Datenschutz im Spannungsfeld von Freiheit und Sicherheit

Dokumentation der Fachkonferenz
Datenschutz 2007 am 14. Juni 2007, Berlin

FRIEDRICH EBERT STIFTUNG

Diese Broschüre ist eine kurze Dokumentation des Forums I der Fachkonferenz Datenschutz 2007 »Herausforderungen für die Modernisierung des Datenschutzrechts« der Friedrich-Ebert-Stiftung am 14. Juni 2007 in Berlin.
Weitere Informationen auf www.fes.de/medienpolitik.

ISBN 978-3-89892-728-4

Herausgeber: Stabsabteilung der Friedrich-Ebert-Stiftung
Redaktion: Beate Martin, Eike-Gretha Breuer

Hiroshimastr. 17, D–10785 Berlin
Stabsabteilung, www.fes.de/stabsabteilung

Umschlagillustration: Pellens Kommunikationsdesign GmbH, Bonn
Gestaltung: Doreen Engel, Berlin
Druck: bub Bonner Universitäts-Buchdruckerei

Printed in Germany August 2007

INHALT

JÖRG TAUSS,
MdB, Sprecher Bildung, Forschung und Medien der SPD-Bundestagsfraktion

EINLEITUNG Die fragile Balance zwischen Sicherheit und Freiheit – Strafverfolgung und Terrorismusbekämpfung vs. Grundrechteschutz

Auch wenn so manche bereits am Nachruf für den Schutz der personenbezogenen Daten schreiben, bleibt die Wahrung des Rechts auf informationelle Selbstbestimmung ein zentrales Ziel bei der politischen Gestaltung der Wissens- und Informationsgesellschaft. Angesichts der immensen technologischen Herausforderungen einer weltweit vernetzten Gesellschaft und angesichts neuer Gefährdungen ist die Wahrung des Rechts auf informationelle Selbstbestimmung wichtiger und notwendiger denn je.

Gegenwärtig wird in Deutschland und in den europäischen Ländern die Umsetzung der umstrittenen Richtlinie zur Vorratsdatenspeicherung beraten. Angesichts der Eingriffstiefe in die Grundrechte der europäischen Bürgerinnen und Bürger und angesichts der Reichweite – betroffen sind 480 Millionen Menschen in Europa, davon 80 Millionen in Deutschland – stellen sich die Fragen der Angemessenheit und Verhältnismäßigkeit in besonderem Maße. Die Politik ist in der Pflicht, diese hinreichend zu beantworten. Hier gilt es, rechtsstaatliche Grundsätze zur Erhebung und Verarbeitung dieser Daten, klare Löschungspflichten sowie Beschränkungen des

Zugangs auf richterliche Anordnung und lediglich zur Aufklärung schwerer Straftaten zu formulieren.

Telekommunikationsüberwachungsmaßnahmen und andere verdeckte Ermittlungsmaßnahmen greifen besonders intensiv in die Grundrechte der Bürgerinnen und Bürger ein. Aus diesem Grund müssen für ihre Zulässigkeit strenge Voraussetzungen gelten und der Rechtsschutz wirksam ausgestaltet sein. Angesichts des entsprechenden vorliegenden Gesetzentwurfes bleiben aber mit Blick auf den Grundrechtsschutz erhebliche Zweifel und massive – auch verfassungsrechtliche – Bedenken bestehen. Dies gilt beispielsweise für die vorgesehene Neuordnung der Zeugnisverweigerungsrechte und die damit einhergehende Relativierung der Zeugnisverweigerungsrechte für Journalisten und Medienvertreter.

> „Wir befinden uns auf einem Weg von einem Rechtsstaat hin zu einem systematischen Verdachtsstaat. Dies kann u.a. nur durch einen modernen Datenschutz verhindert werden.“
>
> (JÖRG TAUSS)

Diese aktuelle Diskussion macht allerdings auch deutlich, dass immer wieder um die Balance zwischen Freiheit und Sicherheit gerungen werden muss und zwar sowohl bezüglich der bürgerlichen Freiheiten wie auch der Medienfreiheiten. Diese Balance zwischen Freiheit und Sicherheit wird immer wieder infrage gestellt. Ich denke schon, dass wir uns zwischenzeitlich an einem Wendepunkt befinden von einer freien Gesellschaft zumindest in die Richtung einer unfreien Gesellschaft.

Notwendig ist in einer demokratisch verfassten Gesellschaft eine verfassungskonforme Abwägung zwischen den notwendigen Mitteln – auch in einer neuen Gefährdungssituation durch organisierte Kriminalität und Terrorismus. Auf der einen Seite stehen dabei Terrorismusbekämpfung und Straf-

verfolgung, auf der anderen der Grundrechteschutz, etwa das Recht auf informationelle Selbstbestimmung, aber auch andere Grundrechte wie etwa die Medienfreiheiten.

Nehmen wir an dieser Stelle stellvertretend die RFID-Technologie mit ihren positiven, aber eben auch mit ihren negativen Aspekten und Gefahren. Der Bürger muss umfassend über den Einsatz, Verwendungszweck und Inhalte von RFID-Tags informiert werden. Als Betroffener muss man die Möglichkeit haben, die RFID-Tags dauerhaft zu deaktivieren respektive die darauf enthaltenden Daten endgültig zu löschen. Eine heimliche Erstellung personenbezogener Verhaltens-, Nutzungs- oder gar Bewegungsprofile darf es nicht geben.

Gerade das Beispiel RFID zeigt in aller Deutlichkeit, dass eine autonome Handlungs- und Kommunikationsfähigkeit der Bürgerinnen und Bürger – als Voraussetzung für die gesellschaftliche Akzeptanz und Entwicklung der zivilen Informationsgesellschaft – gefährdet sein kann. Dies gilt es zu verhindern, da sich die fehlende Akzeptanz seitens der Nutzer auch negativ auf die wirtschaftlichen Entwicklungschancen entsprechender Angebote auswirken. Basis für Akzeptanz ist das Vertrauen der Anwender in die Technologien der Informationsgesellschaft. Und Datenschutz ist – mittlerweile auch weltweit anerkannt – einer der zentralen Akzeptanzfaktoren dafür.

Auch wenn das deutsche Datenschutzrecht international eine führende Stellung einnimmt, ist das gegenwärtige Datenschutzrecht dennoch nur noch bedingt geeignet angesichts der geschilderten Veränderungen. Neue Formen personenbezogener Daten und deren Verarbeitung werden bisher nur ungenügend aufgenommen, die Gefahren und Chancen neuer Techniken der Datenverarbeitung bisher unzureichend berücksichtigt. Darüber hinaus sind zahlreiche Formulierungen zum Teil widersprüchlich oder unübersichtlich.

Datenschutz als dynamischer Prozess

Eins möchte ich mit aller Deutlichkeit sagen: Wirkungsvoller Datenschutz ist kein klar definierter und abgeschlossener Bereich. Das Datenschutzrecht ist in meinen Augen ein überaus dynamischer, sich im permanenten Wandel befindlicher Prozess, so dass bestehende Normen immer wieder aufgrund aktueller Entwicklungen und Erkenntnisse Anpassung finden müssen. Dies bedeutet keine Überregulierung. Das Gegenteil ist nach Auffassung der SPD-Bundestagsfraktion der Fall. Erst ein modernes und fortentwickeltes Datenschutzrecht führt zu unbürokratischen und effizienten Lösungen und ist so ein wichtiges Instrument zum Bürokratieabbau.

Ein modernes und effizientes Datenschutzrecht ist nicht nur ein Instrument des Bürokratieabbaus, es ist vielmehr auch ein wirtschaftlicher Standortvorteil, insbesondere dann, wenn das bestehende Datenschutzrecht um neue Datenschutzinstrumente ergänzt wird. Ein solches wichtiges Instrument ist das Datenschutzauditgesetz wie in § 9a des Bundesdatenschutzgesetzes (BDSG) vorgesehen und wie zum wiederholten Mal auch vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) gefordert.

Die Vorteile eines solchen Datenschutzauditgesetzes liegen in meinen Augen auf der Hand. Dies gilt sowohl für den Verbraucher, als auch für die Wirtschaft:

- Der Verbraucher erhält durch ein Audit erstmalig die Möglichkeit Produkte und Dienstleistungen hinsichtlich ihrer Datenschutzkonformität zu überprüfen bzw. zu vergleichen. Dies führt, davon bin ich überzeugt, u.a. zu der von mir angesprochenen und überaus notwendigen Stärkung der Akzeptanz des Datenschutzes.
- Für die Wirtschaft bedeutet die Möglichkeit, eigene Produkte und Dienstleistungen durch eine unabhängige, und evtl. öffentliche Stelle, auditieren zu lassen, einen nach-

haltigen Wettbewerbsvorteil gegenüber Konkurrenten und kann gleichzeitig die Selbstverantwortung im Bereich des Datenschutzes und der Datensicherheit stärken. Die Firma Microsoft hat uns dies im Februar eindrucksvoll gezeigt, als man zwei Produkte durch das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein auditieren ließ. Auch andere Stimmen aus Wirtschaft und Industrie und insbesondere auch aus den entsprechenden Interessenverbänden zeigen, dass ein solches Datenschutzaudit mehr und mehr gewollt ist.

Biometrische Ausweisdokumente

Biometrische Verfahren rücken nicht zuletzt auch aufgrund gestiegener Sicherheitsanforderungen und des Wunsches nach absolut täuschungs- oder fälschungssicherer Identifikation bzw. Verifikation von Personen immer mehr in den Blickpunkt. Dabei berühren diese Verfahren die unterschiedlichsten und insbesondere für den Bürger weitest reichenden Bereiche.

Mir geht es dabei weniger um die Frage der Kosten einer Nutzung von biometrischen Merkmalen in Ausweisdokumenten, sondern vielmehr um die grundsätzliche Zuverlässigkeit sowie die Angreifbarkeit solcher Systeme. Ich glaube nicht, dass der Einsatz von Biometrie-Pässen wirklich ein Mehr an Sicherheit bringt und bringen wird. Daran haben auch die gebetsmühlenartig vorgebrachten Hinweise und Forderungen des letzten Bundesinnenministers nichts geändert.

Ein digitales Foto und Fingerabdrücke im Pass verraten in meinen Augen gar nichts über mögliche kriminelle oder terroristische Absichten des Passinhabers. Vielmehr bin ich überzeugt, dass ein solcher ePass schnell selbst zum Sicherheitsrisiko werden kann, denn bei einer zehnjährigen Gültigkeit

von Reisepässen kann doch heute niemand seriös ausschließen, dass die biometrischen Daten nicht doch irgendwann unbemerkt gelesen, kopiert oder verändert werden können.

Abschließend sei jedoch noch – auch im Sinne einer Selbstbeauftragung – darauf hingewiesen, dass die Umsetzung eines wirksamen Datenschutzes in den 30 Jahren seiner Geschichte eigentlich nie eine Angelegenheit der Exekutive, sondern immer der Parlamente war.

Hier sind also die Parlamente in den Ländern, im Bund und in Europa in der Pflicht, dem Recht auf informationelle Selbstbestimmung auch in der globalen Wissens- und Informationsgesellschaft Geltung zu verleihen. Ein wichtiges und ermutigendes Zeichen war die große Resonanz, die der erste europäische Datenschutztag in diesem Jahr in der Öffentlichkeit gefunden hat, und die Dringlichkeit, mit der Bürgerinnen und Bürger die oft mangelnde Abwägung zwischen den Sicherheitsinteressen auf der einen und den Freiheitsrechten der Menschen auf der anderen Seite eingefordert haben: Ermutigende Signale der notwendigen politischen Unruhe, wie sie auch von der diesjährigen FES-Datenschutzkonferenz ausgingen.

