

Terrorismusbekämpfung: Steht der Datenschutz im Weg?

Vortrag von

Sabine Leutheusser-Schnarrenberger, MdB

Anlässlich der Tagung

„Vom Volkszählungsurteil zum virtuellen Exhibitionismus - Wertewandel des Datenschutzes“

der Akademie für politische Bildung Tutzing
am 26. bis 28. September 2008 in Tutzing

Anrede,

ich freue mich, kurz vor der morgigen wichtigen demokratischen Weichenstellung für Bayern hier in Tutzing zu sein.

Das Thema meines Vortrages ist: „Terrorismusbekämpfung: Steht der Datenschutz im Weg“?

Manch einer wird sich vielleicht gewundert haben, warum ich gerade diese Fragestellung gewählt habe, ist doch der Datenschutz ganz oben auf der politischen Agenda angekommen. Vereinzelt wird sogar von der Renaissance des Datenschutzes gesprochen.

Kein Zweifel: Die Bedeutung des Schutzes der Privatsphäre, der Vertraulichkeit der Kommunikation und des informationellen Selbstbestimmungsrechts werden von immer mehr Menschen geschätzt.

Nach biometrischen Merkmalen in Reisepässen und künftig auch in Personalausweisen, nach immer intensiverem Zugriff auf die Kontendaten der Bürgerinnen und Bürger, nach immer weiteren Befugnissen für Bundesnachrichtendienst, Verfassungsschutzbehörden, militärischem Abschirmdienst mit Zugriff auf umfangreiche private Datenbestände, nach einem ständigen Anstieg der Telefonabhörmaßnahmen und schließlich nach Vorratsdatenspeicherung und Online-Durchsuchung ist es kein Wunder, dass die Angst vor dem gläsernen Bürger zunimmt und der gesellschaftliche Widerstand wächst.

Diese Sorgen werden nicht immer ernst genommen. Einige von Ihnen werden vielleicht den Beitrag des Münchener Polizeipräsidenten in der Süddeutschen Zeitung vergangenen Mittwoch gelesen haben, in dem er behauptet: Ich zitiere: „Mehr Datenschutz bedeutet keineswegs immer mehr Freiheit, sondern manchmal auch mehr Täter und damit auch mehr unschuldige Opfer.“ Und dann fragt: „Ist uns der Datenschutz dies wert?“ (Zitat Ende).

Genau mit diesen Fragen möchte ich mich in meinem Vortrag beschäftigen.

Dazu werde ich in einem ersten Schritt die Entwicklung des Datenschutzes in Deutschland aus rechtlicher Sicht skizzieren, um die Bedeutung des Datenschutzes für den Rechtsstaat einzuordnen. In dem darauffolgenden Abschnitt werde ich die Terrorismusbekämpfung seit dem 11. September einer kritischen rechtsstaatlichen

Prüfung unterziehen. Abschließend werde ich hoffentlich genug kontroverse Antworten präsentieren, die genügend Raum für Diskussionen lassen.

Lassen Sie mich zunächst auf die Genese des Datenschutzes eingehen.

Bereits 1970 hat Hessen als erstes Bundesland ein eigenes Datenschutzgesetz erlassen, ab 1978 gab es dann mit dem Bundesdatenschutzgesetz auch eine gesetzliche Regelung auf Bundesebene.

1983 hat das Bundesverfassungsgericht bekanntlich mit dem Volkszählungsurteil die verfassungsrechtlichen Grundlagen des Datenschutzes geschaffen. Mit der Schaffung des, aus dem allgemeinen Persönlichkeitsrecht abgeleiteten, informationellen Selbstbestimmungsrechts, verankerte das Gericht den Datenschutz als Grundrecht in der Verfassung. Fortan sollte die Befugnis des Einzelnen gewährleistet werden, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

Datenschutz ist aber viel mehr als ein bloßer Abwehranspruch gegen Datenerhebung und –verwendung. Es ist der auf Informationstechnologie angewandte Schutz der Menschenwürde und des Persönlichkeitsrechts. Als solcher dient der Datenschutz auch dem Schutz der Intimsphäre des Einzelnen vor der Erhebung höchstpersönlicher Daten, auf deren konkrete Auswertung und Weitergabe der Bürger im Einzelfall kaum Einfluss hat. Denn die Erhebung von – getrennt betrachtet – unerheblichen Daten kann durch deren Kombinierung und Bündelung in einem Profil zur Preisgabe von intimen Angaben über das Privatleben des Betroffenen führen.

