Osnabrücker Jahrbuch
Frieden und Wissenschaft
16 / 2009

Neue Fragen an den Rechtsstaat

Wie begegnen Politik, Recht und Exekutive aktuellen Friedensgefährdungen?

■ OSNABRÜCKER FRIEDENSGESPRÄCHE 2008

■ MUSICA PRO PACE 2008

■ BEITRÄGE ZUR FRIEDENSFORSCHUNG

Herausgegeben vom Oberbürgermeister der
Stadt Osnabrück und dem Präsidenten der
Universität Osnabrück

V&R unipress


Osnabrücker
Friedensgespräche
UNIVERSITÄT OSNABRÜCK

Angst vorm »Überwachungsstaat«?

Podiumsveranstaltung in der Aula der Universität
am 31. März 2008

Peter Schaar	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Bonn
Dr. Dieter Wiefelspütz MdB	Innenpolitischer Sprecher der SPD-Bundestagsfraktion
Sabine Leutheusser-Schnarrenberger MdB	Rechtspolitische Sprecherin der FDP-Bundestagsfraktion, Bundesministerin der Justiz a.D.
Prof. Dr. Jens-Peter Schneider	Universität Osnabrück, Gesprächsleitung

Sabine Leutheusser-Schnarrenberger: Seit vielen Jahren, aber besonders intensiv seit dem 11. September 2001, führen wir im Deutschen Bundestag die Diskussion über das Verhältnis von Freiheit und Sicherheit im Zusammenhang mit den notwendigen, angemessenen, richtigen, politisch vertretbaren Antworten auf die aktuellen Herausforderungen. Gegenwärtig verbinden sich mit dieser Thematik vor allem die Begriffe ›Angst‹ und ›Überwachungsstaat‹.

Vor dem 11. September 2001 stand die *organisierte Kriminalität* im Mittelpunkt gerade auch gesetzgeberischer Aktivitäten, die mit dem Stichwort ›Großer Lauschangriff‹ beschrieben wurden, und seither ist es die Herausforderung des *internationalen Terrorismus* mit der Gefahr von Anschlägen auch in Europa, so wie sie in Madrid, Istanbul oder London in den vergangenen Jahren vorkamen. Dass die Politik hierbei nicht nur zusieht, ist selbstverständlich, denn Politiker müssen sich ständig der Frage stellen: Welches sind die angemessenen Antworten auf diese Herausforderungen für unseren demokratisch verfassten Rechtsstaat? Ist er wehrhaft genug? In welcher Form muss der Staat mit seinen Sicherheitsinstitutionen gestärkt werden, inwieweit braucht er mehr Eingriffsbefugnisse? Welche Rolle spielen hier die Grundrechte?

Bei den Friedensgesprächen spielen ja zwei Werte eine Rolle: Frieden und Freiheit. Welche Rolle nehmen in dieser Diskussion die Freiheitsrechte der Bürgerinnen und Bürger ein, die in unseren Grundrechten, in unserer Verfassung verankert sind? Nicht nur über die Frage einer abstrakten ›Bedrohungslage‹ ist im Bundestag immer wieder diskutiert worden, sondern auch über mögliche Antworten, die unter Berücksichtigung der Erfordernisse von Freiheit und Sicherheit gefunden werden müssen. Es gab hier genug Anlass zu Kontroversen, denn mit den gesetzgeberischen ›Sicherheitspaketen‹, die als erste Reaktion noch im Jahre 2001 verabschiedet wurden, traten drei Linien in der Auseinandersetzung und damit in der Politik hervor.

Die erste Linie: Welches Verhältnis haben die Sicherheitsbehörden untereinander, nämlich auf der einen Seite die Polizei, auf der anderen Seite Verfassungsschutzämter auf Bundes- und Länderebene, der Bundesnachrichtendienst und der Militärische Abschirmdienst? Deutlich erkennbar ist hier eine Stoßrichtung, die nicht einfach eine bessere Zusammenarbeit der Institutionen forderte, sondern darauf zielte, die Behörden beider Seiten eng miteinander zu verzahnen. Die Kritiker, die auf das *Trennungsgebot* insbesondere zwischen Polizei und den übrigen Sicherheitsbehörden verwiesen, sahen hier zu Recht Anlass zu Kritik – sowohl beim ›Sicherheitspaket I‹ als auch bei der gemeinsamen ›Anti-Terror-Datei‹, die seit 2006 auf Bundesebene eingerichtet wurde. Nur nach langen Kontroversen konnte dieses Vorhaben so ausgestaltet werden, dass es eben *nicht* eine grundlegend gemeinsame Datei von Verfassungsbehörden und Bundesnachrichtendienst auf der einen und der Polizei auf der anderen Seite gibt. Dies ist wichtig, weil es unterschiedliche Rechtsschutzmöglichkeiten, Benachrichtigungspflichten und damit Vorgehensweisen des Bürgers gegen Eingriffsbefugnisse dieser Organisationen gibt – bei der Polizei strikt rechtsstaatlich gebunden, bei den Sicherheitsbehörden aufgrund ihrer Tätigkeit in einem nur äußerst eingeschränkten Umfang. Dennoch lässt sich hier ein Politikwechsel gegenüber den Jahren vor dem 11. September 2001 konstatieren.

Die zweite Linie, die in dieser Auseinandersetzung deutlich wurde, ist in den Versuchen erkennbar, auf gesetzgeberischem Weg staatliche Eingriffsbefugnisse auf Bund- und Länderebene immer weiter ins Vorfeld möglicher Straftaten zu verlagern. Dort wurden ›Verdachtsschwellen‹ – im Hinblick auf konkrete Situationen vorhandene Anhaltspunkte für das Bevorstehen von Gefahren – abgesenkt, sowohl in Gesetzen als auch in ihrer tatsächlichen Anwendung. So entstand die Diskussion um die Frage: Wieweit darf ein Staat präventiv tätig werden, inwieweit ist sein Eingreifen noch verhältnismäßig? Denn von den entsprechenden Aktionen des Staates sind auch immer mehr unbescholtene Bürgerinnen und Bürger betroffen. Ein

›präventives‹ Vorgehen des Staates greift intensiver in Freiheitsrechte ein – das sagen alle Urteile des Bundesverfassungsgerichts der letzten Jahre –, als wenn es auf der Basis ganz konkreter Gefahr, aufgrund eines ganz konkreten Verdachtsmomentes geschieht, bei dem ganz erhebliche, schwere Straftaten zu gewärtigen sind oder bereits stattgefunden haben. Hier gab es eine Entwicklung hin zu immer weiterer Vorverlagerung des Tätigwerdens von staatlichen Institutionen. Das Bundesverfassungsgericht hat in verschiedenen Entscheidungen, die auch Nordrhein-Westfalen und Niedersachsen betrafen, dem Gesetzgeber aufgegeben, »konkrete Gefahr« als Moment in die Gesetzgebung zwingend aufzunehmen, um möglichst wenige unschuldige Bürgerinnen und Bürger in Überwachungs- und Kontrollmaßnahmen einzubeziehen.

Aktuell erleben wir, dass mit der Ausweitung digitaler Kommunikationsmöglichkeiten und einem intensivierten Kommunikationsverhalten jeder Private in ungeahntem Ausmaß ›Datenspuren‹ hinterlässt. Kaum jemand ist sich dessen bewusst. Das Bundesverfassungsgericht hat mit einer bemerkenswerten Entscheidung zur ›Online-Durchsuchung‹ das sogenannte ›Computergrundrecht‹ geschaffen, mit dem die Vertraulichkeit und Integrität der Kommunikation über informationstechnische Dienste geschützt werden soll. Daraus werden ganz konkrete Anforderungen hergeleitet.