PROF. DR. DRES. H. C. SPIROS SIMITIS,
Forschungsstelle für Datenschutz, Universität Frankfurt a. M.

Datenschutz heute: Prinzipien und Ambivalenz einer Modernisierung

1. »Modernisierung« als Reformaufschub

Einen besseren Zeitpunkt hätte man für diese Konferenz kaum wählen können: Vorratsdatenspeicherung, Online-Durchsuchung, Fluggastdatenübermittlung, Gentests, Schülerdateien, biometrische Angaben – alles Problemkomplexe, die förmlich dazu zwingen, sich zu fragen, ob der Datenschutz in seiner jetzigen Form noch seinen Aufgaben genügen kann.

Nur mit der »Modernisierung« kann ich, zugegeben, wenig anfangen. Aus einem durchaus nahe liegenden Grund: In der Geschichte des Datenschutzes hat sich die »Modernisierung« wieder und wieder als ein wahrlich doppeldeutiges Wort erwiesen. Sie signalisiert einerseits die Bereitschaft, ja, die Notwendigkeit, darüber nachzudenken, wie ein wirklich wirksamer Datenschutz aussehen müsste. Sie ist aber andererseits, wie die Erfahrung nur zu gut zeigt, ein auch und vor allem regelmäßig wiederkehrendes Generalthema endloser Debatten, das Reformen, gerade in Zeiten, in denen sie besonders nötig gewesen wären, nicht bewirkt, sondern nur noch weiter hinausgeschoben hat.

Die Erinnerung an das Bundesdatenschutzgesetz (BDSG) 2003 drängt sich fast von selbst auf. Wohl hatte die Diskussion über eine Revision der gesetzlichen Anforderungen an die Verwendung personenbezogener Daten schon in den achtziger Jahren angesetzt. Doch erst die EG-Datenschutzrichtlinie von 1995 schloss jede Alternative zu einer sofortigen legislativen Intervention ebenso unmissverständlich wie verbindlich aus. Über manche ihrer Vorschriften kann man sicherlich unterschiedlicher Meinung sein.

In einer Hinsicht ist aber die Richtlinie vorbildlich: Anders als sonst nimmt die EG-Kommission nicht ihre vom Europäischen Gerichtshof lange Zeit geteilte Position ein, mit der Entscheidung für die Richtlinie eine einheitliche, von allen Mitgliedstaaten gleichermaßen zu respektierende und deshalb auch genau umzusetzende Regelung geschaffen zu haben. EG-Kommission und Rat waren sich vielmehr nach einer langen und kontroversen Diskussion einig, bei der Verarbeitung personenbezogener Daten auf eine Technologie reagieren zu müssen, die sich konstant wandelt und daher fortwährend neue Fragen aufwirft, auf die es genauso kontinuierlich einzugehen gilt. Wenn deshalb die Richtlinie nicht zum Hemmnis einer effizienten Auseinandersetzung mit den Datenschutzproblemen werden soll, muss sie zwar den Mitgliedstaaten vorschreiben, wie sie vorzugehen haben, ihnen jedoch zugleich die Möglichkeit einräumen, den Datenschutz weiterzuentwickeln. Mit anderen Worten: Harmonisierung darf nicht zu einem eindeutig kontraproduktiven Stillstand führen. Genau diese Überzeugung lässt sich den Erwägungsgründen klar entnehmen.

Kaum ein anderer Mitgliedstaat der Europäischen Union hat so viel zur Anerkennung und Absicherung des Datenschutzes beigetragen wie die Bundesrepublik. Ebenso wenig lässt sich freilich übersehen, dass kaum ein anderer Mitgliedstaat so lange die Umsetzung der Richtlinie hinausgezögert hat und so bemüht war, das eigene Recht möglichst nicht zu ändern. Gerade in diesem Zusammenhang avancierte die »Moderni-

sierung« alsbald zu einem der zentralen Stichworte. Sie sollte über die evidenten Mängel der beabsichtigten Novellierung des BDSG hinwegtrösten und die Hoffnung auf eine echte Reform aufrechterhalten. Ganz in diesem Sinn wurde auch eine Modernisierungsstudie vergeben. Ihre präzisen, eingehend begründeten Vorschläge sind allerdings bis heute folgenlos geblieben und reihen sich mittlerweile in die immer längere Liste fehlgeschlagener Reformansätze ein.

Doch nicht nur deshalb mahnt die »Modernisierung« zur Vorsicht. Allzu leicht könnte sie dazu verführen, die Tragweite der unumgänglichen Korrekturen zu unterschätzen. Wie weit sie reichen müssen, illustrieren die jüngsten Ansätze zur Verarbeitung der Telekommunikationsdaten ebenso wie der nahezu grenzenlose Zugriff auf personenbezogene Angaben im nichtöffentlichen Bereich. Beides zwingt dazu, Kontext, Verlauf und Bedingungen der Verarbeitung zu bedenken, und erst recht den Akzent auf jenen Punkt zu legen, der wie kein anderer die Geschichte des Datenschutzes von Anfang an bestimmt hat: die Verarbeitungstechnologie. Schlägt man aber diesen Weg ein, dann zeichnet sich deutlicher denn je die Notwendigkeit einer »Modernisierung« ab, die einer radikalen Reform der bisherigen Regelungsprämissen gleichkommt.

2. Technische Infrastruktur und vorhandene Daten wecken Begehrlichkeiten

Lassen Sie mich nun versuchen, diese Aussage in der Kürze der mir zur Verfügung stehenden Zeit wenigstens stichwortartig zu präzisieren:

a. Datenschutzgesetze sind durchweg vor dem Hintergrund einer automatisierten Verarbeitung personenbezogener Angaben entstanden. So evident die – allen Vorbehalten zum Trotz – ungleich besseren Verarbeitungsmodalitäten waren, so klar schien es zu sein, dass auch bei einer automatisierten Verarbeitung mit einer begrenzten Speicherungskapazität gerechnet werden müsste. Genau diese heute noch verbreitete Annahme ist überholt. Speicherungsgrenzen sind nur noch Merkmale einer überwundenen Entwicklungsetappe der Verarbeitungstechnologie.

Zudem: Wo sich die Daten jeweils befinden, ist inzwischen ebenso gleichgültig, wie sich am besten an jenem Verarbeitungsziel nachvollziehen lässt, das wie kein anderes jahrzehntelang die Diskussionen über die Dringlichkeit von Datenschutzvorkehrungen beherrscht hat: die Einrichtung systematisch ausgebauter zentraler Datenbanken. Was im Vorfeld des ersten Datenschutzgesetzes, des Hessischen Gesetzes von 1970, oder bei der Auseinandersetzung über das Volkszählungsgesetz von 1983 und bei der Kritik an manchen der vor gar nicht langem vorgelegten Verarbeitungspläne im Sicherheits-, Sozial- oder Gesundheitsbereich noch als Sinnbild einer regelungspflichtigen Verwendung personenbezogener Angaben erschien, ist einer Verarbeitungsrealität gewichen, welche ganz im Zeichen einer »Vernetzung« steht, die multiple, unendlich variable Verwendung sichert.

Nicht von ungefähr warnte deshalb Jennifer Barret im Namen des wohl größten kommerziellen »Data Warehouse« der Vereinigten Staaten, Acxiom, anlässlich der Vorgespräche über eine Kooperation der Sicherheitsbehörden mit den bei der Verarbeitung personenbezogener Daten führenden Unternehmen im Rahmen der nach dem 11. September 2001 eingeleiteten Antiterrorismus-Maßnahmen und besonders der Bestrebungen, Täterprofile so schnell wie möglich zu erstellen, nachdrücklich davor, von zentralen Datenbanken zu sprechen, ja, sie überhaupt in Erwägung zu ziehen. Ärgerliches Misstrauen, ganz zu schweigen von einer unverhohlen verarbeitungsfeindlichen Kritik, ließen sich ansonsten nicht vermeiden. Demgegenüber sei eine Vernetzung weitaus unspektakulärer und ohnehin jeder wie immer zentralisierten Verarbeitung überlegen. Lediglich sorgfältig konstruierte »Links« würden

daher einen ebenso schnellen wie komplikationslosen Zugriff auf alle nur gewünschten Daten, damit aber auch eine erfolgreiche Zusammenarbeit öffentlicher und nichtöffentlicher Stellen garantieren.

Wie konsequent die Dezentralisierung angegangen wird, illustriert eine ständig wachsende Zahl von Beispielen, darunter die unmittelbar bevorstehende »Telekommunikationsüberwachung«. Die vorgeschlagene gesetzliche Regelung sieht bewusst davon ab, die Erhebung und Speicherung der dafür in Betracht kommenden Daten den Sicherheitsbehörden zu übertragen. Sie begründet stattdessen eine Pflicht der »Telekommunikationsdiensteanbieter«, bestimmte, genau umschriebene Angaben auch und gerade auf Vorrat zu verarbeiten. Noch einmal: Die Verwendung der Daten ist eindeutig nicht auf besondere Interessen der jeweils spezifischen Unternehmen zurückzuführen, sondern ausschließlich auf die schon in der EG-Richtlinie zur Vorratsdatenspeicherung vom März 2006 betonten und sanktionierten Erwartungen der Sicherheitsbehörden.

b. Die veränderte technische Infrastruktur hat sich längst auf die Verarbeitung personenbezogener Daten ausgewirkt. Angaben, die nicht verarbeitet werden, gibt es praktisch nicht mehr. Die Gründe sind verschieden. Drei der wichtigsten möchte ich ausdrücklich ansprechen:

> ***Erstens: eine Verarbeitungspolitik***, die sich zunehmend an der Prävention orientiert. Vorschriften, wie die eben erwähnten zu den Telekommunikationsdaten, gesetzlich angeordnete, sich in genau vorgeschriebenen Zeitabständen wiederholende Vorsorgeuntersuchungen für immer weitere Krankheiten, oder die Einbeziehung aller Schulkinder in langfristig angelegte, minutiös ausgestaltete Dateien sind Wahrzeichen konsequent intensivierter Anstrengungen, Risiken rechtzeitig aufzudecken und abzufangen.

Die Verarbeitung personenbezogener Daten hört also auf, in erster Linie Reaktion auf einzelne Vorgänge zu sein und ihrer Aufklärung zu dienen, und wird zum primären Mittel einer generellen, eindeutig präventiven Verhaltenssteuerung. Sie kommt der jeweiligen Gefahr zuvor, indem sie den Weg markiert, den die Betroffenen befolgen müssen. Wohlgemerkt, die Prävention mag zwar vor allem mit staatlichen Aktivitäten assoziiert werden. Sie ist jedoch keineswegs darauf beschränkt, sondern durchdringt genauso den nichtöffentlichen Bereich, wie allein schon das Beispiel der Kranken- und Lebensversicherungen verdeutlicht.

