mein Tätigkeitsbericht für die Jahre 2003 und 2004, den ich vor Kurzem dem Präsidenten des Deutschen Bundestages übergeben und im Anschluss der Öffentlichkeit vorgestellt habe, zeigt, dass das Grundrecht auf informationelle Selbstbestimmung durch den rasanten technologischen Fortschritt und andere Entwicklungen - insbesondere bei der öffentlichen Sicherheit - bedroht ist.
So wurden immer wieder - nicht erst nach den terroristischen Anschlägen vom 11. September 2001 - zusätzliche Befugnisse für die Sicherheitsbehörden eingeführt. Die Liste der realisierten und geforderten Grundrechtseinschränkungen ist lang, und ein Ende ist leider noch nicht abzusehen: Die - im letzten Jahr vom Bundesverfassungsgericht beanstandeten - Regelungen zum "Großen Lauschangriff", also zur akustischen Wohnraumüberwachung, sind zwar öffentlich besonders kritisch diskutiert worden; im Hinblick auf ihre praktische Bedeutung, also ihren Einsatz durch die Ermittlungsbehörden, bleiben sie aber weit hinter anderen gesetzlichen Befugnissen zurück, insbesondere hinter der Überwachung der Telekommunikation. So ist nicht nur der Straftatenkatalog für die Telekommunikationsüberwachung immer wieder erweitert worden, auch die Anwendung dieser Befugnisse hat in den letzten Jahren drastisch zugenommen.
Weil es sich beim Datenschutz um ein Grundrecht handelt, müssen diejenigen, die ihn einschränken wollen, den Beweis antreten, dass der geforderte Eingriff erforderlich ist und dem Grundsatz der Verhältnismäßigkeit entspricht. Die bloße Behauptung, diese oder jene Maßnahme diene der Bekämpfung des Terrorismus oder der allgemeinen Kriminalität, reicht bei weitem nicht aus. Und auch die Befugnisse, die staatlichen Stellen bereits eingeräumt wurden, müssen regelmäßig überprüft und gegebenenfalls zurückgenommen werden.
Dies gilt auch für die nach den Anschlägen 2001 als "Sicherheitspakete" befristet eingeführten Befugnisse. Sie müssen auf ihre Effizienz und Erforderlichkeit hin überprüft werden, wie es bereits im damaligen Gesetzgebungsverfahren vorgesehen war und seinerzeit als wichtige Voraussetzung für ihre Verabschiedung gesehen wurde. Ich halte es für dringend erforderlich, die bei der "Evaluation" verwendeten Kriterien und die Ergebnisse der Öffentlichkeit zugänglich zu machen, damit die politische Debatte auf Basis einer gesicherten Faktenlage geführt werden kann. Dies ist deshalb besonders wichtig, weil über die Fortsetzung von Grundrechtseingriffen zu entscheiden ist, bei denen der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz gewahrt bleiben muss. Eingriffsbefugnisse, die nicht gebraucht werden oder die sich nicht bewährt haben, sind zurückzunehmen. Einen Automatismus darf es bei der anstehenden Verlängerung nicht geben. Eine generelle Entfristung der Befugnisse, wie sie vom Bundesinnenminister gefordert wurde, lehne ich ab.
Für nicht angemessen hielte ich es, wenn im Prinzip jedes Ergebnis als Argument für die Beibehaltung oder gar Ausweitung der Grundrechtseingriffe verwendet würde. So überzeugt es nicht, wenn eine geringe oder völlig fehlende Nutzung der neuen Befugnisse als Beweis für einen "verantwortungsvollen Umgang" damit gewertet und daraus zusätzliche Forderungen abgeleitet würden, zugleich aber - wie bei der Telekommunikationsüberwachung - eine starke Nutzung als Beleg dafür angeführt wird, dass neue Eingriffsbefugnisse erforderlich seien.

"Für nicht angemessen hielte ich es, wenn im Prinzip jedes Ergebnis als Argument für die Beibehaltung oder gar Ausweitung der Grundrechtseingriffe verwendet würde."