Mit der rhetorischen Frage: »Angst vor dem Überwachungsstaat?« wird der Zweifel an der Sinnhaftigkeit dieser Maßnahmen nahegelegt: Sind die Ausdehnungen von Eingriffsbefugnissen, die mit der Einschränkung von Grund- und Freiheitsrechten verbunden sind, wirklich dringend geboten? Bringen sie wirklich das Mehr an Sicherheit, das als einzige Legitimation staatlichen Handelns bei Strafverfolgung und bei Gefahrenabwehr gelten kann? Ist das Spannungsverhältnis zwischen Freiheit und Sicherheit ausgewogen? Genau dort setzt die Kritik – nicht nur meiner Fraktion im Bundestag – an. Wir sind der Ansicht: In vielen Fällen ist dieses Spannungsverhältnis nicht richtig aufgelöst worden. Wir kritisieren eine allzu pauschale Verdächtigung von Bürgerinnen und Bürgern, allzu anlasslose, verdachtslose Möglichkeiten, Daten von Bürgern zu speichern und nutzbar zu machen. Dies ist die klassische Argumentation derjenigen, die die Freiheitsrechte argumentativ vertreten.

Viele neuere Entscheidungen des Bundesverfassungsgerichts unterstreichen, dass es einen Kernbereich privater Lebensgestaltung geben muss, der unbedingt schützenswert ist, über den es letztendlich keine behördliche Abwägung zwischen Freiheit und Sicherheit geben darf und über den nicht alle Kenntnisse auch verwertet werden dürfen.

Weil es immer strikte Bedingungen konkreter Art für Eingriffe in Freiheitsrechte geben muss und weil gerade das, was verdachtslos und anlass-

los erfolgt und damit sehr viele Menschen – uns alle vielleicht – betreffen kann, mit unserem Grundgesetz und den dort verankerten und weiterentwickelten Grundrechten nicht in Einklang zu bringen ist, hat das Bundesverfassungsgericht in vielen Fällen den Gesetzgeber aufgefordert, auf Bundes- und auf Länderebene Korrekturen vorzunehmen. Die Kritiker dürfen sich also in ihrer Kritik bestätigt fühlen. Es wäre aber sicher gut, wenn nicht das Bundesverfassungsgericht als eine Art Ersatzgesetzgeber, als Korrektiv des Gesetzgebers in Anspruch genommen werden müsste, sondern wenn die gewählten Politiker Gesetze so machen würden, dass das Verfassungsgericht hinterher gar nicht erst angerufen werden muss.

Peter Schaar: Ich möchte zunächst über diese kurzfristige, aktuelle Sichtweise hinaus- und mehr als 100 Jahre zurückgehen in die Zeit, als der Datenschutz erfunden wurde: 1890 veröffentlichten zwei amerikanische Juristen, *Samuel Warren* und *Louis D. Brandeis*, in der *Harvard Law Review* ein bahnbrechendes Werk unter dem Titel *The Right to Privacy*. Damals war gerade die Fotografie aufgekommen. Zum ersten Mal hatte man es mit Massendatenverarbeitung zu tun, damals noch auf Lochkartenbasis. Seinerzeit fand eine Volkszählung statt, die die Gemüter erregte. Das Telefon war zwar noch nicht weit verbreitet, aber in Sichtweite.

Es war ein Umfeld entstanden, in dem sich kluge Leute Gedanken machten: Was bedeuten diese Entwicklungen für die Gesellschaft und das Rechtssystem? Die Erfindung der beiden Juristen, jenes »Recht auf Privatsphäre«, war die Fortentwicklung traditioneller Lehren und gesetzlicher Vorschriften zum Thema Eigentumsschutz, zum Verhältnis von Staat und Bürger, beispielsweise im Hinblick auf den Schutz vor unrechtmäßiger Verhaftung. Die damals formulierten Ideen ließen sich zusammenfassen in einem ›Recht, alleine gelassen zu werden‹.

1983 traf das Bundesverfassungsgericht seine bahnbrechende Entscheidung über das Volkszählungsgesetz: Das Gericht erfand damit ein neues Grundrecht, das Recht auf informationelle Selbstbestimmung. Die Situation war ganz anders als 1890: Erneut wurde heiß diskutiert über die weit reichenden Auswirkungen der technologischen Entwicklung auf den Alltag. Damals wurde vielen bewusst, dass man mittels Computern sehr viele personenbezogene Daten erfassen kann. Der Begriff ›Universalcomputer‹ kursierte – und damit die Vorstellung, Daten aus unterschiedlichen Quellen zu verknüpfen. Diese Befürchtung verbreitete sich in der Öffentlichkeit. Das Bundesverfassungsgericht hatte sich damit auseinanderzusetzen, dass es in diesem Zeitalter der automatisierten Datenverarbeitung keine ›unsensiblen Daten‹ mehr gibt, dass es vielmehr immer auf den Kontext ankommt, ob Daten als sensibel oder als weniger sensibel anzusehen sind.

1983 war auch noch allen der Terrorismus der sogenannten Rote-Armee-Fraktion und der Kampf dagegen diesen Terrorismus in lebhafter Erinnerung. Viele Menschen meiner Generation sahen sich zeitweise dem ›Fahndungsblick‹ der Polizei ausgesetzt und erinnern sich noch heute daran, wie unangenehm das war. Die Befürchtung, überwacht zu werden – auch wenn sie vielleicht irreal war, hatte sie teilweise ja durchaus einen realen Hintergrund –, war vorhanden und bildete eine Quelle für die Entschiedenheit, in der diese Auseinandersetzung um die Volkszählung damals geführt wurde.

Ein zweiter, eher zufälliger Faktor, der den ›Überwachungsstaat‹ seinerzeit als eine aktuelle Bedrohung erscheinen ließ, war die Zahl »1984«. In dem gleichnamigen Roman von *George Orwell* wird vom »Großen Bruder« erzählt und davon, wie durch einen Überwachungsstaat Menschen gebrochen werden. So vermischte sich die reale Situation in der Bundesrepublik mit der Vorstellung eines alles überwachenden Staates. Das Bundesverfassungsgericht nahm den Faden auf, setzte sich mit den Sorgen vieler Menschen auseinander und kam so zu seinem Volkszählungsurteil.

Der Begriff der »informationellen Selbstbestimmung« macht deutlich, worum es dem Bundesverfassungsgericht ging, nämlich um das Recht des Einzelnen, selbst zu bestimmen, *wer* über ihn *was* weiß. Das Gericht sagte allerdings auch, dass dieses Recht nicht grenzenlos sei. Es verschloss nicht die Augen davor, dass sich der Einzelne in vielfältigen sozialen und politischen Zusammenhängen bewegt und dass daher auch der Staat einiges über das Individuum wissen muss, aber dieses in gesetzlich und verfassungsrechtlich definierten Grenzen und nicht darüber hinausgehend. Die Entscheidung des Bundesverfassungsgerichts hatte eine starke friedensstiftende Wirkung. Auch wenn es im Jahr 1987 anlässlich der nunmehr tatsächlich stattfindenden Volkszählung einzelne Proteste gab, so war die Datenschutzdiskussion doch weitestgehend aus den Schlagzeilen verschwunden. Die von vielen Volkszählungsgegnern formulierten Ängste schienen sich als unberechtigt zu erweisen. Es gab keinen ›Überwachungsstaat‹; die Volkszählungsdaten wurden nicht verwendet, um die Menschen zu unterdrücken – das wurde insgesamt so wahrgenommen, und mir ist kein einziger Fall bekannt geworden, in dem die erhobenen Daten zu repressiven Zwecken verwendet worden sind.