Darüber hinaus kann der Datenschutz aber auch betrachtet werden als Schutz des sozialen Wert- und Achtungsanspruchs des Einzelnen vor Vergegenständlichung durch eine datentechnische Katalogisierung seiner Persönlichkeit.

Schon 1969 führte das Bundesverfassungsgericht im Mikrozensus-Urteil dazu aus: „Es widerspricht der menschlichen Würde, den Menschen zum bloßen Objekt im Staat zu machen. Mit der Menschenwürde wäre es nicht zu vereinbaren, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist.“ (Zitat Ende)

Allerdings hat sich seit dem Volkszählungsurteil 1983 das Datenumfeld durch die Informationsgesellschaft gravierend verändert. Damals füllten Computer noch ganze Räume und beim Einkaufen wurden noch Rabattmarken statt Kredit- oder Kundenkarten benutzt. Heutzutage werden Kunden-, Täter-, Bewegungs- und Gesundheitsprofile erstellt, die durch Verknüpfung ein genaues Persönlichkeitsprofil ergeben können.

Außerdem musste bei der Volkszählung der Staat noch an die Tür der Bürger klopfen und die Daten erfragen, während heute Daten in damals unvorstellbarem Ausmaß versteckt erhoben werden, wovon der Bürger in der Regel nichts erfährt.

Stetige Aktualisierungen und Anpassungen des einfachgesetzlichen Datenschutzes waren und werden daher immer nötig sein, um ein gleichbleibendes Schutzniveau bei weiterem informationstechnischen Fortschritt zu gewährleisten.

Daher ist es nur konsequent, dass das Bundesverfassungsgericht den grundrechtlich gebotenen Schutz der Privatsphäre (im Urteil zum Verfassungsschutzgesetz Nordrhein-Westfalen) durch die Schaffung des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aufgewertet und angepasst hat. In Anbetracht der neuen technischen Möglichkeiten der Ermittlungsbehörden war dies datenschutzrechtlich geboten.

So begrüßenswert dieses Urteil für die datenschutzrechtliche (Grundrechts-) Dogmatik auch ist, in der Praxis geht der Trend eher in die gegenteilige Richtung:

Im Jahr 2006 war Deutschland noch Spitzenreiter der internationalen Vergleichstudie zum Datenschutz, die von der renommierten Menschenrechtsorganisation „Privacy International“ erstellt wurde. Dies ging vor allem zurück auf die verfassungsrechtlich verbrieft Rolle des Datenschutzes in Deutschland und auf das dichte Netz von Datenschutzbehörden, das zum Teil der föderalistischen Struktur der Bundesrepublik zu verdanken ist.

Die aktuelle Studie kommt zu einem anderen Ergebnis. Deutschland ist innerhalb eines Jahres ins Mittelfeld abgerutscht. Der Status der datenschutzrechtlichen Veränderung zum Vorjahr wird als „decaying“ bezeichnet, die schlechtmöglichste Kategorie, die soviel bedeutet wie ‚zerfallend‘ oder ‚zugrunde gehend‘. Diese Verschlechterung geht laut der Studie vor allem darauf zurück, dass Deutschland europaweit mit die höchste Abhör- und Überwachungsrate aufweist. Diese Entwicklung wird sich in Anbetracht der neu gefassten Eingriffsbefugnisse wie der Onlinedurchsuchung in Zukunft wohl noch verstärken. Besonders negativ hat sich auch der Beschluss ausgewirkt, biometrische Daten in Ausweisdokumenten einzuführen. Die Folgen dieser Maßnahme sind, insbesondere in Anbetracht der weiter fortschreitenden Vernetzung der Datenbanken, noch nicht abzuschätzen.

Gerade bei der Einführung von biometrischen Merkmalen in Ausweisen wurden die Begründungsfiguren immer wieder gewechselt. Einmal hieß es, Ausweisdokumente sollten fälschungssicherer werden. Dann hieß es, biometrische Merkmale seien auch ein unverzichtbares Mittel in der Terrorismusbekämpfung.

Lassen Sie mich das unmissverständlich deutlich sagen: Letzteres ist ein Argument, das wir seit dem 11. September 2001 immer und immer wieder hören.

Seit den Anschlägen vom 11. September ist die Gefahr des Terrorismus in den Mittelpunkt der staatlichen Sicherheitspolitik gerückt. Eine Vielzahl von Gesetzen wurde national und international erlassen, die unmittelbar der Bekämpfung des Terrorismus dienen sollen.