Die Akzentuierung der Prävention bleibt nicht ohne Folgen für den Datenbestand. So begnügt sich die britische Biobank keineswegs mit medizinischen und genetischen Angaben. Will sie ihr Ziel wirklich erreichen, die Ursachen typischer Krankheiten einer alternden Gesellschaft zu erforschen und die Grundlagen für eine verlässliche Prävention von Demenz, Parkinson oder Alzheimer zu schaffen, muss sie ihre Informationsansprüche sehr viel weiter spannen und Daten zur familiären Situation mithin genauso umfassend einbeziehen wie Angaben zu den professionellen Aktivitäten, zum sozialen Umfeld oder zu möglicherweise relevanten Umweltfaktoren. Wie die Informationsansprüche im Einzelnen aussehen, richtet sich verständlicherweise nach dem konkreten Präventionszweck. In einer Beziehung decken sich freilich alle präventionsbestimmten Verarbeitungsaktivitäten: Sie erhöhen und differenzieren zugleich den Datenbestand um ein Vielfaches.

Zweitens: die zunehmende Individualisierung der Datenbestände im nichtöffentlichen Bereich. Beispielhaft dafür ist die fortschreitende Verdrängung der Kredit- durch die Kundenkarten. Sie spiegelt eine Politik wider, die einzelne Kunden langfristig an das Unternehmen binden und sie damit dazu bringen möchte, es als den einzig in Betracht kommenden Lieferanten der jeweils gewollten Produkte anzusehen. Um

genau dieses zu erreichen, optieren die Unternehmen für eine bereits von der Werbung vorexerzierte Strategie.

Die Kunden werden aus der Anonymität geholt und, soweit es nur geht, individualisiert. Was also zuvörderst interessiert, ist eine möglichst exakte Kenntnis der individuellen Gewohnheiten, Wünsche, Reaktionen und überhaupt aller für eine verlässliche Bewertung der Kunden hilfreichen Daten. Die Kundenkarte schafft die Voraussetzungen dafür, hat aber noch einen zweiten, mindestens ebenso wichtigen Vorteil: Sie sichert eine exklusive Verarbeitung. Wie die Prävention wirkt sich jedoch auch die Individualisierung auf die Datenbestände aus und das Ergebnis ist erneut eine beträchtliche Zunahme der Angaben, verbunden mit einer ebenso bemerkenswerten Differenzierung.

Drittens: eine Kommerzialisierung der Daten. Multifunktionalität und jederzeitige Erreichbarkeit verleihen den personenbezogenen Angaben einen wirtschaftlich nutzbaren Mehrwert und verwandeln sie so in ein selbständig verwertbares Informationskapital. Die Konsequenz ist allerdings einmal mehr ein Ausbau der Datenbestände. Eine erfolgreiche Vermarktung zwingt sehr bald dazu, die bereits gespeicherten Angaben, mit weiteren, dank einer möglichst allgemein formulierten Einwilligung der Betroffenen erhobenen Daten anzureichern, um zusätzlichen Informationsanforderungen nachkommen und vor allem neue Kunden gewinnen zu können.

c. Die Auswirkungen der nachhaltig veränderten Datenbestände im nichtöffentlichen Bereich lassen sich nur richtig einschätzen, wenn eine weitere, zumeist nicht berücksichtigte Folge bedacht wird: ***die Reaktion der öffentlichen Stellen***. Die bereits angesprochenen Erfahrungen in den Vereinigten Staaten sind dafür genauso bezeichnend wie der Reflex auf das britische Großprojekt einer Biobank. Die Intention, sie einzurichten, war noch gar nicht richtig angekündigt, als sich schon

die Sicherheitsbehörden meldeten. Was sie so schnell auf den Plan gerufen hatte, war die Absicht der Biobank, alle von ihr verarbeiteten Daten in fortlaufend ergänzte persönliche Profile umzusetzen: für die Sicherheitsbehörden eine geradezu einmalige Informationsquelle, die neue, viel versprechende Fahndungsmöglichkeiten eröffnete. Grund genug, um keinen Zweifel am Anspruch zu lassen, die Profile jederzeit verwerten zu können.

Spätestens daran wird aber auch deutlich: Die öffentlichen Stellen verzichten zunehmend auf eigene Erhebungen und greifen dafür auf die von nichtöffentlichen Stellen verarbeiteten Angaben zurück. Multifunktionalität und Vernetzung bahnen dazu den Weg. Je mehr sich solche Tendenzen verfestigen, desto nachhaltiger weicht der einst für selbstverständlich gehaltene Aufbau ebenso umfassender wie klar getrennter öffentlicher und nichtöffentlicher Datenbanken einer grauen Verarbeitungszone. In dieser Grauzone sind personenbezogene Daten, die von nichtöffentlichen Stellen für ihre spezifischen Zwecke erhoben und genutzt werden, von vornherein auch für eine Verwendung durch öffentliche Stellen bestimmt.

3. Gesetzeskonforme Verfassungssprache entsprechend des Technologiefortschritts

Punktuelle Korrekturen reichen vor diesem Hintergrund nicht aus. Vielmehr ist ein Datenschutzkonzept nötiger denn je, das die Verwendung personenbezogener Angaben, auch in Kenntnis des Technologiewandels und seiner Folgen, an entschieden schärfere Voraussetzungen knüpft.

a. Die erste und wichtigste Bedingung ist ein ***gesetzlich abgesicherter Informationsverzicht***. Gerade weil es keine Schwierigkeiten mehr bereitet, alle vorhandenen Daten dank einer technisch jederzeit möglichen Vernetzung zu bekommen und für beliebig neue Zwecke zu nutzen, muss es Zugriffsgrenzen

geben, die nicht überschritten werden dürfen. An der Bereitschaft dazu wird sich letztlich nicht nur die Existenz des Datenschutzes entscheiden. Lediglich mit dieser Bereitschaft kann es gelingen, eine Balance von Freiheit und Sicherheit zu finden, die weder durch die Priorität eines wie auch immer begründeten »Grundrechts auf Sicherheit« noch durch eine Unzahl von Generalklauseln, mit denen sich jede Verarbeitungsschranke problemlos umgehen lässt, unterlaufen wird und ebenso wenig verdrängt, dass eine demokratische Gesellschaft Risiken in Kauf nehmen muss, wenn sie den eigenen Prämissen wirklich gerecht werden will.

> „Wo es technisch keine Verarbeitungsgrenzen mehr gibt und die Anzahl der gespeicherten Daten ständig wächst, entscheidet sich die Existenz des Datenschutzes nicht mehr wie bislang an der Frage, ob und welche Daten überhaupt verarbeitet werden dürfen, sondern an der Bereitschaft, auf den Zugriff gerade dann zu verzichten, wenn die Daten vorhanden sind und durchaus verarbeitet werden könnten.“
>
> (Prof. Dr. jur. Drs. h.c. SPIROS SIMITIS)

Wie schwer es freilich fällt, einen Informationsverzicht zu akzeptieren, lässt sich schon an den Diskussionen über die geplante Einrichtung von Biobanken erkennen. Bei der britischen Biobank herrscht mittlerweile wohl Konsens darüber, dass die Sicherheitsbehörden unter bestimmten Bedingungen durchaus berechtigt sind, auf sämtliche Daten zuzugreifen. Der »UK Biobanks Ethics and Governance Council« hat jedoch in seinem Jahresbericht für 2006 ausdrücklich bestätigt, jedem Versuch an die Daten heranzukommen, »rigoros« zu widersprechen. Zweifel gab es auch im Nationalen Ethikrat. Und wiederum wurden diese mit dem Hinweis auf die Bedeutung begründet, die den Daten besonders bei der Aufklärung schwerer Straftaten zukommen könnte. Doch die Mehrheit

des Rates ließ sich nicht beirren. Sie stimmte dem Aufbau von Biobanken nur unter der Bedingung zu, dass die Daten ausschließlich für wissenschaftliche Zwecke verarbeitet werden dürften.

Beispiele wie dieses sind freilich nach wie vor seltene Ausnahmen. Der Streit um die Maut illustriert die unverändert vorherrschende Tendenz. Gleich zweimal hat sich der Bundestag für eine klare Zweckbindung der Mautdaten ausgesprochen und besonders bei seiner zweiten Entscheidung alle Versuche einer Zweckentfremdung mit noch präziseren Formulierungen zurückgewiesen. Doch die Forderungen, Ausnahmen gerade für die Sicherheitsbehörden vorzusehen, haben nicht nachgelassen. Im Augenblick spricht deshalb alles dafür, dass es zu einer genau diesen Erwartungen entsprechenden Korrektur der gesetzlichen Vorschriften kommen wird.

b. Die Rückkehr zu einer verfassungskonformen Gesetzessprache ist eine weitere Voraussetzung für ein Datenschutzkonzept, das wirklich halten kann, was es verspricht. Gemeint ist jene vom Bundesverfassungsgericht schon im Volkszählungsteil für jeden Eingriff in die informationelle Selbstbestimmung geforderte »Normenklarheit«. Doch die Erinnerung an die so eindringliche, auch später immer wieder betonte Mahnung des Gerichts ist offensichtlich verblasst. Vorschriften zur Verarbeitung personenbezogener Daten sind mittlerweile Musterfälle einer exzessiven Verwendung von Generalklauseln und unbestimmten Begriffen. Sicher, bewusst allgemein gehaltene Formulierungen hatte es schon in den frühesten Datenschutzvorschriften gegeben. Doch dahinter stand die Absicht, den Anwendungsbereich der Verarbeitungsvorgaben in Anbetracht einer noch nicht hinreichend bekannten Technologie und ihrer deshalb nur schwer abschätzbaren Folgen möglichst offen zu halten und so zugleich den Schutz der Betroffenen zu maximieren.

Genau das Gegenteil ist gegenwärtig der Fall. Generalklauseln sowie eine zunehmend unklare Wortwahl sind Instrumente einer Verarbeitungspolitik, die kaum verhüllt den Zweck verfolgt, die Betroffenen zurückzudrängen. So hat sich etwa der »Terrorismus« zum Schlüsselbegriff des Zugriffs der Sicherheitsbehörden auf personenbezogene Daten entwickelt. Doch so bereitwillig der Gesetzgeber darauf verweist, so auffällig ist der Verzicht auf eine Definition. Weder die, um nur die vergangenen achtzig Jahre zu nehmen, so überaus unterschiedlichen Vorstellungen darüber, wer zu den »Terroristen« rechnet, noch die verfassungsrechtlichen Anforderungen an die Gesetzessprache haben den Gesetzgeber veranlasst, sich um eine auch nur halbwegs präzise Umschreibung zu bemühen. Wohl wurde ein bestimmter Kontext präsumiert, aber nicht dort ausdrücklich angesprochen, wo es entscheidend darauf ankommt: im Gesetzestext.