Bald hatten wir es mit anderen Themen zu tun: Vor allem mit dem Zusammenbruch des real existierenden Sozialismus in der DDR – übrigens auch ein Überwachungsstaat, nahezu des Typs, den George Orwell beschrieb.

Der 11. September 2001 veränderte erneut die Perspektive dramatisch – auch im Hinblick auf die Frage: Wo ist staatlichem Wissensdrang über menschliches Verhalten und Privatsphäre eine Grenze zu setzen? Das

Bundesverfassungsgericht hatte in immer kürzerer Frequenz tätig zu werden, als eine Vielzahl von Gesetzen verabschiedet wurde, die diese Grenze zu Lasten der Privatsphäre verschoben. Richtig ist, dass wir es mit einer neuartigen Bedrohung zu tun hatten. Ob diese Bedrohung größer war als jene, der sich die freiheitlichen Gesellschaften ab Ende der 1940er Jahre während der sogenannten *McCarthy-Ära* ausgesetzt sahen, oder ob sie größer war als die Bedrohung für die Freiheit in den 1960er und 1970er Jahren, sei dahingestellt. Aber es war eine neuartige Bedrohung, und eine Antwort lautete: Man will dem Staat zusätzliche Informationen zur Verfügung stellen. Das war keine singuläre deutsche Entwicklung; das haben Gesetzgeber weltweit getan. Andere Staaten sind diesen Weg zum Teil sogar wesentlich weiter gegangen, indem sie ihren Behörden deutlich weiterreichende Befugnisse einräumten als bei uns. Aber auch bei uns gibt es seither eine Reihe zusätzlicher Datenerhebungsbefugnisse, zusätzlicher Ermittlungs- und Verwendungsregelungen für personenbezogene Daten Auch die Technologie hat sich dramatisch verändert. Zur Zeit des Volkszählungsurteils hatten wir es zu tun mit einigen großen Computern, die in großen Rechenzentren standen. Das machte sie vielleicht unheimlich, aber letztlich wurden dort relativ wenige Daten gespeichert, verglichen mit dem, was derzeit geschieht. Heute leben wir im Zeitalter der allgegenwärtigen Datenverarbeitung. Stichworte wie das »Internet der Dinge« oder *»Pervasive Computing«*, d.h. die elektronische Vernetzung von Gegenständen des Alltages bzw. die alles durchdringende Datenverarbeitung, weisen darauf hin, dass wir, wo wir gehen und stehen, persönliche Daten und Informationen hinterlassen, die gesammelt werden können.


Peter Schaar

Greift der Staat auf diese Informationen zu, dann ist das eine neue Qualität, weil er sich jener Informationen bedient, die im Alltag beiläufig anfallen und die unser Leben meist sehr genau abbilden.

Wenn z.B. das Handy eingeschaltet ist, gibt es Standortmeldungen ab, die registriert werden können. Sobald telefoniert wird, werden diese Standortmeldungen zusammen mit den gewählten Rufnummern gespeichert, seit Januar 2008 für ein halbes Jahr. Surfe ich im Internet, so wird jeder Mausklick verfolgt; jede Anfrage bei einer Suchmaschine wie *Google* wird registriert, letzteres ohne staatliche Verpflichtung. Dies wird bald noch viel weiter gehen: Wir werden sehr genaue Ortungsdienste haben. Schon heute ist es möglich, auf einige hundert Meter genau den Aufenthaltsort einer Person anhand des aktiven Handys zu bestimmen. Das geschieht teilweise zu Unrecht, teilweise unter Verstoß gegen Gesetze. Auch der Staat bedient sich dieser Möglichkeiten und greift auf Informationen zu, die die Wirtschaft für eigene Zwecke verwendet oder erhoben hat. Die Möglichkeiten, unsere Wege nachvollziehbar zu machen, werden immer besser.

Die Frage ist, wo die Grenze zwischen dem, was an Datenverarbeitung für Unternehmen und staatliche Stellen erlaubt ist, und unserem Recht auf informationelle Selbstbestimmung gezogen werden soll. Hier hat das Bundesverfassungsgericht in seiner Entscheidung zur »Online-Durchsuchung« nun ein neues »Computer-Grundrecht« formuliert. Das Gericht folgt bei seiner Ableitung dieses neuen Grundrechts aus dem allgemeinen Persönlichkeitsrecht einem Ansatz, der von einem Missbrauchs-Risiko informationstechnischer Systeme ausgeht. Auf diesen Systemen, die aktuell vielleicht noch gar keine persönlichen Daten enthalten, könnten in Zukunft Daten gespeichert werden, so dass diese Systeme daher besonders zu schützen sind. Das Bundesverfassungsgericht ist hier auf der Höhe der Zeit bzw. hat seine Rechtsprechung zeitgemäß fortführt.

Daraus die notwendigen Konsequenzen zu ziehen hieße, den Wissensdrang, den Datenhunger privater Stellen zu reduzieren, aber auch den Staat zu begrenzen. Natürlich kann jede Information auf irgendeine Weise nützlich sein. Dies kann aber nicht heißen, Informationsverarbeitung als Überwachungsmaßnahme zu organisieren. Hier wieder das richtige Maß zu finden, ist die Herausforderung und sicher ein Streitthema. Ich wünsche mir, dass der Deutsche Bundestag und die Bundesregierung es eben nicht dem Bundesverfassungsgericht überlassen, die Grenze des Zulässigen zu bestimmen. Es ist Aufgabe der Politik, diese Grenzziehung vorzunehmen und die widerstreitenden Interessen richtig zu bewerten.

In den letzten Jahren ist die Sicherheit vielfach höher gewichtet worden als die Freiheit. Gerade in der Auseinandersetzung mit einem fundamentalistischen Terrorismus kommt es darauf an, Freiheit zu bewahren. Wenn wir unsere Gesellschaft – nicht nur die deutsche, das gilt auch für die USA und alle anderen Demokratien gleichermaßen – in Richtung immer weitergehender Überwachung, immer autoritärerer Sichtweisen entwickeln,

verlieren wir die moralische Rechtfertigung im Kampf gegen Terrorismus. Die Grenzziehung muss wieder stärker den Aspekt der Privatsphäre und den Schutz von Persönlichkeitsrechten beinhalten.

Jens-Peter Schneider: Was bedeutet das Recht auf Privatheit heute überhaupt noch? Der ehemalige Vorstandsvorsitzende von *SUN Microsystems* hat gesagt: »Sie haben sowieso kein Recht auf Freiheit, vergessen Sie es schlicht«. Wir sollten auch der Frage nachgehen, ob das, was Brandeis und Warren 1890 formulierten, heute noch von Belang ist oder ob wir es ›schlicht vergessen‹ können. Insofern freue ich mich auf die Worte von Herrn Wiefelspütz, der sicher auch das Spiel um die Rolle des Bundesverfassungsgerichts aufnehmen wird.