Das Bundesverfassungsgericht hat die Bedeutung des Grundrechts auf informationelle Selbstbestimmung in mehreren Entscheidungen eindrucksvoll unterstrichen. So betont das Verfassungsgericht in seiner Entscheidung zum Großen Lauschangriff vom 3. März 2004, dass ein unantastbarer Kernbereich privater Lebensgestaltung vor jeglicher Überwachung geschützt bleiben muss. Diese Entscheidung hat Konsequenzen weit über die akustische Wohnraumüberwachung hinaus, insbesondere für die Telefonüberwachung. Denn das Gericht hat am gleichen Tag in einer weiteren Entscheidung festgestellt, dass die aufgestellten Grundsätze auch bei der Befugnis zur präventiven Telekommunikationsüberwachung durch das Zollkriminalamt zu beachten sind. Ich erwarte deshalb von der Bundesregierung, dass sie noch in dieser Legislaturperiode einen Gesetzentwurf zur Begrenzung und Neuregelung der Telekommunikationsüberwachung vorlegt.
Kritisch sehe ich die auf europäischer Ebene diskutierte Initiative zur Einführung einer Verpflichtung zur Speicherung von Telekommunikationsdaten. Diese Daten (Wer hat wann mit wem telefoniert? Wo hat er/sie sich dabei aufgehalten? Unter welcher IP-Adresse wurde im Internet gesurft und welche Seiten wurden dabei angesehen?) sollen in Zukunft generell zwölf bis 36 Monate aufbewahrt werden. Dies wäre datenschutzrechtlich bedenklich, wie der Deutsche Bundestag mehrfach mit großer Mehrheit festgestellt hat, zuletzt in seinem einstimmigen Beschluss vom 17. Februar 2005. Als Alternative zur generellen und massenweisen Datenspeicherung auf Vorrat könnte die Strafverfolgungspraxis in den USA dienen, bei der auf Ersuchen der Strafverfolgungsbehörden zwar in begründeten Einzelfällen die elektronischen Daten von den Diensteanbietern weiter zu speichern sind, aber nur herausgegeben werden müssen, wenn innerhalb von 90 Tagen ein entsprechender richterlicher Beschluss vorgelegt wird. Ein solcher Ansatz wäre wesentlich datenschutzfreundlicher und würde den geltend gemachten Belangen der inneren Sicherheit in gleicher Weise gerecht.
Ein weiterer wichtiger Punkt sind biometrische Systeme und Verfahren, die in mehreren Bereichen kurz vor der Anwendung stehen, um die Identifikation von Personen zu erleichtern. Sie ermöglichen es jedoch auch, den Einzelnen heimlich zu überwachen. Noch in diesem Jahr sollen die ersten Pässe mit biometrischen Merkmalen ausgegeben werden. Die Biometrie hält aber häufig nicht, was man sich von ihr verspricht. Vor allem ist sie kein Allheilmittel zur Gefahrenabwehr oder Kriminalitätsbekämpfung. Wissenschaftliche Untersuchungen und Anwendungstests zeigen vielmehr, dass sie oft nicht so zuverlässig funktioniert, wie es für ihren flächendeckenden Einsatz erforderlich wäre.
Im Hinblick auf die geplante Einführung der Biometrie-Pässe hat das Bundesinnenministerium kürzlich erklärt, Tests hätten die Zuverlässigkeit der Verfahren belegt. Was spricht dann dagegen, diese Untersuchungen zu veröffentlichen? Schließlich hat die Öffentlichkeit ein Recht darauf, zu erfahren, welche Konsequenzen die Ausstattung der Personalpapiere der EU-Bürgerinnen und -Bürger mit digitalem Gesichtsbild und Fingerabdruck auf einem kontaktlos auslesbaren Funkchip haben wird. Ich halte eine offene und breit geführte Diskussion über biometrische Verfahren für unverzichtbar. Für die Einführung biometrischer Merkmale in Reisepässen erscheint mir deswegen ein Moratorium angebracht, zumal die entsprechenden Vorgaben der EU-Verordnung erst Mitte 2006 und nicht etwa in diesem Jahr umgesetzt werden müssen.