Kein Zweifel, um »terroristischen« Aktivitäten rechtzeitig und wirksam zu begegnen, kann, ja, muss es unter Umständen nötig sein, den Sicherheitsbehörden mehr Befugnisse einzuräumen, personenbezogene Daten zu verwenden. Nur darf sich der Gesetzgeber nicht auf eine solche Kurzformel beschränken. Die gesetzlichen Vorschriften müssen vielmehr in einer auch und besonders für die Betroffenen nachvollziehbaren Weise angeben, welche Daten wofür genau unter welchen Bedingungen von wem und für wie lange verarbeitet werden sollen. Wo es an diesen Aussagen fehlt, wird das Gesetz zu einer rein formalen Voraussetzung degradiert. Erst recht erweist sich aber die Normenklarheit als eine verbindlich vorgeschriebene, eindeutig inhaltliche Anforderung, die sicherstellen soll, dass Verlauf und Tragweite der Verwendung personenbezogener Daten erkannt und damit auch kontrolliert werden können.

c. Ferner: Die supranationalen Instanzen müssen endlich akzeptieren, dass der Datenschutz eine auch für sie verbindliche Vorgabe ist, die deshalb bei allen personenbezogene Daten betreffenden Entscheidungen beachtet werden muss. Das immer deutlichere Übergewicht supranationaler Anforderungen und die parallel dazu schrumpfende Kompetenz des nationalen Gesetzgebers sind längst feste Merkmale einer gewandelten Regelungskompetenz. Die EG-Datenschutzrichtlinie von 1995 war ein erstes unübersehbares Zeichen dafür. Wie der Datenschutz konkret auszusehen hat, war fortan, jedenfalls für den nicht-öffentlichen Bereich, zuvörderst ihr zu entnehmen. Doch dabei konnte es nicht bleiben.

Eine Europäische Union, die sich spätestens seit den Verträgen von Maastricht und Amsterdam als politische Einheit versteht und sich auch so verhält, muss Regelungen treffen, die zwangsläufig eine Verwendung personenbezogener Daten festschreiben, gleichviel, ob es generell um den Justiz- und Sicherheitsbereich oder spezieller um Immigrations-, Asyl- oder Zollfragen geht. Schengen, Europol, Eurodac sowie das Visa- und das Zollinformationssystem sind nur einige der Stationen auf diesem Weg, die allerdings schon genau erkennen lassen, wie die Datenverarbeitung einerseits in die Politik der Europäischen Union integriert und von ihrer Initiative sowie ihren Entscheidungen bestimmt wird, andererseits jedoch zunehmend dazu führt, in den nationalen, diesmal aber öffentlichen Bereich mit ebenso weit reichenden Folgen wie bei der EG-Datenschutzrichtlinie einzugreifen.

Mit einem Unterschied freilich: Die EG-Kommission wollte mit der Richtlinie gemeinschaftsweite Datenschutzgrundsätze durchsetzen. Der Rat hat die Datenverarbeitung genauso unionsweit umgestaltet, ohne aber auf den Datenschutz Rücksicht zu nehmen. Alle Bemühungen, Datenschutzgrundsätze zu beschließen, an denen jede vom Rat beschlossene Regelung gemessen werden müsste, sind bislang gescheitert. Mehr noch: Der Rat hat, wie zuletzt beim europaweiten Direktzugriff auf die Datenbanken der Sicherheitsbehörden demonstriert, seine Interventionschancen nachhaltig genutzt, um den Verarbeitungsspielraum besonders im Justiz- und Sicherheitsbereich

auszubauen, ohne sich überhaupt, oder allenfalls ganz am Rande auf durchaus nahe liegende Datenschutzeinwände einzulassen.

So überrascht es nicht weiter, dass die Mitgliedstaaten es immer häufiger vorgezogen haben, sich mit Verarbeitungsabsichten direkt an den Rat zu wenden, um dann seine Entscheidung als supranationale Vorgabe für eine möglichst komplikationslose Anpassung des nationalen Rechts zu nutzen. Der Vorschlag, die unter Datenschutzgesichtspunkten unverändert unhaltbare Vereinbarung über die Weitergabe von Flugpassagierdaten in die Vereinigten Staaten zum Anlass zu nehmen, um ähnliche Regeln für die Einreise von Flugpassagieren in die Europäische Union vorzusehen, ist das jüngste Beispiel dafür. Einmal mehr werden die auf der nationalen Ebene unvermeidlichen Datenschutzvorbehalte überspielt und alle weiteren Überlegungen einem Gremium anvertraut, das sich eben nicht an diese Vorbehalte gebunden fühlt, um dann die Mitgliedstaaten – wie sonst auch – vor vollendete Tatsachen zu stellen.

Gewiss, anders als die EG-Kommission kann der Rat keine verbindlichen Vorgaben machen. Die Erfahrung zeigt jedoch, dass die Vorschläge des Rates von den nationalen Parlamenten in aller Regel ohne größere Diskussionen akzeptiert werden. Zudem: Rat und EG-Kommission haben inzwischen eingesehen, dass sie ihre Erwartungen am besten durchsetzen können, wenn sie gemeinsam handeln.

Sie bestehen also nicht mehr auf den jeweils eigenen Regelungsinstrumenten. Wo es deshalb um Ziele geht, die von beiden getragen werden, bekommt die Richtlinie den Vorzug. Sie gibt die gemeinsamen Vorstellungen wieder und garantiert zugleich ihre sofortige sowie gegen alle Modifikationsbestrebungen abgeschirmte Umsetzung in das nationale Recht. Die Richtlinie zur Vorratsspeicherung von Telekommunikationsdaten vom März 2006 illustriert genau diese Strategie. Viel

spricht dafür, dass sich Rat und EG-Kommission auch bei den Flugpassagierdaten auf dieses Verfahren einigen werden.

So wenig sich freilich am immer stärkeren Einfluss der Europäischen Union zweifeln lässt, so sehr gilt es, die Vorzeichen umzukehren. Dieser Einfluss sollte also genutzt werden, um ein Datenschutzkonzept zu realisieren, das die Verarbeitung personenbezogener Daten national wie supranational durchweg an der Bedeutung misst, welche ihr für die in einer demokratischen Gesellschaft unverzichtbare Partizipations- und Kommunikationsfähigkeit des Einzelnen zukommt.

Die Voraussetzungen dafür sind durchaus gegeben. Artikel 8 der Grundrechte-Charta der Europäischen Union erkennt das »Recht jeder Person auf Schutz der sie betreffenden personenbezogenen Daten« ausdrücklich an. Der Vorschlag für einen Vertrag über eine Europäische Verfassung geht noch einen Schritt weiter. Der Datenschutz wird genauso explizit zu den Grundbedingungen der demokratischen Struktur der Europäischen Union gerechnet (Titel 6, Art. 50).

Der Union fällt es offensichtlich trotzdem schwer, sich danach zu richten. So hat sich die EG-Kommission im März 2001 feierlich verpflichtet, alle geplanten Entscheidungen auf ihre Vereinbarkeit mit der Grundrechte-Charta zu prüfen, ihre im Amtsblatt jederzeit nachlesbare Erklärung aber beim Abkommen zur Übermittlung der Passagierdaten in die Vereinigten Staaten ebenso offensichtlich verdrängt wie bei der Richtlinie zur Vorratsspeicherung von Kommunikationsdaten. Das Europäische Parlament hat deshalb die EG-Kommission gleich mehrmals kritisiert. Und auch der Europäische Gerichtshof dürfte beim bereits anhängigen Verfahren über die Vorratsspeicherung nicht anders reagieren, es sei denn, er beschränkt sich, wie bei den Flugpassagierdaten, darauf, die mangelnde Kompetenz zu rügen.

Im Unterschied zur EG-Kommission fehlt es beim Rat an einer vergleichbaren Grundlage für datenschutzkonforme Ent-

scheidungen. Der Rat kann dennoch keine Sonderstellung beanspruchen. Für ihn, wie für die gesamte Europäische Union, muss uneingeschränkt gelten: Datenschutzexklaven gibt es nicht und ebenso wenig lässt sich beliebig mit dem Datenschutz umgehen. Der Geltungsbereich der Grundrechte-Charta mag beschränkt sein. Artikel 8 unterstreicht und gewährleistet ein Recht, das im nationalen Bereich durchweg anerkannt ist und sich daher selbstverständlich auf der supranationalen Ebene wiederfindet.

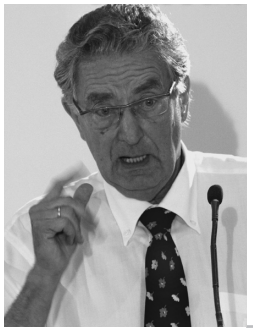
Nicht von ungefähr verknüpft die EG-Datenschutzrichtlinie von 1995 den Datenschutz in ihrem ersten Artikel sowie in den Erwägungsgründen explizit mit den Grundrechten. Den Mitgliedstaaten fällt also gerade dort, wo es, wie im Rat, auf ihre Mitwirkung ankommt, die Aufgabe zu, sich allen Versuchen zu widersetzen, den Datenschutz zu übergehen. Deutschland hat sich besonders in den Jahren 2002 und 2003 nachdrücklich dafür eingesetzt, verbindliche Datenschutzregeln für die »Dritte Säule« zu verabschieden. Erst recht gilt es, nicht nur weiter darauf zu bestehen, sondern genauso eindringlich eine datenschutzkonforme Politik für den Gesamtbereich der Union zu fordern.

d. Schließlich: Die fortwährende und immer schnellere ***Weiterentwicklung der Verarbeitungstechnologie*** muss sich auch auf den Gesetzgebungsprozess auswirken. Legislative Interventionen mögen noch so notwendig sein, sie stehen durchweg unter dem Vorbehalt des Technologiewandels und sind deshalb nicht mehr als vorläufige Reaktionen. Genau dieser Einsicht muss der Gesetzgeber ebenfalls Rechnung tragen. Der Tradition gesetzlicher Regelungen widerspricht es zwar, die Kurzlebigkeit der vorgeschlagenen Bestimmungen offen anzusprechen.

Wenn jedoch die Effizienz der Datenschutzvorkehrungen mehr als nur rhetorische Floskel sein soll, dann müssen die jeweiligen Vorschriften mit einem verbindlichen Verfallsdatum versehen werden. Norwegen ist bereits in den achtziger Jahren diesen Weg gegangen. Island hat sich wenig später ebenso verhalten. Nachahmer haben sich aber seither nicht gefunden, von wenigen, zumeist auf den Umgang mit den Telekommunikationsdaten beschränkten Ausnahmen einmal abgesehen. Die Befristung gilt immer noch als Demontage legislativer Normalität und folglich als ungewöhnliches Produkt genauso ungewöhnlicher Situationen.

Wie verfehlt eine solche Sicht ist, hat sich erst vor kurzem bei den Biowissenschaften gezeigt. Die Ausgangslage deckt sich mit den Erfahrungen beim Datenschutz. Der Gesetzgeber hat es also einmal mehr mit einer sich rasch verändernden Technologie zu tun. 2004 wurde deshalb in das novellierte französische Bioethikgesetz eine Vorschrift aufgenommen, die sich für die Forschung an Embryonen ausspricht, allerdings nur für die kommenden fünf Jahre. Die positive Reaktion gilt daher lediglich für einen beschränkten, ausdrücklich angegebenen Zeitraum. Ähnlich ist die Entscheidung in

Japan ausgefallen. Beide Gesetzgeber betrachten mithin ihre Entscheidungen als Teil einer keineswegs abgeschlossenen, vielmehr eindeutig weitergehenden Diskussion. Die primäre Verpflichtung des Gesetzgebers und damit des Parlaments ist so gesehen auch bei der Informationstechnologie nicht, eine bestimmte Regelung zu verabschieden, sondern sich konstant mit dem Technologiewandel auseinander zu setzen und die jeweils getroffenen Entscheidungen in einem offenen Diskurs zu überprüfen und gegebenenfalls zu revidieren.



GERHART R. BAUM,
Bundesinnenminister a.D., Rechtsanwalt

Die deutsche Perspektive

Meine Damen und Herren, ich bin in erster Linie ein unabhängiger Liberaler, der auch in der FDP ist.