Dieter Wiefelspütz: Zunächst möchte ich feststellen: Die Bundesrepublik Deutschland ist ein außerordentlich entwickelter demokratischer Rechtsstaat, dessen Mittelpunkt die Freiheit des Bürgers ist. Es gibt weltweit keinen Rechtsstaat der Qualität, die wir seit 1949 in Deutschland aufzuweisen haben. Diese Qualität ist nicht gemindert worden, sondern im Lauf der Jahrzehnte eher gewachsen. In keinem Staat der Welt gibt es ein Gericht von der Machtfülle, dem Ansehen und der Bedeutung unseres Bundesverfassungsgerichtes. Und man müsste hinzufügen: wie die Verfassungsgerichtshöfe der Länder. In keinem Land hat der Grundrechtsschutz einen so hohen Stellenwert wie in Deutschland. Kein Land hat eine vergleichbare Norm wie den Artikel 19 Absatz 4, der gewährleistet, dass nahezu jeder staatliche Akt, bezogen auf einen Bürger, einer unabhängigen richterlichen Kontrolle unterworfen werden kann. Die Bürger unseres Landes sind selbstbewusst; sie machen davon häufig Gebrauch. Kaum ein Land leistet sich eine Verwaltungsgerichtsbarkeit, die sozusagen die Verfassungsgerichtsbarkeit der unteren Ebene darstellt. Auch das ist eine Errungenschaft, die weltweit ihresgleichen sucht.

Wir haben bei allen unterschiedlichen Auffassungen und Akzenten, die wir setzen, miteinander die Aufgabe, dass sich an dieser Qualität nichts negativ verändert, sondern dass die Qualität vielleicht sogar da und dort gesteigert wird.

Wir leben in einem sehr freien Land, und in den letzten Jahrzehnten ist die Freiheit eher noch gewachsen. Wir sind aber auch ein sehr sicheres Land. Wir haben in Deutschland eine hoch entwickelte Sicherheitsarchitektur. Unser Land ist dezentral, föderal organisiert, was im Sinne von *Checks and Balances*, der gegenseitigen Kontrolle von Verfassungsorganen zur Aufrechterhaltung eines dem Erfolg des Ganzen förderlichen Systems partieller Gleichgewichte, eine große Stärke ist. Es gibt keinen ›Sicherheitszentralismus‹ in Deutschland, der es einem Innenminister erlaubte, die

Macht alleine auszuüben und nur das zu tun und zu lassen, was er für richtig hält. Dies sind alles Errungenschaften, die nicht in Frage stehen, die im Grunde nicht strittig sind. Niemand will daran etwas ändern.

Als Innenpolitiker spreche ich jetzt womöglich zu viel über Sicherheit. Ein Innenminister ist aber nicht nur ein Sicherheitsminister, sondern auch ein Freiheitsminister. Denn den jeweiligen Innenministern von Bund und Ländern ist die Verfassung anvertraut, es ist ihre besondere Aufgabe, diese Verfassung zu schützen. Das Kennzeichen unserer Verfassung liegt in der Kurzformel: Freiheit und Menschenwürde. Wenn nun über das Spannungsverhältnis von Sicherheit und Freiheit geredet wird, so ist häufig zu hören, dass das eine doch ›die Kehrseite des anderen‹ sei. Ich halte dies für falsch, denn so wichtig Sicherheit ist: Freiheit und Menschenwürde sind im Zweifel noch wichtiger.

Sicherheitsbedürfnisse der Menschen sind keinesfalls gering zu schätzen. Auch in der Rechtsprechung des Bundesverfassungsgerichtes spielt die Sicherheit der Bürger vor Verbrechen eine große Rolle. Sicherheit hat Verfassungsrang. Aber Freiheit ist im Zweifel noch wichtiger. Ich wünschte, dass dies in unserer öffentlichen Debatte deutlicher würde, denn es kommt darauf an, welche Prioritäten man setzt. Selbstverständlich haben wir uns der Herausforderung veränderter Sicherheitslagen zu stellen: Terrorismus ist eine ›Qualität‹, auf die der Staat reagieren *muss*. Aber nicht hysterisch, wie das da und dort weltweit geschieht, sondern mit Augenmaß. Wir bekämpfen auch Terrorismus *im Rahmen des Rechtsstaates* und nicht außerhalb dessen. Aber neuen Herausforderungen im Sicherheitsbereich wird man sich stellen müssen, ebenso wie den Herausforderungen veränderter Kommunikationsbeziehungen und -technologien.

Für die Entfaltung unseres Grundrechtsstaates hat das Bundesverfassungsgericht sehr große Bedeutung. Aber unser Verfassungswesen ist nicht nur von den Gerichten, sondern auch von den Parlamenten geprägt. Viele haben ihren Anteil daran. Ich verstehe allerdings die Botschaften, die aus Karlsruhe kommen, nicht dahingehend, dass es einen *Grunddissens* zwischen dem Bundesverfassungsgericht und den Parlamenten von Bund und Ländern gäbe. Das Bundesverfassungsgericht hat nämlich *keine* entscheidenden Einwände gegen den ›Großen Lauschangriff‹, gegen die Online-Durchsuchung von Festplatten, gegen die präventive Telefonüberwachung, gegen das Scannen von Kfz-Kennzeichen vorgebracht. Es verlangt allerdings Normenklarheit, präzise Eingriffsvoraussetzungen, klare Zweckbestimmungen.

Ich verstehe die Botschaft aus Karlsruhe so: Arbeitet handwerklich präziser und genauer! Diese Mahnung ist an der einen oder anderen Stelle vielleicht auch durchaus zutreffend; sie ist aber etwas anderes als ein Grunddissens.

Der *Terrorismus* ist allerdings eine Realität in diesem Land. Es gibt eine Reihe von erfolgreich ermittelten Sachverhalten, die zeigen, dass wir einige Male mit knapper Not schrecklichsten Anschlägen entgangen sind. Wie sich die öffentliche Debatte entwickelt hätte, wenn eine jener Bomben explodiert wäre, die nur aufgrund eines technischen Fehlers nicht funktionierten, ist kaum abzusehen.

Ich bin der Auffassung, dass wir in Deutschland an der einen oder anderen Stelle *zu viel* über Terrorismus reden. Die Wahrscheinlichkeit, dass jemand Opfer eines terroristischen Anschlages in Deutschland wird, ist tausendmal geringer als die Wahrscheinlichkeit, Opfer von herkömmlicher Kriminalität zu werden. Mit dem Stichwort ›Terrorismus‹ wird inzwischen alles Mögliche begründet, was im Sicherheitsbereich in Vorbereitung ist. Augenmaß ist gefragt, um die Realität unserer Kriminalität in Deutschland richtig wahrzunehmen. Wir haben ein hohes Niveau an Freiheit und Sicherheit, aber Verbrechen gibt es eben auch in dieser Gesellschaft; dagegen muss man gewappnet sein. Es ist wichtig, die Kriminalitätswertigkeit Deutschlands realistisch zur Kenntnis zu nehmen und sie nicht zu instrumentalisieren. Das Stichwort ›Terrorismus‹ darf nicht gleichsam der Türöffner für alles Mögliche sein.

Insofern ist eine vertiefte Debatte über Freiheit und Sicherheit sehr wünschenswert. Was an Beobachtung und Überwachung im privaten Bereich in Deutschland und innerhalb von Wirtschaftsunternehmen wie etwa der Firma *Lidl* passiert, gibt Anlass zur Sorge. Es wäre doch undenkbar, dass in einer staatlichen Institution stattfindet, was bei Lidl offenbar passiert ist. Also – was passiert im privaten Bereich? Wie lange, Herr Schaar, speichert *Google*, wenn wir googeln? Wenn ich bei *amazon.de* ein Buch bestelle und zwei-, dreimal auf der Internetseite war, bekomme ich beim vierten Mal Empfehlungen, was man mir vermutlich sinnvollerweise anbieten könnte, weil man Informationen verknüpft. Das ist eine ganz simple Form der Datennutzung.