Auch bei anderen elektronischen Verfahren, die derzeit diskutiert werden oder unmittelbar vor der Einführung stehen, muss der Grundsatz gelten, Sorgfalt geht vor Schnelligkeit. Dies gilt sowohl für die Gesundheitskarte als auch für die JobCard, zwei anspruchsvolle elektronische Verfahren, die auch für den Datenschutz eine große Herausforderung darstellen. Die damit verbundenen Probleme sind sicherlich lösbar, aber Entwicklung und Einführung müssen gründlich und sorgfältig vorbereitet werden, nicht zuletzt damit diese Karten auf die zwingend erforderliche Akzeptanz bei den Betroffenen stoßen. Im Mittelpunkt stehen dabei das Selbstbestimmungsrecht der Patientinnen und Patienten und die Vertraulichkeit der medizinischen Daten.
Leider hat die Entwicklung technologischer Instrumente, mit denen sich der Einzelne gegen die Erfassung seiner Daten schützen kann, nicht mit der allgemeinen technologischen Entwicklung Schritt gehalten. Umso wichtiger ist es, bei neuen Systemen den Datenschutz bereits in der Entwicklungs- und Konzeptionsphase zu berücksichtigen, wie dies das Bundesdatenschutzgesetz (BDSG) bereits seit 2001 vorsieht. Offenbar hat diese Erkenntnis noch nicht alle Beteiligten erreicht. So musste ich feststellen, dass selbst bei einem

Großprojekt wie der Umstellung der Arbeitslosen- und Sozialhilfe auf das Arbeitslosengeld II elementare Datenschutzanforderungen bei der Systemgestaltung nicht beachtet wurden.
Von grundlegender Bedeutung sind auch die neuen Erkenntnisse bei der Erforschung des menschlichen Genoms und die daraus erwachsenen Anwendungsmöglichkeiten. Aus der DNA lassen sich sowohl die Identität und die Abstammung feststellen als auch Hinweise auf persönliche Eigenschaften und über die Veranlagung zu Krankheiten gewinnen. Die Kontroversen um die Nutzung der DNA als "Fingerabdruck des 21. Jahrhunderts" und über die Zulässigkeit heimlicher Vaterschaftstest sind dabei nur ein erster Ausdruck für die Umwälzungen, die sich aus den neuen Erkenntnissen ergeben. Die hiermit verbundenen Fragen gehen weit über das kodifizierte Datenschutzrecht hinaus. Die kommenden Jahre werden entscheidende Weichenstellungen bringen, ob angesichts dieser qualitativ neuen Möglichkeiten das Persönlichkeitsrecht bewahrt werden kann. Vor diesem Hintergrund mag zwar der sog. "Richtervorbehalt" bei der DNA-Identitätsfeststellung bei anonymen Tatortspuren verzichtbar sein, seine weitere Einschränkung, etwa bei Vorliegen zweifelhafter, weil nicht wirklich freiwilliger Einwilligungen, geht jedoch zu weit.
Unverändert kontrovers bleibt auch die staatliche Kontenabfrage, die auch das Bundesverfassungsgericht beschäftigt. Auch wenn das Bundesministerium der Finanzen inzwischen mit einem "Anwendungserlass" den datenschutzrechtlichen Bedenken zum Teil Rechnung getragen hat und jetzt eine Information der Betroffenen vorsieht, sind noch nicht alle Einwände ausgeräumt. Ich rege deshalb an, dass zumindest die bereits in dem Anwendungserlass geregelten Vorgaben zur Gewährleistung des Datenschutzes in das Gesetz übernommen werden. Generell stellt sich jedoch weiterhin die Frage, ob die in dem Gesetz vorgesehene Verpflichtung der Banken, die Kontostammdaten generell für sehr vielfältige staatliche Aufgaben zum Online-Abruf bereitzuhalten, mit dem Grundsatz der Verhältnismäßigkeit zu vereinbaren ist.