Ich begrüße Sie, und ich habe Ihnen mit großer Aufmerksamkeit zugehört, Herr Professor Simitis. Sie erinnern mich an unser beider Vergangenheit, als wir das erste Bundesdatenschutzgesetz – nach hessischem Vorbild – auf den Weg gebracht haben. Ich habe es damals als Parlamentarischer Staatssekretär im Bundesinnenministerium betreut – eine Materie, die vielen, auch den meisten Abgeordneten, überhaupt nicht vertraut war. Man musste also werben und erklären.

Wir wollten Sie, Herrn Simitis, dann für das Amt des Bundesdatenschutzbeauftragten gewinnen. Das ist leider nicht gelungen. Sie haben aber Ihre Tätigkeit, Ihren Kampf für den Datenschutz auf andere Weise fortgesetzt und Erhebliches bewirkt. Im übrigen hat sich das Netz der Datenschutzbeauftragten sehr gut entwickelt. Ich habe gerade den 21. Tätigkeitsbericht des Bundesdatenschutzbeauftragten vor Augen; auch die Länderberichte sind von großem Interesse. Die Datenschutzbeauftragten sind inzwischen ein wichtiger und unentbehrlicher Faktor gerade auch in der Diskussion über die innere Sicherheit.

Ich freue mich, dass dies, was wir damals auf den Weg gebracht haben, institutionell gelungen ist. Nicht gelungen ist, das haben Sie eben ausgeführt, Herr Simitis, ein allgemeines Datenschutzbewusstsein zu verankern. Im Streit um die Volkszählung war dieses sehr stark entwickelt. Damals gingen mir die Befürchtungen sogar ein bisschen zu weit. Aber das Urteil des Bundesverfassungsgerichts war wunderbar: Der Datenschutz hat Verfassungsrang erhalten.

> „Datenschutz – ein Grundrecht im Kampf gegen den Überwachungsstaat.“ (GERHART R. BAUM)

Die Bevölkerung, wenn sie über dieses Thema überhaupt nachdenkt, ist längst nicht mehr so sensibel. Im Spannungsbereich Sicherheit und Datenschutz stehen wir mit dem Rücken an der Wand, wenn wir die Grundrechte verteidigen. Wir verteidigen inzwischen eine ganze Reihe von Grundrechten: Die Menschenwürde, die Unverletzbarkeit der Wohnung, die Pressefreiheit und jetzt auch das Versammlungsrecht, wenn wir die unerträglichen Beschränkungen in Heiligendamm vor Augen haben. Zuletzt mit dem inakzeptablen Einsatz eines Tornado-Flugzeugs, um ein Camp zu fotografieren, wurde die ganze Vorsorgehysterie sichtbar, die immer wieder an den Grenzen der Verfassung entlanggeschrammt ist.

In der Auseinandersetzung um die Haftdauer für RAF-Häftlinge hatten wir die auf dem Prinzip der Menschenwürde beruhende Position zu verteidigen, dass auch eine lebenslange Freiheitsstrafe die Perspektive der Freiheit enthalten muss. In Köln geht es zur Zeit im Streit um einen Moschee-Neubau um die Religionsfreiheit. Immer wieder gilt es, in schwierigen Situationen, möglicherweise auch gegen die Mehrheit der Bevölkerung – ich denke nur an den Folterfall Daschner – die Grundrechte zu verteidigen.

Wir sind in einer Situation, in der wir es sehr schwer haben, uns in den Parlamenten mit Datenschutzforderungen durchzusetzen. Wir müssen uns fragen: Woran liegt das? Was können wir ändern?

Meine Lebenserfahrung ist, dass Politiker auf Druck ihrer Wähler reagieren. Dieser Druck ist nicht da. Es wird Terrorismusangst verbreitet. Mit Recht wird gefragt: Was ist eigentlich Terrorismus? Die UNO hat mehrfach den Versuch unternommen, das zu definieren. Es ist nicht gelungen. Was geht in den Köpfen der Menschen vor? Werden sie manipuliert, um einer diffusen Terrorismusangst zu erliegen? Ich meine schon. Es wird ihnen nicht gesagt, dass wir selbst in einem totalen Überwachungsstaat die Risiken nicht ausschalten können. Es wird eine Stimmung erzeugt, die die Bevölkerung zu dem berühmten Spruch bringt: Wer nichts zu verbergen hat, hat auch nichts zu befürchten. Meine Antwort darauf ist: Was sind Sie für ein langweiliger Mensch. Aber für die Geltung von Grundrechten kann es keine Bedeutung haben, ob einzelne Bürger oder gar die Mehrheit auf sie verzichten wollen.

Rutschbahn der Angst

Also: Es besteht Angst vor dem Verbrechen, und diese hat zu immer neuen Schüben von Ausnahmegesetzen geführt. Wir sind auf einer Rutschbahn. Mit der RAF-Zeit begann es: In einer Ausnahmesituation haben wir Ausnahmegesetze gemacht. Einen Teil der Gesetze und der Fahndungsmaßnahmen haben wir revidiert, beispielsweise das Kontaktsperregesetz oder auch die Einbeziehung von Unverdächtigen in die Fahndung aufgrund von allgemeinen Merkmalen.

Dann haben wir eine weitere Phase erlebt. Sie war gekennzeichnet durch die angebliche Drohung einer organisierten Kriminalität. Ein fatales Ergebnis dieser Debatte war der Große Lauschangriff. Er hat zum Rücktritt einer FDP-Ministe-

rin geführt, die später in einer bisher nicht gekannten Weise durch das Gericht bestätigt worden ist. Das Bundesverfassungsgericht hat uns, Herrn Dr. Hirsch, Frau Leutheusser-Schnarrenberger in wesentlichen Punkten Recht gegeben. Es hat die Grenzen der staatlichen Ermittlungstätigkeit aufgezeigt.

Wenigstens das, Herr Simitis, haben wir: Wir haben eine Verfassung, die Grenzen aufzeigt. Die Grenze liegt vor allem in dem Schutz der Menschenwürde. Das Gericht hat auch in anderen Urteilen diese sehr genau bestimmt, zum Beispiel im Urteil zur Rasterfahndung. Ich erwähne noch das Luftsicherheitsgesetz, das in wesentlichen Punkten für nichtig erklärt wurde. Der Staat darf von seinen Bürgern nicht erwarten, dass sie sich für andere opfern. Leben darf nicht gegen Leben nach Kriterien von Qualität oder Quantität aufgewogen werden. Die Folge dieses Urteils war, dass einige Politiker sofort nach Umwegen gesucht haben und dazu die Konstruktion eines »Quasi-Verteidigungsfalles« ins Gespräch gebracht haben.

Das heißt also: Wir haben das Bundesverfassungsgericht, das in einer bemerkenswerten Serie von Entscheidungen dem Gesetzgeber in den Arm gefallen ist, während die Politiker immer wieder die Belastbarkeit der Verfassung erproben. So etwas hat es in der Geschichte der Bundesrepublik noch nicht gegeben: Niedersächsisches Polizeigesetz, Europäischer Haftbefehl, Zollfahndungsgesetz, Cicero-Entscheidung, Entscheidungen zu Maßnahmen gegen einzelne Anwälte, zum Beispiel zu Abhörentscheidungen von Anwaltskanzleien.

Die Reaktion der Öffentlichkeit auf diese Urteile war eher verhalten. Ich merke das dann immer, wenn ich angesprochen werde. Die Taxifahrer haben auf das Luftsicherheitsgesetz reagiert, das war darstellbar. Aber der Lauschangriff, das viel wichtigere Urteil, ist schon sehr viel schwerer darstellbar.

Diese ganze Serie von Entscheidungen ist von der Sorge geprägt, dass es in einem Präventionsstaat – und den haben

wir mittlerweile – keine Bürger mehr gibt, sondern nur potenzielle Täter. Das Volkszählungsurteil von 1983 ist erwähnt worden. Es stellte auf einen Aspekt ab, der auch heute ganz wichtig ist: In einer freiheitlichen Demokratie darf die freie Auseinandersetzung nicht behindert werden.

Die Bürger dürfen nicht in die Furcht geraten, dass ihre Kommunikation überwacht wird mit der Folge, dass sie ihre Rechte nicht mehr wahrnehmen. Dadurch, so hat das Gericht argumentiert, nimmt die Demokratie Schaden. Diese Argumente können und müssen auch herangezogen werden, wenn wir das neue Instrument der Vorratsdatenspeicherung von Telekommunikationsverbindungen beurteilen. Es ist in meinen Augen verfassungswidrig. Es muss jetzt geprüft werden, ob die Hürde zum Bundesverfassungsgericht genommen werden kann. Die Maßnahme greift so weit in die geschützte Privatheit der Bürger ein, dass ich mir nicht vorstellen kann, dass sie Bestand hat, wenn es allein um das Grundgesetz geht.

Ich komme zurück auf den Schub »Bekämpfung des organisierten Verbrechens«. In diesem Zusammenhang wurde auch monatelang über das so genannte Vermummungsverbot gestritten, mit dem ein Stück Gesinnungsstrafrecht eingeführt wurde.

Kaum war diese Phase abgeklungen, kam der nächste Schub mit der Reaktion auf den 11. September. Wieder kam es zu der bekannten Gemengelage. Die einen versprechen mehr Sicherheit, ohne Erforderlichkeit und Verfassungskonformität penibel zu prüfen. Die anderen machen es sich schwerer, wenn sie Sicherheitsbedürfnisse und Freiheit gegeneinander abwägen.

Ich meine, dieses Spannungsverhältnis muss ausgehalten werden, das müssen auch die verantwortlichen Politiker aushalten. Dieses Spannungsverhältnis muss auch den öffentlichen Diskurs prägen. Es scheint ja so zu sein, dass jetzt in der Großen Koalition dieser Diskurs wieder beginnt – nachdem Herr Schily in weiten Teilen mit der CDU/CSU einig gewesen

ist –, dass man nicht ohne weiteres das akzeptiert, was zugunsten der Sicherheit vorgeschlagen wird.

Maßlosigkeit des Sicherheitsstaates

Dann erfolgte die Reaktion auf den 11. September. Erhard Denninger hat in einem Vortrag in Frankfurt zur Sicherheitspolitik bemerkenswerte Aussagen gemacht, unter anderem die Aussage, dass zur Logik des Sicherheitsstaats seine Maßlosigkeit gehört. Er findet kein Maß, das ist so. Das ist auch meine Lebenserfahrung, denn ich war Datenschutzminister und Sicherheitsminister. Ich habe das Spannungsverhältnis in mir selber aushalten müssen.

Denninger weist darauf hin, dass in diesen Sicherheitsgesetzen, die Schily vorgelegt hat, das Wort ›Terrorismus‹ 37 Mal, das Wort ›Freiheit‹ kein einziges Mal vorkommt. Das ist bezeichnend für die Situation. Die Parteien bewegen sich in einer Kontroverse: Der eine sagt: Ich kämpfe erfolgreich gegen den Terrorismus. Du hinderst mich daran. Du bist mitverantwortlich, wenn etwas passiert. Das ist eine fatale Diskussion. Wir wissen, dass absolute Sicherheit nicht herstellbar ist. Wir haben schon damals in der RAF-Debatte bei den Gesetzen zur Bekämpfung der RAF die CDU/CSU-Opposition gegen uns gehabt und haben das bis zu einem gewissen Grad sogar ausgehalten.