Und wie sorglos, fahrlässig und verantwortungslos gehen wir manchmal selber mit unseren privaten Daten um? Herr Schaar, haben Sie eine *Payback*-Karte oder so etwas? Bei *Aral* etwa? Wer sich auf so etwas einlässt, muss wissen, dass bestimmte persönliche Daten überall verfügbar werden. Diese Art von Leichtfertigkeit, wie wir beispielsweise im Internet selber mit Daten umgehen, mahnt uns, dass wir auch selber als Bürger unseren Teil der Verantwortung wahrnehmen müssen.

Gerade weil ich von der Qualität unseres freiheitlich-demokratischen Rechtsstaats in Deutschland überzeugt bin, macht mir die europäische Entwicklung Sorge. Der EU-Kommissar für Justiz, Freiheit und Sicherheit ist derzeit *Franco Frattini*, ein politischer Kampfgefährte von Herrn *Berlusconi*. Seine Arbeit in Brüssel überzeugt ganz und gar nicht, manches ist

sogar hochgefährlich. Man muss sich sorgen um die Erhaltung der gewohnten Grundrechtsstandards im Kontext der europäischen Entwicklung. Auch hier ist Handlungsbedarf, den man nicht aus den Augen verlieren darf, denn Freiheit ist noch ein bisschen wichtiger als Sicherheit.

Jens-Peter Schneider: Sie haben den Blick erweitert: Sorgen müssen wir uns in der Tat nicht nur wegen staatlichen Datensammelns und -speicherns machen. Wo würden Sie die ganz aktuellen, wichtigsten rechtspolitischen Debatten sehen, die wir jetzt in der Gesellschaft und an diesem Tisch diskutieren müssten?

Sabine Leutheusser-Schnarrenberger: Zu Recht ist davor gewarnt worden, die Furcht vor Terrorismus für die Verschärfung von Gesetzen, die mit der Einschränkung von Freiheitsrechten verbunden sind, zu instrumentalisieren. Umso wichtiger ist es, das Bewusstsein der Bürgerinnen und Bürger für die Vorhaben und ihre Bedeutung im Umgang mit Daten zu schärfen.


Sabine Leutheusser-Schnarrenberger

Die Entscheidung zur Online-Durchsuchung, die jetzt eine Richtschnur für den Gesetzgeber bildet, ist von großer Tragweite, denn sie wirft mehr Fragen auf als nur diejenige nach den künftigen Befugnissen des Bundeskriminalamts. Aktuell wäre auch zu fragen: Kann im Hinblick auf die Online-Durchsuchung unsere *Strafprozessordnung* unverändert bestehen bleiben? Wie darf mit jenen Daten verfahren werden, die durch Kommunikation entstehen und die ein Gesamtbild über die Art der Kommunikation ermöglichen, die ein Einzelner betreibt? Gerade die Vertraulichkeit der Kommunikation selbst, d.h. auch die Gefahr der Einschüchterung des Bürgers durch Aufzeichnen von Daten, spielte in der jüngsten Entscheidung, einer einstweiligen Anordnung des Bundesverfassungsgerichts zur Vorratsspeicherung, eine wichtige Rolle. Schon in dieser ersten, vorläu-

figen Entscheidung wird deutlich, welch hohen Stellenwert im Hinblick auf die Entfaltung der Freiheit und den Schutz der Privatsphäre des Einzelnen das Bundesverfassungsgericht diesen Daten beimisst.

Ich denke, es gibt durchaus ernstzunehmende Bestrebungen, an unserem wunderbaren demokratischen Rechtsstaat nicht alles so zu belassen, wie es ist, sondern ganz grundsätzliche Änderungen in die Debatte zu bringen. Anlass dazu boten häufig Vorschläge des Bundesinnenministers. Es fragt sich: Kann unser Rechtsstaat überhaupt mit den Herausforderungen umgehen? Können wir ihn angemessen ausgestalten, oder brauchen wir ganz andere Rechtsformen? Das sogenannte ›Feindstrafrecht‹, das in besonderen Gefahrenlagen angewandt werden soll, war ein ›Denkanstoß‹ des Innenministers. Er regte auch an, gegen mutmaßliche Terroristen in anderer, höchst bedenklicher Weise vorsorglich vorzugehen, als es unsere Gesetzeslage erlaubt.

Die aktuelle wissenschaftliche Literatur zum Verfassungsrecht und zum Staatsverständnis zeigt mir, dass Autoren wie etwa *Josef Isensee* oder *Otto Depenheuer* sehr wohl andere Vorstellungen vom Rechtsstaat haben als wir. Ich sehe jedenfalls die Lage nicht so gelassen, dass ich sage: Wunderbar, wir haben ja das Bundesverfassungsgericht. Zu fragen ist vielmehr: Wie setzt man früher schon Grenzen, sodass letztlich unser Rechtsstaat nicht deformiert und in einen Überwachungsstaat umfunktioniert wird?

Dieter Wiefelspütz: Den Roman *1984*, damals ein Zukunftsroman, las ich als Jugendlicher. Heute gibt es eine Reihe von Ansätzen dazu, dass ein Überwachungsstaat rein technisch, computergestützt, realisierbar wäre. Jeder von uns erzeugt täglich einen riesigen Datenstrom. Früher waren es einzelne Fingerabdrücke, heute sind es Daten vom Umgang an einem Bankschalter, mit einer *EC-Card*, mit dem Handy, am Computer, im Internet. Rechtsstaatlich gesehen, ist nicht die *einzelne* Eingriffsmaßnahme das Problem. Hochproblematisch ist heute das *Vernetzen* verschiedenster Daten. Die ganze Tragweite dessen haben wir noch nicht realisiert. Bald werden durch Vernetzung von Daten nicht nur Bewegungsprofile, sondern *Persönlichkeits*profile von Menschen erstellbar sein. Diese werden Dinge enthalten, die man von sich selber nie wusste oder längst vergessen hat.

Solche Profile wird es vielleicht eines nicht zu fernen Tages geben können. Heute existieren dafür die ersten Bausteine; weitere werden folgen, die es möglich machen, ein Persönlichkeitsprofil eines Menschen mit einer außerordentlich intimen Tiefe zu erstellen – über alle Facetten seines Lebens, die der Ehepartner nicht kennt, die die Kinder nicht kennen, die man sich selber vielleicht vorenthält oder deren man sich ungern bewusst ist.


Dieter Wiefelspütz

Wir werden im Bereich der Grundrechte Schranken und Hürden entwickeln müssen, die uns jetzt noch nicht genau vor Augen stehen. Darin liegen für mich wirklich dramatische Risiken. Ich sehe kein Problem darin, dass, wenn ein Verbrecher mit einem Handy telefoniert, die Strafverfolgungsbehörden mit Richtervorbehalt dieses Telefongespräch abhören, und Entsprechendes muss auch für E-Mails mit kriminellem Inhalt möglich sein. Dafür aber haben wir gegenwärtig ausreichend Rechtsgrundlagen.

Was aber passiert, wenn die verschiedensten Möglichkeiten, etwas über einen Menschen zu erfahren, vernetzt werden? Das ist die noch nicht durchdachte Gefahr, die in der Zukunft eine große Rolle spielen kann. Auch im juristischen Bereich sind wir da noch ganz am Anfang. Aber es gilt von unseren Persönlichkeitsvorstellungen, von den Werteordnungen des Grundgesetzes her: Der Staat darf die Persönlichkeit eines Menschen nicht ausleuchten. Das meint nicht nur bestimmte intime Bereiche wie Sexualität, das meint auch beispielsweise Vorlieben für Musik, für Literatur. Es gibt private Bereiche, die gehen niemanden etwas an. Wir brauchen selbstbewusste Bürger, die sagen: Bis hierher und nicht weiter.