Dieses Beispiel macht im Übrigen deutlich, wie staatliche Stellen zunehmend Zugriff auf Datenbestände der privaten Wirtschaft nehmen, die zu ganz anderen Zwecken angelegt worden sind. Dies ist eine Entwicklung, die in ihrer Tragweite von vielen Bürgerinnen und Bürgern noch gar nicht wahrgenommen worden ist und grundsätzliche Fragen zur Struktur und Wirksamkeit unseres Datenschutzrechts aufwirft, da die klare Trennung zwischen der Datenspeicherung für geschäftliche Zwecke und für staatliche Aufgaben verschwimmt. Bedenklich ist in diesem Zusammenhang auch, dass die Nutzungshäufigkeit von Befugnissen, die das Telekommunikationsgesetz Strafverfolgungs- und Sicherheitsbehörden einräumt, drastisch angestiegen ist. Im Jahr 2004 wurden in fast drei Millionen Fällen Stammdaten von Telekommunikationskunden in einem automatisierten Verfahren bei der Regulierungsbehörde für Telekommunikation und Post nachgefragt (2001: 1,5 Mio.). Diese hat daraufhin insgesamt rund 10 Millionen Abfragen bei Telekommunikationsunternehmen gestellt (2001: 3,2 Mio.). Diese ausufernde Abfrage der Stammdaten von Telekommunikationskunden sollte gesetzlich begrenzt werden.
"Es darf nicht nur den Datenschutzbeauftragten überlassen bleiben, auf Gefährdungen für den Datenschutz hinzuweisen."
Die grenzüberschreitende Datenverarbeitung und vor allem die Datenübermittlungen zwischen den nunmehr 25 Mitgliedstaaten der EU nehmen deutlich zu. Zwar ist die Europäische Datenschutzrichtlinie inzwischen durchgehend in nationales Recht umgesetzt; sie bezieht sich jedoch nicht auf die Verarbeitung personenbezogener Daten im Sicherheitsbereich. Wenn Polizei- und Strafverfolgungsbehörden intensiver zusammenarbeiten und dabei auch personenbezogene Daten ohne Rücksicht auf nationale Grenzen austauschen sollen, wie dies im Haager Programm beschlossen wurde, muss der Datenschutz auch auf diesem Gebiet europäisiert werden. Ausgangspunkt müssen dabei die Datenschutz-Grundrechte der Europäischen Grundrechtecharta sein, die unverändert in den Entwurf für eine Europäische Verfassung übernommen wurden.
Aber auch der nationale Gesetzgeber bleibt weiter gefordert, denn angesichts der rasanten technologischen Entwicklung ist eine stetige Weiterentwicklung der geltenden datenschutzrechtlichen Bestimmungen zwingend erforderlich. Leider herrscht hier aber eher Stillstand: Das für den Vollzug des BDSG 2001 erforderliche Datenschutzauditgesetz, das vom Bundestag seit langem geforderte Arbeitnehmerdatenschutzgesetz und das dringend notwendige Gendiagnostikgesetz lassen weiter auf sich warten. Auch die angekündigte grundlegende Modernisierung des Datenschutzrechts kommt nicht voran. Lediglich in einigen gesetzlichen Spezialregelungen konnten erfreuliche Ergebnisse erreicht werden, etwa bei der Gesundheitskarte.
Es darf nicht nur den Datenschutzbeauftragten überlassen bleiben, auf Gefährdungen für den Datenschutz

hinzuweisen. Vielmehr müssen die Bürgerinnen und Bürger ihr Grundrecht auf informationelle Selbstbestimmung aktiv wahrnehmen und den hierfür erforderlichen gesetzlichen Rahmen einfordern. Denn gerade für bedrohte Grundrechte gilt, dass sie sich nur behaupten werden, wenn sie in Anspruch genommen und verteidigt werden.