Wir haben immer wieder Flagge gezeigt und im übrigen in den Wahlen, ich denke vor allem an die Bundestagswahl 1980, keinen Schaden genommen. Ich brauche das nicht im Einzelnen aufzuführen, was alles im Lauf der Jahre passiert ist: erhöhte Strafdrohung, erleichterte Verhaftung, elektronische Belauschung, anlasslose Personenkontrolle, polizeiliche Recherchen im Vorfeld über ahnungslose Kontakt- und Begleitpersonen, Rasterfahndungen – die letzte ist vom Verfassungsgericht an enge Kriterien gebunden worden –, Telefonkontrollen mit

den höchsten Steigerungsraten weltweit, Kontrollmöglichkeiten aller grenzüberschreitenden Telekommunikation, Ausdehnung der Zuständigkeit der Dienste, schleichender Abbau der Trennung zwischen Polizei und Verfassungsschutz; das Bankgeheimnis fiel; die Pässe werden mit Fingerabdrücken und biometrischen Merkmalen ausgerüstet; das Terrorismusbekämpfungsergänzungsgesetz – ein schreckliches Wort – hat vor kurzem drastisch und ohne ernsthafte Evaluierung des Vorgängergesetzes die Auskunftsrechte der Dienste erweitert und bezieht sich keineswegs nur auf den Terrorismus; gemeinsame Arbeitsdateien von Geheimdiensten und Polizei, deren Inhalt, Dauer und Zugang ohne parlamentarische Beteiligung allein von der Verwaltung bestimmt wird; die Vorratsdatenspeicherung; das Zollfahndungsgesetz und schließlich jetzt der Versuch, den privaten Computer heimlich zu erfassen. Schon die Erforderlichkeit dieser Maßnahme ist angesichts der anderen Möglichkeiten, die das Internet bietet, zu bestreiten. Ich meine: Der Grundrechtseingriff geht tiefer als im Falle des Lauschangriffs.

Das alles geschieht mit dem Ziel eine allgemeine Prävention einzuführen, da man die Täter nicht mehr kennt. Es hat ein gefährlicher Paradigmenwechsel stattgefunden: Es ist wichtiger, eine Straftat zu verhindern – und hierzu nimmt man Grundrechtsverstöße in Kauf –, als sie hinterher aufzuklären. Damit begibt man sich auf eine Rutschbahn vom gegenwärtigen Angriff über die konkrete und abstrakte Gefahr bis hin zu vagen Vermutungen. Immer mehr präventive Eingriffsbefugnisse werden geschaffen. »Die präventive Logik«, sagt Heribert Prantl »ist expansiv«, und erfügt hinzu: »Wer vorbeugen will, weiß nie genug – und so verwandelt sich der Rechtsaat in den Präventionsstaat.«

Ich erzähle überall, wo ich rede, den Bürgern: Ihr seid heute in einer Weise mit euren elektronischen Spuren im Visier des Staates, wie das noch nie in der Geschichte der Fall gewesen

ist und stoße auf Gleichgültigkeit. Diese Gleichgültigkeit macht mir zunehmend Angst.

Ich wiederhole noch einmal: Die Entwicklung ist gekennzeichnet durch eine Politik, in der Angst verbreitet wird. Zur Bekämpfung der Angst werden Vorschläge gemacht. Derjenige, der die Angst zum Thema macht, tritt gleichzeitig als Retter auf die Bühne und sagt: Ich habe das Konzept. Ihr braucht nur diese ganzen Gesetze zu beschließen, dann braucht ihr keine Angst mehr zu haben. Das sind dann zum Teil auch reine Symbolgesetze, mit denen Aktionismus vorgespiegelt wird.

Verführerische technische Entwicklung

Ich will nicht bestreiten, dass ein Teil der Maßnahmen nach dem 11. September notwendig war. Meine Kritik gilt denen, die zu weit gehen. Angst verbindet sich mit einer rasanten technischen Entwicklung, die ungemein verführerisch ist.

Es ist fantastisch, was man alles machen kann. Ich habe mich bei den TÜVs vergewissert, was das Auto heute schon elektronisch kann und künftig elektronisch kann. Es wird künftig möglich sein, jeden Meter, den wir mit dem Auto fahren, nachzuverfolgen. Am Ende des Monats bekommen wir eine Abrechnung über alle Geschwindigkeitsübertretungen, die wir gemacht haben – per Satellit.

Auch wenn die einzelne Maßnahme relativ harmlos ist, es ist die Summe der Maßnahmen, die mir Angst macht und die Dynamik, die sich entwickelt hat. Es wird mit den Fingerabdrücken angefangen. Es wird gesagt: Die brauchen wir in den Pässen, um wirklich festzustellen, ob derjenige, der den Pass vorlegt, auch identisch ist mit dem, auf den der Pass ausgestellt worden ist.

Was war die nächste Überlegung? Wir richten eine Datei ein, denn schließlich haben wir die Daten. Vorher wurde uns gesagt: Die Daten werden gelöscht, wenn der Pass ausgegeben worden ist. Was hören wir diese Woche? Für die mehr als 3 Millionen Ausländer in unserem Lande soll eine Fingerabdruckdatei eingerichtet werden. Das heißt: Eins kommt zum anderen. Bei den Mautdaten wurde uns gesagt: Sie sind für Abrechnungszwecke notwendig. Jetzt sollen sie helfen, Verbrechen aufzuklären. Hier würde ich sogar ein Stück mitgehen, wenn die Kriterien klar bestimmt sind.

Der biometrische Code im Pass wird in Kürze mit den Videokameras kombiniert werden, befürchte ich. Man wird sagen: Wir haben die Videokameras, wir haben die biometrischen Daten. Also verbinden wir beides.

Ein Problem ist die Gleichgültigkeit der Bevölkerung. Was ist da passiert? Hat das Internet die Sensibilität der Menschen verändert? Sind die Menschen heute eher bereit, gleichgültig gegenüber der Preisgabe von Daten zu sein? Hat sich die Schamgrenze gesenkt? Die Schamgrenze, die eigentlich da sein müsste, um das Private zu schützen? Immerhin flackert Widerstand auf. Zum Beispiel bei den neuen Zugriffsmöglichkeiten auf Bankkonten und jetzt bei der beabsichtigten, heimlichen Online-Überwachung.

Schily hat immer behauptet, es gäbe ein Grundrecht auf Innere Sicherheit. Das haben wir natürlich nicht. Sicherheit ist nur als Bedingung für die Möglichkeit der Freiheit zu begreifen.

Und nun stehen wir vor den neuen Vorschlägen von Schäuble. Man muss sich wirklich fragen, ob wir nicht auf dem Wege zur Rehabilitierung des Staatsrechtlers Carl Schmitt sind, der bekanntlich ein Wegbereiter des Nazi-Unrechtsstaates war. Er hat sich intensiv mit dem Phänomen des Ausnahmezustandes befasst und legitimiert die Aufhebung von wichtigen Elementen der Rechtsordnung in solchen Situationen. Er sagt: Um Recht zu schaffen, muss man nicht Recht haben. Schmitt hat dem Staat das Kriegsrecht im Inneren eingeräumt. In der Tat sind wir in unseren Diskussionen auf dem Wege zur Ein-

führung eines Feindstrafrechts zur Bekämpfung des Terrorismus. Bush hat uns das vorgemacht.

Wir sind in einer Phase der Ausnahmegesetze. Die Grundrechte stehen mit dem Rücken an der Wand. Das einzige Bollwerk ist, wie gesagt, das Bundesverfassungsgericht. Wann wacht das Parlament endlich auf? Ich hoffe, dass die SPD die Schäuble-Vorschläge kritisch bewertet und sich nicht auf faule Kompromisse einlässt. Die FDP-Fraktion, allerdings in der Opposition, hat die meisten Gesetze abgelehnt.

Ich habe hier vor meinen Augen die Begründung der Verfassungsbeschwerde, die ich mit einigen Kollegen gegen die Online-Durchsuchung im NRW-Verfassungsschutzgesetz eingelegt habe. Nach unserer Ansicht verstößt es gegen mehrere Grundrechte. Insbesondere beachtet es nicht den vom Verfassungsgericht geforderten Schutz eines Kernbereichs privater Lebensgestaltung.

Es stellt sich die Frage, wie sich andere Staaten, mit denen wir auf der Basis einer gleichen Werteordnung zusammenarbeiten, entscheiden. Denken wir an die Vorratsdatenspeicherung, so sehen wir einen Prozess der Aufweichung von Datenschutzprinzipien. Wird sich das fortsetzen? Wird die zunehmende Übertragung von Kompetenzen auf die Europäische Gemeinschaft dazu führen, dass wir unsere Standards nicht behaupten können? Standards, die geprägt sind von den bitteren Erfahrungen, die unser Land mit Diktaturen gemacht hat.

Datenschutzbericht = Horrorkatalog

Wenn ich mir den letzten Bericht des Bundesbeauftragten für den Datenschutz ansehe, so ist das ein Horrorkatalog. Wir müssen inne halten und wir brauchen dringend, im öffentlichen wie im privaten Sektor, ein neues Datenschutzrecht, das uns besser schützt. Die Vorschläge, die der Bundesbeauftragte zur Weiterentwicklung des Datenschutzrechtes macht,

finde ich sehr beachtlich. Er sagt: Ohne entsprechende Reformschritte wird die Lücke zwischen dem technologischen Fortschritt und dem Einsatz elektronischer Datenverarbeitung immer größer.

Ich komme zum Schluss: Der Berliner Journalist Christian Bommarius beschäftigt sich mit der Serie von Gesetzen zur Kriminalitätsbekämpfung in allen Bereichen der Kriminalität und kommt zu dem Schluss: »Die Angst vor dem Verbrechen ist furchtbarer als das Verbrechen und gefährlicher als der Verbrecher, denn sie lässt sich nicht festnehmen, nicht anklagen, nicht verurteilen, nicht bestrafen.«

Und an anderer Stelle fährt er fort: »Verglichen mit dem Aberglauben, dessen sich der neue Gesetzgeber bedient, waren die Abwehrriten des Volksglaubens Manifestationen der Rationalität. Der Glaube, die Gefahren der Risikogesellschaft ließen sich durch Kriminalisierung bezwingen, verrät weniger Realitätssinn als die Hoffnung, das Böse mit dem Blick zu töten.«

Recht hat der Mann!

SOPHIE IN'T VELD,
Mitglied des Europäischen Parlaments,
Ausschuss für bürgerliche Freiheiten, Justiz
und innere Angelegenheiten, Democraten 66
(Niederlande)

Die europäische Perspektive

Zunächst: Ich hoffe es nicht, und es täte mir leid, wenn Ihnen nach zwanzig Minuten die Ohren wehtun sollten, weil ich den Vortrag in schlechtem Deutsch halten muss. Ich bin Holländerin, aber ich werde es versuchen.

Es wurde schon viel gesagt und ich werde zunächst einmal einige allgemeine Bemerkungen hinzufügen und dann etwas tiefer auf das eingehen, was in Europa und besonders im Europa-Parlament geschieht.