Jens-Peter Schneider: Würden Sie die Gefahren eher bei staatlichen oder eher bei gesellschaftlichen und wirtschaftlichen Vernetzungen sehen?

Dieter Wiefelspütz: Missbrauch ist in beiden Bereichen denkbar. Ich habe Vertrauen in unsere staatlichen Einrichtungen, weil sie sehr stark kontrolliert werden. Wir haben einen Bundesdatenschutzbeauftragten, wir haben Expertise auf diesem Sektor. Solange Deutschland ein demokratischer

Rechtsstaat ist, wird dieser Staat kein Überwachungsstaat sein dürfen und sein können, weil das Grundgesetz das strikt verbietet.

Peter Schaar: Durch die Entscheidungen des Bundesverfassungsgerichts der letzten fünf Jahre ziehen sich zwei Botschaften: Zum einen wird der Kernbereich der Privatsphäre anerkannt, ein absoluter Tabubereich der privaten Lebensgestaltung, der den Staat nichts angeht. Der zweite Grundsatz ist: Es darf keine Ermittlungen ins Blaue hinein geben.

Auf die Frage, was das zentrale Problem sei, sage ich: Es ist *nicht* der gezielte Eingriff im Falle eines Verdachts. Die ›Online-Durchsuchung‹ wird heiß diskutiert, sie ist allen unheimlich. Die Wahrscheinlichkeit aber, dass eine staatliche deutsche Institution auf meinem Computer einen Trojaner platziert, um auszuleuchten, was ich mache, ist außergewöhnlich gering. Dies wäre auch der Fall, wenn das Bundesverfassungsgericht anders entschieden hätte. Aber das Stichwort ›Vorratsdatenspeicherung‹ führt zum Aspekt ›Ermittlung ins Blaue hinein‹. Hier haben wir es mit einer Vielzahl von technologischen Möglichkeiten zu tun, alltägliches Verhalten zu registrieren, z.B. die Verkehrsdaten der Telekommunikation: Wer hat wann wen angerufen? Wer hat wann im Internet gesurft? Wo hat man sich dabei gerade aufgehalten?

Aber das ist nicht das Einzige. Bei Fahrten mit dem Pkw können die Kennzeichen automatisiert erkannt werden, aus verschiedenen Gründen, etwa um Autobahn-Maut zu erheben bei Lkws oder eine City-Maut wie in Großbritannien. Staatliche Stellen greifen auf Daten zu, die Dritte erhoben haben oder verpflichten diese sogar dazu zu, Daten zu speichern, die sie für eigene Zwecke nicht benötigen. Das nennt man Vorratsdatenspeicherung für Zwecke einer möglichen späteren Strafverfolgung.

Diese generelle Vorratsdatenspeicherung, und zwar nicht nur der Telekommunikationsdaten, ist das zentrale Problem. Kfz-Kennzeichen wollen die Bundes- und die Landesinnenministerien, bei denen eine solche Maßnahme bereits durch Gesetz zugelassen wurde, nicht auf Dauer speichern. Aber ein Blick nach Großbritannien zeigt, was die nächsten Schritte sein könnten. Dort werden diese Daten fünf Jahre auf Vorrat gespeichert mit der Begründung, jemand könnte ja als Straftäter auffällig werden. Damit nicht genug: Von der Europäischen Kommission kommt das Stichwort ›Fluggastdatenspeicherung‹. Mit den USA wurde ein System vereinbart, das die Reisenden mit einer Vielzahl von Daten registriert. Die Daten werden bei USA-Reisen vorab übermittelt, bleiben dort 15 Jahre gespeichert. In Europa sollen solche Ein- und Ausreisedaten ›nur‹ für 13 Jahre gespeichert werden.

Wenn Sie in die USA einreisen, werden nicht nur Fotos gemacht, sondern auch noch Fingerabdrücke genommen. Bis vor kurzem waren es zwei

Fingerabdrücke, jetzt sind es zehn, und zwar völlig unabhängig davon, ob Sie schon einen Biometriepass haben. All diese Daten werden über viele Jahre gespeichert. Nun schlägt die Europäische Kommission vor, dass auch Reisende nach Europa entsprechend behandelt werden sollen. Und auch Aufnahmen der Iris sollen über viele Jahre auf Vorrat hinweg gespeichert werden, für die Europäer allerdings auf freiwilliger Basis.

Es ist nicht das verdächtige Verhalten, das Registrierung auslöst, nicht die besondere Gefährdungslage, etwa eine Anschlagsdrohung an einem Flughafen, wo man Daten speichert, bis die Gefahr vorbei ist. Nein: Die Tatsache, dass ich surfe, telefoniere, reise, mein Auto benutze, führt zur Registrierung und gegebenenfalls eben auch zu staatlichen Zugriffen auf solche Daten. Dazu darf es nicht kommen, sagt das Bundesverfassungsgericht. In Hinblick auf diese Vorratsdaten-Entscheidung ist in der Hauptsache ja noch nicht entschieden worden, insbesondere deshalb, weil es eine europarechtliche Vorgabe gab.

Die jetzt eingeführten Biometriepässe, die den Fingerabdruck und das Gesicht abbilden, schienen auf nationaler Ebene politisch nicht durchsetzbar. So sind die interessierten Innenminister den Weg über ›Europa‹ gegangen. Bei der Vorratsdatenspeicherung war es nicht die deutsche, sondern die britische Regierung, die im Inland nicht durchsetzen konnte, die Vorratsdatenspeicherung der Telekommunikationsdaten gesetzlich zu regeln. Auf dem Weg über ›Europa‹ hat sie sich mittlerweile doch durchgesetzt. Regierungen gehen mit manchen Vorhaben auch deshalb häufig ›über Europa‹, weil da die demokratische Kontrolle durch die Öffentlichkeit und durch starke Parlamente nicht so ausgeprägt ist wie auf nationalstaatlicher Ebene. Parlamente sind aber die Kontrolleure der Regierung. In einem parlamentarischen System wie in der Bundesrepublik, das auch die Wahl von Regierungen vorsieht, haben die Regierungsfraktionen die Mehrheit. Gleichwohl entbindet das die Parlamentarier – egal welcher Fraktion – nicht ihrer kritischen Begleitung von solchen Vorhaben. Es darf nicht sein, dass die Parlamente sich wie Prätorianergarden vor den Regierungen aufbauen.

Dieter Wiefelspütz: Das Mautdatensystem wurde als Abrechnungsgrundlage für die Inanspruchnahme unserer Autobahnen durch Lkws eingerichtet. Es ist kein Fahndungssystem und darf es auch nie werden.

Gibt es aber einen konkreten Anhaltspunkt mit Richtervorbehalt dafür, dass mittels eines Lkws auf einem Parkplatz an einer Autobahn ein schweres Verbrechen begangen worden ist, so muss die Polizei an die Daten herankommen können. Sie muss die Möglichkeit haben, zu prüfen, ob ein Ermittlungsansatz besteht, dem man nachgehen kann. Es wäre unhaltbar, dass man mit diesen Daten zwar jemanden haftbar machen kann, wenn er

die Maut nicht bezahlt, dass aber nicht mithilfe dieser Daten ermittelt werden darf, wenn er einen Mord oder ein anderes schweres Delikt begangen hat.