Zunächst bin ich etwas befremdet, wenn ich sehe, dass der Staat und die Staaten auf europäischer Ebene sich darauf einigen, dass der Staat ein Recht darauf hat, alle Einzelheiten meines Privatlebens zu wissen einschließlich meines Sexuallebens. Das ist kein Scherz. Es steht jetzt in einem Richtlinienentwurf. Auf der anderen Seite gibt es immer mehr Geheimnisse über das, was der Staat macht. Ich sehe zum Beispiel nicht ein, warum der Staat alles über mein Privatleben wissen sollte, aber warum ich als Bürger kein Recht darauf habe zu wissen, ob die CIA hier in Europa tatsächlich gefoltert hat. Das ist Staatsgeheimnis. Da stimmt irgend etwas nicht.

Ich glaube, das wichtige Thema ist nicht nur Datenschutz und Privatsphäre, sondern die Qualität unserer Demokratie, das

heißt das Verhältnis zwischen Bürger und Staat. Es wurde schon gesagt, dass sich die Bürger eigentlich ziemlich wenig aufregen, dass es ihnen eigentlich ziemlich gleichgültig ist, was der Staat über sie weiß. Das kann man zum Teil so verstehen, dass die Bürger, also wir, ziemlich wenig Ahnung davon haben, was der Staat schon alles über uns und über unser Privatleben weiß. Gleichzeitig glaube ich auch, dass die Leute das Gefühl haben: Alle Einzelheiten meines Privatlebens sind sowieso schon bekannt. Das wissen die Leute. Das Verständnis, die Bedeutung von ›privacy‹ hat sich in den vergangenen zehn, fünfzehn Jahren völlig verändert.

Ich glaube, es ist wichtig, dass sich die Bürger dem Staat gegenüber wehren und auf ihren Rechten bestehen können. Das haben sie noch nicht kapiert. Ich glaube, deswegen ist es auch wichtig, dass wir so eine Debatte wie heute führen.

Es gibt immer mehr Dateien, Datenbanken. Die sind natürlich immer interessant für die Polizei, Justiz und Sicherheitsdienste. Und es sind vor allem die Politiker, die immer wieder neue Kompetenzen für Sicherheitsdienste, Polizei und Justiz fordern. Klar, die Polizei freut sich immer, wenn sie neue Kompetenzen bekommt. Aber es sind vor allem die Politiker, die nach dem 11. September immer wieder neue Kompetenzen fordern und sagen: Das brauchen wir, weil wir mehr Sicherheit brauchen. Es gibt nämlich an jeder Ecke auf der Straße Terroristen, vor denen wir uns schützen sollten. Deswegen müssen sie, die Bürger, ein bisschen Freiheit und *privacy* aufgeben, damit sie sicherer sind.

Staatliche Geheimhaltung vs. Datenpreisgabe des Einzelnen

Stimmt das auch? Bekommen wir mehr Sicherheit? Das wissen wir nicht, weil die Ergebnisse nämlich wiederum geheim sind. Da haben wir wieder das Problem: Wir sollten Freiheit und *privacy* aufgeben. Aber der Staat hat immer mehr Geheimnisse.

Als wir zum Beispiel eine Evaluierung der Ergebnisse des Programms mit Fluggastdaten gefordert haben, haben die Amerikaner gesagt – leider hat die Kommission zugestimmt: Wir können leider nicht sagen, ob das größere Sicherheit bringt. Das ist nämlich geheim. Dann hat aber der amerikanische Sicherheitsminister in den letzten Wochen, als wir uns in Brüssel getroffen haben, drei, vier ziemlich dramatische Anekdoten erzählt und gesagt: Wenn wir am 11. September diese Fluggastdaten gehabt hätten, dann hätte es keine Attentate gegeben.

Das ist Unsinn. Das stimmt nicht. Die Attentäter wurden schon über Jahre hinweg von den Behörden beobachtet; sie wussten eigentlich ganz genau, was die machen. Nur: Die Sicherheitsbehörden haben nicht zusammengearbeitet.

Immer wieder werden die Datensammlung und die Verarbeitung der Daten damit begründet, dass wir eine viel größere Sicherheit bekommen. Wenn aber kein Austausch zwischen Behörden und Ländern stattfindet, dann ergibt es überhaupt keinen Sinn.

Erstens: Bringt es mehr Sicherheit? Das wissen wir nicht, weil die Ergebnisse geheim sind.

Zweitens: Die Begründung ›Sicherheit‹ ist nur ein Teil der Wahrheit. Wenn man zum Beispiel die Ziele für die Speicherung oder die Sammlung der Fluggastdaten ansieht, dann ist das Kampf gegen Terrorismus und Kriminalität, aber auch gegen Seuchen und sonstige Risiken. Was sind sonstige Risiken? Das kann vieles sein. Ich weiß es nicht.

Auch deswegen ist es den Bürgern so egal – sie meinen, es geht nur um Sicherheit. Aber nein! Es geht nicht nur um Sicherheit.

Drittens – das ist meine Antwort: Ich glaube, unsere Kollegen aus den osteuropäischen Ländern können sich noch gut daran erinnern, wie sicher sie waren, als der Staat alle Einzelheiten des Privatlebens gewusst hat. Also: Das bringt nicht unbedingt größere Sicherheit und man muss sich auch gegen den Staat schützen können.

Es war natürlich schon immer so, dass die Behörden das Recht haben, persönliche Daten zu fordern, wenn es einen konkreten Verdacht gibt. Aber heute gibt es das Problem, dass die Daten auch für Prävention benutzt werden. Das heißt, wir haben immer mehr Profiling. Was bedeutet das? In konkreten Verdachtsfällen sollte der Staat beweisen, dass tatsächlich ein Verdacht oder auch eine Schuld vorliegt. Im Profiling funktioniert es genau anders herum: Der Verdächtige muss beweisen, dass er unschuldig ist. Da stimmt etwas nicht. Da findet eine Verschiebung statt, ohne dass dieses den Bürgern bewusst ist.

Es gibt zum Beispiel ein Google E-Mail-Programm, G-Mail. Ich habe es nicht, aber man hat es mir erklärt: Wenn man einen Bericht verschickt, wird der Text des Berichtes automatisch durchsucht und ein gewisses Profil aufgestellt. Dann wird automatisch Werbung geschickt, die mit dem Profil zusammenhängen. Das scheint sehr praktisch, für den Verbraucher ist das sehr bequem. Aber wenn wir wissen, dass diese Profile auch den Sicherheitsbehörden zur Verfügung stehen, und zwar weltweit – auch den Amerikanern, Chinesen, Russen und so weiter –, ist uns das auch noch gleichgültig? Ich glaube nicht. Dieses Profiling ist wirklich ein großes Problem.

Herr Baum hat schon darauf hingewiesen, dass es nicht nur die einzelnen Maßnahmen sind; es ist der kumulative Effekt. Es gibt wirklich eine Rund-um-die-Uhr-Überwachung. Jeder Schritt, alles, was wir machen, kann gegebenenfalls vom Staat überwacht werden. Die Frage ist: Was macht der Staat damit? Solange unsere Demokratie stark ist, ist das kein Problem. Aber der Staat könnte auch Missbrauch betreiben. Deshalb brauchen wir Mechanismen, uns gegen einen eventuellen Missbrauch zu schützen.

Was jetzt auf europäischer Ebene geschieht, macht mir große Sorgen. Das hängt auch mit der Qualität unserer Demokratie

zusammen. Ich komme immer wieder darauf zurück: Demokratie. Sehr oft wird gesagt: Daten sind keine Dateien, das ist keine Papier-Sache, keine nationale Sache. Daten sind innerhalb von wenigen Sekunden überall auf der Welt. Sie sind überall zugänglich. Also müssen wir Datenschutz, Datenaustausch, aber auch Datenverarbeitung gemeinsam auf europäischer Ebene behandeln. Das ist auch sinnvoll. Das sehe ich auch so.

Undemokratische Entscheidungen hinter verschlossenen Türen

Nur: Leider ist im Bereich Justiz und Sicherheit der Nationalstaat noch kompetent, hat die Macht. Aber es wird schon längst auf europäischer Ebene zusammengearbeitet. Nur wie? Nicht in einem demokratischen öffentlichen Verfahren, sondern hinter geschlossenen Türen. Und nicht mal im Rat, sondern in kleinen informellen Kreisen. Es gibt keine Tagesordnung. Es gibt keine Protokolle. Es werden Entscheidungen getroffen. Und wir haben keine Ahnung, was passiert.

» Es wird schon längst auf europäischer Ebene zusammengearbeitet. Nur wie? Nicht in einem demokratischen öffentlichen Verfahren, sondern hinter geschlossenen Türen. Und nicht mal im Rat, sondern in kleinen informellen Kreisen. Es gibt keine Tagesordnung. Es gibt keine Protokolle. Es werden Entscheidungen getroffen. Und wir haben keine Ahnung, was passiert. «

(SOPHIE IN'T VELD)

Zum Beispiel wurde im letzten Jahr im Juli in England ein Attentat verhindert; das hat man uns gesagt. Zwei Wochen später: Es war August, Sommer, alle waren im Urlaub, keiner hat darauf geachtet, was passiert. Da haben sich sechs Innenminister mit dem Europäischen Kommissar Franco Frattini und dem damaligen EU-Antiterrorkoordinator Gijs de Vries in England getroffen. Das Treffen wurde von den Briten organisiert, sie haben es ›de-briefing‹ genannt. Hinter geschlossenen

Türen haben sie sich über mehrere Sachen geeinigt. Wir wissen nicht genau über was. Wahrscheinlich auch auf ›ethnic profiling‹. Das heißt, dass alle Leute, die ein bisschen anders aussehen, zusätzlichen Kontrollen unterworfen werden. Man kann nun meinen, das ist eine gute oder keine gute Idee. Aber es darf doch nicht so sein, dass das auf so eine Weise entschieden wird.

Was passiert? Die Engländer wollten das unbedingt. Sie haben die anderen sechs überzeugt. Ihre Entscheidung wird dann dem Rat mit 27 Ländern vorgelegt und der Rat muss einstimmig entscheiden. Das geht natürlich nicht. Mit 27 kann man sich nie auf etwas einigen. Dann haben die sechs gesagt: Wir sollten das einfach verabschieden. Das ist eine komplizierte Sache. Wenn wir jetzt wieder die Debatte eröffnen, dann wird niemals eine Entscheidung getroffen.

Es wird tatsächlich so ein Kuhhandel nicht nur über unsere Sicherheit, sondern auch über unsere Bürgerrechte getrieben! Die meisten – nicht mal alle – Nationalparlamente haben formal irgendein Zustimmungsrecht. Das wird aber eigentlich kaum benützt. Man hat mir gesagt, dass der Bundestag über diese Sache mit Datenschutz in der Dritten Säule – ich werde darauf noch eingehen – gerade eine ganze halbe Stunde beraten hat. Aber das ist exakt jener Vorschlag, dem zu Folge alle Einzelheiten unseres Privatlebens frei ausgetauscht werden können. Das ist wirklich schlimm, was da passiert. Das holländische Parlament hat überhaupt nicht beraten! So werden unsere Bürgerrechte behandelt. Das ist wirklich ein großes Problem für die Demokratie.

Wir brauchen wirklich eine Europäische Verfassung. Leider haben meine Landsleute nein gesagt. Dieser Bereich Justiz und Sicherheit muss unbedingt europäisch werden. Das heißt nicht, dass es neue Kompetenzen, neue Bereiche auf europäischer Ebene geben wird. Es wird längst auf europäischer Ebene gemacht. Aber nicht öffentlich und nicht demokratisch. Das ist einfach nicht richtig!