Ich plädiere nicht für den verdachtslosen Online-Zugriff auf diese Mautdaten. Vielmehr muss ein konkreter Verdacht bestehen, ein konkretes, schweres Verbrechen wie Raub oder ein Tötungsdelikt muss begangen worden sein. Dann muss ein Richter prüfen, ob sinnvollerweise die umliegenden Mautstellen punktuell überprüft werden.

Jens-Peter Schneider: Sie möchten die Mautdaten für bestimmte Zwecke nutzen. Wo wäre da für Sie die Grenze, um das handhabbar zu haben?

Dieter Wiefelspütz: Ich hätte gerne – und das wäre eine Novelle der Strafprozessordnung – die Möglichkeit, auf solche Mautdaten zurückzugreifen, wenn ein Verbrechen, eine schwere Straftat begangen worden ist.

Jens-Peter Schneider: Frau Leutheusser-Schnarrenberger, wäre das für Sie als liberale Rechtspolitikerin machbar?

Sabine Leutheusser-Schnarrenberger: Es ist bei den Mautdaten lange diskutiert worden, dass sie nur zu einem einzigen Zweck gespeichert werden, nämlich zur Kontrolle, ob jemand die Mautgebühr zahlt oder nicht. Deshalb werden nicht alle Mautdaten von Lkw-Fahrern erfasst, sondern – wir haben das in einer Anfrage spezifiziert und auch genau beantwortet bekommen – derzeit nur die Daten von Lkw-Fahrern, die *nicht* die Maut zahlen. Es müsste also erst einmal dieser Datenbestand umfangreicher werden, damit er im Fall eines konkreten Verdachtes bei einer schwersten Tat wie etwa Mord nutzbar wäre.

Dieter Wiefelspütz: Damit würde aus dem Mautsystem ein Ermittlungssystem, und das ist nicht in Ordnung. Ich gehe davon aus, dass das Mautdatensystem weiterhin ein Wirtschaftsberechnungssystem ist, um Gebühren zu vereinnahmen. Aber wenn ein konkretes Verbrechen begangen worden ist, halte ich es für skandalös und völlig unhaltbar, dass Daten, die einen Ermittlungsansatz bilden könnten, nicht mit Richtervorbehalt verwendet werden dürfen.

Wir haben gegenüber der Öffentlichkeit erklärt, vor unserem Mautdatensystem müsse niemand Angst haben, denn es sei unter Datenschutzgesichtspunkten garantiert unbedenklich. Das ist für mich ein Beispiel dafür, wie im Grunde mit der Öffentlichkeit nicht wirklich ehrlich und korrekt umgegangen wird.

Sabine Leutheusser-Schnarrenberger: Die Beratungen des Parlaments beim ersten Gesetz zur Telekommunikation sind genau dokumentiert. Man hat einvernehmlich begrüßt, dass gewisse Daten, die beim Telefonieren entstehen, zu Abrechnungszwecken gespeichert werden – auch damit Sie Ihre eigene Telefonrechnung überprüfen lassen und einen Einzelnachweis bekommen können. Gefährlich ist aber, dass diese gewaltige Sammlung von Telekommunikationsverbindungsdaten nun auch zu anderen Zwecken verwandt werden soll. Die strittige Frage, wie eng oder wie weit das verfassungsrechtlich überhaupt sein darf, prüft das Bundesverfassungsgericht. Die grundsätzliche Problematik ist die Begehrlichkeit auf Datenbestände, die zu ganz anderen Zwecken angelegt worden sind. Nach einer gewissen Zeit wird dann diskutiert, die Zweckbestimmung zu ändern und eine weitere Verwendungsmöglichkeit – bei Vorratsdatenspeicherung in sehr viel weiterem Umfang als ursprünglich gedacht – zu gestatten.

Peter Schaar: Schon zu Anfang der Diskussion über das Mautsystem gab es starke Bedenken von Datenschützern, dass hier unter der Hand ein Fahndungssystem entsteht. Denn nicht nur die Nichtzahler, auch jeder Zahler wird für sieben Jahre registriert. Richtig ist: Nicht jeder, der unter so einer Mautbrücke hindurchfährt, hinterlässt einen Datensatz. Gleichwohl werden schon sehr viele Daten dort registriert und für Jahre gespeichert.

Den Kritikern wurde versprochen, dass diese Daten für keinen anderen Zweck als die Gebührenerhebung verwendet werden. Auch mein Vorgänger im Amt des Bundesdatenschutzbeauftragten stellte daraufhin seine Bedenken zurück, da die Zweckbestimmung genau definiert war. Zwei spektakuläre Tötungsdelikte – ein Lastwagenfahrer soll einen Parkwächter überfahren haben, und ein Serienmörder, wahrscheinlich auch ein Lastwagenfahrer, brachte Frauen in Nordrhein-Westfalen um – führten dann zu der Forderung, die Mautdaten künftig zu Ermittlungszwecken in solchen Fällen zu nutzen. Ich gebe Herrn Wiefelspütz Recht: Diese Mautdaten sind nicht schützenswerter, sondern eigentlich eher weniger sensibel als etwa Telekommunikationsdaten.

Ich habe daraufhin gesagt: Wenn die Daten nachweislich für diesen Zweck erforderlich sind und ihre Verwendung in Fällen schweren und schwerster Straftaten begrenzt bliebe, würde ich mich einer solchen Gesetzesänderung nicht entgegenstellen, trotz genereller Bedenken gegen ein Aufweichen von Zweckbindungsregelungen.

Man muss vor der Einführung eines jeden neuen Systems dieser Art fragen: Wie wird die Verwendung der Daten begrenzt? Auch bei der Steueridentifikationsnummer gibt es die gebetsmühlenartige Zusicherung einer strikten Zweckbindung. Es komme keineswegs ein allgemeines Personen-

kennzeichen. Aber in Italien beispielsweise gibt es bereits eine Steuernummer, die als allgemeines Personenkennzeichen gilt. Das heißt: Es geht nicht allein um die reine Zweckbindung, sondern auch um die Technik, nämlich um die Frage: Wie sind technische Systeme zu gestalten, dass diese Daten eben nicht so lückenlos entstehen, dass sie möglichst frühzeitig gelöscht werden, dass bestimmte datenschutzfreundliche Techniken zum Einsatz kommen?

Jens-Peter Schneider: Es geht demnach um die Frage: Welche Datenbestände wollen wir überhaupt schaffen? Und wenn man diese Entscheidung gefällt hat, ist der weitere Weg nach Ihrer Darstellung ziemlich klar: Zuerst öffnet man nur ein kleines Tor, und irgendwann lässt sich dieses Tor nicht mehr kontrollieren.

Jens-Peter Schneider

Dieter Wiefelspütz: Das ist ein großes Problem, wie ich freimütig einräume: Es gibt bei unseren Sicherheitsbehörden – womöglich als eine beruflich bedingte Eigenschaft – einen unersättlichen, im Prinzip unbegrenzten Datenhunger. Das sage ich bei allem Respekt vor der Seriosität der Leute, die dort arbeiten. Manche Fachleute, auch Politiker, sind in ihrem Ringen um Problemlösungen zunächst zufrieden, wenn sie einmal den Einstieg, den Fuß in der Tür haben. Wenn dann Jahre später, in denen sich alle daran gewöhnt haben, die Sache erneut auf die Tagesordnung kommt, weil ein spektakulärer Bezugsfall passiert ist, der die Empörung breiter Schichten der Bevölkerung hervorruft, dann geht man ein gutes Stück weiter. Mit dieser Dialektik muss man sich auseinandersetzen; dagegen gibt es keine Patentlösung. Man muss immer wieder konkret ringen um das, was man glaubt verantworten zu können und was nicht.