Sie haben gerade von dem Verhältnis Rat und Kommission gesprochen. Ich glaube, das Parlament sollte eine wichtige Rolle spielen. Wir diskutieren diese Sache öffentlich. Alle Bürger können sehen, welche Argumente benutzt werden, wie entschieden wird. Das ist Demokratie.

Notwendigkeit einer europäischen Stimme

Es gibt noch einen zweiten Vorteil, nämlich dass wir den Vereinigten Staaten gegenüber mit einer Stimme sprechen. Die Vereinigten Staaten bestimmen eigentlich unsere Sicherheitspolitik. Sie wird nicht in Brüssel, nicht in Berlin und nicht in Den Haag bestimmt, sondern in Washington. Darüber kann man natürlich klagen: Die Amerikaner drängen uns das auf… Aber so lange es die Amerikaner machen können, werden sie es auch machen! Das würden wir wahrscheinlich auch tun. Statt zu klagen und zu nölen über die Amerikaner, sollten wir in Europa endlich mal mit einer Stimme sprechen. Dann hätten wir nämlich eine kräftige Stimme. 27 verschiedene Stimmen bringen überhaupt nichts.

Weswegen ist es so wichtig, dass wir den Vereinigten Staaten, aber auch anderen Ländern gegenüber mit einer Stimme sprechen? Weil, wie gesagt, die Daten um die ganze Welt gehen. Sie sind längst nicht mehr nur hier in Deutschland oder in Holland. Das heißt, nicht nur unsere Regierung oder unsere Behörden wissen alles über unser Privatleben, sondern auch die Amerikaner, CIA, aber auch die Russen, Chinesen. Alle! Deswegen ist es wichtig, dass transatlantisch oder mit anderen Ländern Datenschutzregelungen getroffen werden.

Es wurde gesagt, dass die Amerikaner nicht viel von *privacy* und Datenschutz halten. Stimmt nicht! Die Amerikaner sind sogar viel kritischer als wir. Was die Amerikaner mit unseren persönlichen Daten machen, das würden die selbst nie hinnehmen von ihren Behörden. Es gibt zum Beispiel eine Datei:

automated targeting system. Ich werde Sie jetzt nicht mit den Einzelheiten langweilen, aber das ist eine Riesendatei, in der *unsere* Daten gespeichert sind. Die Kommission und der Rat hatten Angst, die Bush-Regierung zu beleidigen und wollten keine Fragen stellen. Aber die Amerikaner haben gesagt: Das ist gegen unsere Datenschutzgesetze. Das heißt, jetzt vertreten die amerikanischen Parlamentarier fast unsere Interessen. Da stimmt doch etwas nicht! Wir als Europäer sollten da viel kritischer und viel selbstbewusster sein.

Die Amerikaner haben sogar sehr gute Datenschutzgesetze. Ich wünschte mir, dass wir in Europa auch solche hätten. Warum das so wichtig ist, will ich abschließend an ein paar Beispielen aufzeigen:

Der Fall ›Fluggastdaten‹ wurde schon erwähnt. Das ist Ihnen wahrscheinlich bekannt. Wenn Sie nach Amerika fliegen und einen Flug buchen, werden alle Daten den Amerikanern übergeben. Jetzt haben auch die Russen ein großes Interesse daran. Ich frage mich wirklich, ob die europäischen Bürger auch in dem Fall, wenn die Russen damit anfangen, so gleichgültig sind?

Zweiter Fall, auch bekannt: ›Swift‹. Es ist bereits seit einem Jahr bekannt, dass die Amerikaner via ›Swift‹ schon seit 2002 Zugang zu unseren Bankdaten haben. Die Amerikaner können unsere Bankkonten überwachen. Wir wissen das schon seit einem Jahr. Wir wissen auch, dass das nicht in Einklang mit unseren Gesetzen ist – es passiert trotzdem überhaupt nichts. Das heißt, hinter verschlossenen Türen wird seit Januar mit den Amerikanern verhandelt. Der Kommissionsbeamte, der die Verhandlungen führt – nicht nur für ›Swift‹, sondern auch für Fluggastdaten –, nennt das nicht ›Verhandlungen‹, sondern ›informelle Gespräche‹. Wenn es ›informelle Gespräche‹ sind, gibt es nämlich keine demokratische Kontrolle. Er braucht auch kein Mandat, das vom Rat verabschiedet wird. Er macht

das alles alleine. Er macht das übrigens toll – ein kluger, vernünftiger Mann.

Es sind zwar immer noch ›informelle Gespräche‹, aber es gibt schon einen Vertragsentwurf mit den Amerikanern. Innerhalb der nächsten zwei, drei Wochen sollte es verabschiedet werden. Es gibt überhaupt keine demokratische Kontrolle mehr! Nicht mal vom Rat! Die Kommission hat nämlich gesagt: Das ist eine rein administrative Sache. Wieso administrativ? Mein Bankkonto ist keine administrative Sache, das ist mein Privatleben.

Und was machen die Nationalparlamente?

Tatenlose Nationalparlamente

Überhaupt nichts! Die Nationalparlamente machen nichts, weil die, erstens, immer zu spät sind, die werden kaum informiert. Und am Ende des Verfahrens können die nur noch ja oder nein sagen. Wenn die nein sagen, dann sagen die anderen 26: Nun haben wir überhaupt keinen Datenschutz gegenüber den Amerikanern. Sie sind also mehr oder weniger gezwungen.

Zweitens haben die immer das Gefühl, was auch gerechtfertigt ist: Das ist eine europäische Sache. Es ist auch eine europäische Sache, denn sie wird auch von der Europäischen Kommission verhandelt. Nur: Das Europäische Parlament hat in dieser Sache keine Kompetenz. Die nationalen Parlamente haben formal schon die Kompetenz, können aber in der Praxis überhaupt nichts mehr.

Vielleicht noch ein letztes Beispiel: Datenschutz in der Dritten Säule. Wir haben die Datenschutzrichtlinie für die Erste Säule, das heißt, für alles, was den kommerziellen Bereich anbelangt. Das ist eigentlich mehr oder weniger in Ordnung. Es sollte vielleicht modernisiert werden, aber wenigstens haben wir da Datenschutz und alles ist europäisch gemacht. Das Problem ist, dass die Dateien, die für kommerzielle Zwecke geschaffen werden, jetzt auch von Polizei und Sicherheitsbehörden benutzt werden. Das ist aber die Dritte Säule: Nationaler Bereich.

Jetzt versuchen die 27, ein Datenschutzgesetz in der Dritten Säule zu schaffen. Tolle Sache. Nur: Die werden sich wahrscheinlich nicht einigen. Das ist klar. Sie versuchen das schon seit Jahren und werden sich in absehbarer Zeit nicht einigen.

Darüber hinaus ist mir aufgefallen, dass der Entwurf nicht von Datenschutzbehörden der Mitgliedsstaaten ausgearbeitet wird, sondern von Sicherheitsbehörden. Sie sollten sich den Entwurfstext einmal ansehen. Da wird klar, dass die Datenschutzbehörden ziemlich wenig damit zu tun gehabt haben. Es geht eigentlich kaum um Datenschutz und Bürgerrechte. Es geht eigentlich nur darum, wie die Sicherheitsbehörden unbegrenzt und unkontrolliert Daten austauschen können. Ich habe schon gesagt, das war kein Witz: Die gehen wirklich auf die Einzelheiten des Privatlebens bis hin zum Sexleben. Das steht wörtlich im Entwurf. Ich finde das erschreckend. Beispielsweise steht da: Alle sensiblen Daten, wie medizinische Daten, politischen Meinungen, Gewerkschaftsmitgliedschaft oder Sexleben, dürfen im Prinzip nicht ausgetauscht werden – nur wenn es notwendig ist. Was ist notwendig und wer bestimmt das? Das wissen wir nicht.

Das Parlament und alle Fraktionen sind sich einig: Das geht so nicht weiter. So können wir nicht mit Bürgerrechten umgehen. Das Europäische Parlament ist sich ziemlich einstimmig einig, dass hier etwas passieren muss. Ich hoffe auch, dass solche Debatten wie heute uns helfen, diese Gleichgültigkeit und den Informationsmangel zu überwinden, dass wir die Bürgerrechte auch auf europäischer Ebene fordern. Es geht schließlich um die Demokratie. Das war doch Ziel und Zweck der Europäischen Union. Ich danke Ihnen.

Programm der Veranstaltung vom 14. Juni 2007

10.00 Uhr **Begrüßung**
Beate Martin, Friedrich-Ebert-Stiftung, Berlin

Forum I
Datenschutz heute – Im Spannungsfeld von Freiheit und Sicherheit
Grundsatzreferat: Prämissen und Ambivalenzen einer Modernisierung
Prof. Dr. Spiros Simitis, Institut f. Arbeits- u. Wirtschaftsrecht, Universität Frankfurt
Moderation:
Dr. Johann Bizer, Unabhängiges Landeszentrum f. Datenschutz Schleswig-Holstein (ULD)

10.30 Uhr **Impulsreferate:**
Deutsche Perspektive
Gerhart R. Baum, Bundesinnenminister a.D., Rechtsanwalt
Europäische Perspektive
Sophie In't Veld, MdEP, Democraten 66, Ausschuss f. bürgerliche Freiheiten, Justiz u. innere Angelegenheiten

11.30 Uhr **Podiumsdiskussion**
Prof. Dr. Spiros Simitis, Institut f. Arbeits- u. Wirtschaftsrecht, Universität Frankfurt
Gerhart R. Baum, Bundesinnenminister a.D., Rechtsanwalt
Sophie In't Veld, MdEP, Democraten 66, Ausschuss f. bürgerliche Freiheiten, Justiz u. innere Angelegenheiten
Cornelia Rogall-Grothe, Ministerialdirektorin im Bundesministerium des Inneren

13.30 Uhr **Forum II**
Ubiquitous Computing – Auf dem Weg zum Gläsernen Bürger?
Vorstellung d. Gutachtens »Datenschutz in einem informatisierten Alltag«
Prof. Dr. Alexander Roßnagel, Institut für Wirtschaftsrecht, Universität Kassel
Perspektive der Datenschützer
Dr. Johann Bizer, Unabhängiges Landeszentrum f. Datenschutz Schleswig-Holstein (ULD)

Perspektive der Verbraucherschützer
Prof. Dr. Oliver Günther, Institut f. Wirtschaftsinformatik, Humboldt-Universität zu Berlin
Moderation:
Dr. Alexander Dix, Berliner Beauftragter f. Datenschutz u. Informationsfreiheit

14.30 Uhr **Podiumsdiskussion**
Prof. Dr. Alexander Roßnagel, Institut f. Wirtschaftsrecht, Universität Kassel
Dr. Johann Bizer, Unabhängiges Landeszentrum f. Datenschutz Schleswig-Holstein (ULD)
Prof. Dr. Oliver Günther, Institut f. Wirtschaftsinformatik, Humboldt-Universität zu Berlin
Dr. Kai Kuhlmann, BITKOM - Bundesverband Informationswirtschaft, Telekommunikation u. neue Medien e.V.
Dr. Michael Bürsch, MdB, SPD-Bundestagsfraktion

15.30 Uhr **Zusammenfassung der Konferenzergebnisse:**
Jörg Tauss, MdB, Sprecher Bildung, Forschung u. Medien d. SPD-Bundestagsfraktion

Diese Veranstaltung wurde u.a. gefördert von der Stiftung Deutsche Klassenlotterie Berlin.