Sicherheit, nicht nur im sozialen Bereich, auch im Bereich von Schutz vor Verbrechen hat bei vielen einen manchmal überragend hohen Stellenwert. Wer aber wirklich versucht, einen totalen Schutz der Bürger zu

organisieren, schafft totalitäre Verhältnisse. Wir haben letztlich die Politik, die Parlamentarier, die wir verdienen. Es ist unser aller Verantwortung, und ich wünschte mir sehr, dass wir an der einen oder anderen Stelle Freiheit intensiver diskutieren, auch mit den Risiken, denn wer Freiheit als wichtiger empfindet als Sicherheit, muss sich darüber im Klaren sein, dass man sich nicht vor jedem Risiko schützen kann.

Publikum: Die Datenfülle, die wir bekommen, schreitet fort mit der ganzen Computerisierung. Ist das überhaupt in Zukunft alles noch kontrollierbar? Nützt unsere Diskussion überhaupt etwas?

Peter Schaar: Ja, ich glaube, die Diskussion nützt etwas, weil es darum geht, über Lösungen zu sprechen und zu fragen: Gibt es Möglichkeiten, nicht nur für den Gesetzgeber, sondern auch für diejenigen, die die Technik entwickeln, Möglichkeiten, die den Einzelnen bereitgestellt werden können?

Es geht auch darum, sich selbst bewusst zu werden, was man im Internet öffentlich macht. Wo hinterlässt man welche Daten? Das fängt schon in früher Jugend an, wo sich die Frage stellt, was ich preisgebe und was nicht. Wichtig ist, dass der Staat die Menschen dabei unterstützt, ihre Privatsphäre zu wahren und als ein Schutzgut zu betrachten, dass er darauf hinwirkt, dass auch die Wirtschaft nicht unermesslich viele Daten sammelt und menschenunwürdige Überwachungen durchführt. Die Diskussion nützt etwas, aber letztlich nur dann, wenn sie bei den Entscheidungsträgern zu bestimmten Schlussfolgerungen führt. Ich habe das Gefühl, dass wir uns hier ziemlich einig sind, dass das aber, wenn es um Mehrheiten geht, zum Beispiel im Deutschen Bundestag, nicht ganz so eindeutig ist.

Dieter Wiefelspütz: Ich habe den Eindruck, dass unsere technische Entwicklung in den verschiedensten Bereichen, auch im kommunikationstechnischen Bereich, schneller vonstatten geht, als wir zu moralisch-ethischen Verstandesurteilen kommen können. Ein Beispiel: Wir haben die Nutzung der Atomenergie betrieben und überhaupt nicht begriffen, was damit an Sicherheitsanforderungen verbunden ist. Ein anderes Beispiel: Ich gehe inzwischen täglich mit dem Internet um und nutze diesen wunderbaren, neuen Raum der Freiheit. Manche Leute werden sogar süchtig im Umgang mit diesem neuen Instrument. Es ist sehr schnell, sehr preiswert, für Information, Kommunikation, Austausch hervorragend geeignet, genial. Aber diskutieren wir die Risiken, die sich damit verbinden? Wo sind die Leitplanken? Freiheit ist ganz wichtig, aber es gibt ja irgendwo auch Grenzen.

Wir wissen, dass das Internet eben nicht nur ein Raum der Freiheit ist, sondern auch ein Raum, in dem praktisch jede Untat dieser Welt denkbar

ist. Und um das zu verhindern, um einen *fairen* Raum der Freiheit zu schaffen, hätte ich schon gerne ein paar Verkehrsregeln. Da das alles international ist, ist es unendlich schwer, diese überall durchzusetzen. So diskutieren wir gerade, wie man *Google* und *YouTube*, diese wunderbaren Plattformen, daran hindern kann, zugleich schlimmste Menschheitsverbrechen wie etwa Rassismus und Antisemitismus zu ermöglichen. Es ist schwer, die Verantwortlichen zur Rechenschaft zu ziehen: Wen verklagt man da eigentlich? Wen kann man wo anzeigen?

Da hat eine Entwicklung abgehoben, da läuft etwas, das wir nutzen, ohne moralisch, ethisch, rechtlich, verfassungsrechtlich, national und international auf der Höhe des Problems zu sein. Dies scheint mir im Übrigen nicht nur ein Problem des Internets zu sein, sondern ein sehr grundlegendes Dilemma unserer technischen Zivilisation, die sich an manchen Stellen schneller entwickelt, als wir es im Geist tun; das ist ein Wettlauf. Bei manchen Themen scheint mir der Abstand zwischen den Leuten, die die modernsten Kommunikationstechnologien aus kriminellen Gründen nutzen, und unseren Sicherheitsbehörden eher größer geworden zu sein. Das gilt nicht für die große Masse der Menschen, die völlig friedlich und gesetzestreu leben. Wer sich aber *Hightech* zunutze machen will, um ganz bösartige Dinge zu tun, hat es heute leichter. Auch das ist ein Wettlauf, eine Dialektik.

Sabine Leutheusser-Schnarrenberger: Dieser Punkt wurde in der mündlichen Verhandlung des Bundesverfassungsgerichts zur Online-Durchsuchung angesprochen. Daran nahmen Experten teil, die genau wissen, was man im Internet machen kann, wie man sich selbst schützen kann. Sie kamen aus verschiedensten Bereichen, vom *Chaos Computer Club* bis hin zu Universitäten. Im Hinblick auf die Effektivität der Online-Durchsuchung wurde einhellig die These vertreten, dass jeder, der es will, seine digitale Kommunikation durch *Verschlüsselung* so schützen kann, dass sie auch mit dem größten Aufwand nicht zu entschlüsseln ist. Auch unter diesem Aspekt muss man die Frage der Sinnhaftigkeit einer Regelung der Online-Durchsuchung diskutieren, denn diese macht womöglich nur den ›digitalen Eierdieb‹ dingfest, während all diejenigen, die die digitale Kommunikationstechnik notorisch und mit hoher krimineller Energie nutzen, nicht überführt werden können.

Dort, wo die Entscheidungen über die Nutzung verfügbarer Daten noch nicht gefallen sind, müssen wir künftig eher ansetzen. Beispielhaft ist hier die »Elektronische Gesundheitskarte« zu nennen. So sehr sie Vorteile für manche Einrichtungen bringt – sie speichert Daten, die dem Arzt schnell über die gesundheitliche Befindlichkeit seiner Patienten Auskunft geben –, so sicher ist damit zu rechnen, dass es nur kurze Zeit dauern wird, bis es

nicht mehr freiwillig ist, welche Daten auf der Karte gespeichert sind, obwohl ja die Freiwilligkeit, mit der die Patienten in die Datenspeicherung einwilligen oder ihr widersprechen, Grundvoraussetzung für die Akzeptanz dieser Karte ist. Wenn diese Karte erst eainmal da ist, werden die Begehrlichkeiten für diese Datenbestände wachsen, und zwar nicht in erster Linie seitens der staatlichen Institutionen, sondern seitens der Arbeitgeber, Versicherungen, Banken und allen, die sich Prognosen hinsichtlich der Lebenserwartungen von Menschen davon versprechen. Deshalb lehne ich diese Gesundheitskarte ab. Das ist meine Entscheidung zu Beginn eines Projektes, das viele Fragen zum Umgang mit entstehenden, höchstpersönlichen Daten nach sich ziehen wird, denn ich habe eine genaue Vorstellung davon, welche Debatten danach innerhalb kürzester Zeit entstehen und wofür sich im Zweifel Mehrheiten finden lassen.