Als unmittelbare Reaktion auf den 11. September wurden eine ganze Reihe von neuen Sicherheitsgesetzen erlassen. Schnell sollte es der damaligen Bundesregierung Schröder damals gehen. Den Startschuss gab das Anfang Januar 2002 verabschiedete Terrorismusbekämpfungsgesetz (TBG – Schily 2). Vorläufiger Höhepunkt war dessen Erweiterung, das Terrorismusbekämpfungsergänzungsgesetz (TBEG) von 2007. Diese beiden Gesetzespakete sahen Änderungen in mehr als 15

Fachgesetzen vor: vom Bundesverfassungsschutz-, MAD-, BND-, BKA- und Bundespolizeigesetz; über das Pass-, Vereins- und Artikel 10-Gesetz; bis zum Straßenverkehrsgesetz und dem ominösen Luftsicherheitsgesetz. Ziel dieser Änderungen war die Schaffung einer „neuen Sicherheitsarchitektur“. Geheim- und Nachrichtendienste wurden besser vernetzt, neue Behörden - wie das Gemeinsame Terrorabwehrzentrum - wurden geschaffen, neue Straftatbestände wurden eingeführt, neue Datenbanken errichtet.

Geplante Gesetzesinitiativen und Befugnisse wie das neue BKA-Gesetz oder die Onlinedurchsuchung und der polizeiliche Zugriff auf Melderegister zeigen, dass der Bau der „neuen Sicherheitsarchitektur“ noch lange nicht abgeschlossen ist.

Das Kernelement der Gesetzesinitiativen zur Bekämpfung des Terrorismus ist die Erweiterung der Kompetenzen der verschiedenen Sicherheitsbehörden. Dies kann durch die Befugnis zu weitreichenden Abhör- und Überwachungsmaßnahmen erfolgen oder durch Zugriff auf personenbezogene Daten.

Ein anderes Wesensmerkmal der Gesetze zur Terrorismusbekämpfung ist eine immer weiter ins Vorfeld verlagerte Eingriffsbefugnis. Der Staat soll möglichst früh einschreiten dürfen, um die Gefahr abzuwenden. Das führt dann zu Beobachtung, Kontrolle und Überwachung von Personen, die zwar noch nichts Gesetzwidriges getan haben, denen die Sicherheitsbehörden aber wegen bestimmter Persönlichkeitsmerkmale einen Verstoß zutrauen. Dieses präventionsstaatliche Konzept bedeutet aber auch die Strafbarkeit von Absichten und Ermittlungsmethoden, die sich an der Effektivität orientieren - statt an der Unschuldsvermutung.

Die Verfassungsmäßigkeit dieser Maßnahmen zur Bekämpfung des Terrorismus wird zu Recht beanstandet. Fast alle diese Maßnahmen berühren Fragen des Datenschutzes und treffen die Abwägung zwischen Freiheitsrechten und den Sicherheitsbelangen zu Gunsten der Sicherheit. Das Ergebnis ist der – im Titel meines Vortrags angedeutete – Antagonismus zwischen dem Datenschutz und anderen Freiheitsrechten sowie der Terrorismusbekämpfung.

Dazu hätte es aber nicht kommen müssen.

Dass es überhaupt zu der Frage kommt, ob der Datenschutz der Terrorismusbekämpfung im Weg steht, ist eher auf ein einseitiges und verzerrtes Verfassungs- und Grundrechtsverständnis zurückzuführen.

Die Verfassung wird von manch einem Sicherheitsapologeten als Gefängnis betrachtet, aus dem sich die Exekutive befreien muss, um endlich uneingeschränkt effektiv Gesetze erlassen zu können.

Ein Blick in den Koalitionsvertrag der Bundesregierung Merkel belegt, wie weit dieses Denken verbreitet ist. Ich zitiere aus Seite 135 des Koalitionsvertrages von Union und SPD:

„Die Sicherheitsbehörden in Deutschland sind gut aufgestellt. Wir werden jedoch die im Grundsatz bewährte Sicherheitsarchitektur wo es nötig ist weiterentwickeln und überprüfen, inwieweit rechtliche Regelungen, etwa des Datenschutzes, einer

effektiven Bekämpfung des Terrorismus und der Kriminalität entgegenstehen.“ (Zitat Ende)

Diese Formulierung impliziert, dass Grundrechte - wie das informationelle Selbstbestimmungsrecht - von vornherein als lästige Einschränkungen des Regierungshandelns verstanden werden und nicht als Errungenschaften des modernen Rechtsstaates, die es auch in Zeiten terroristischer Bedrohung zu erhalten gilt.

Anrede,

nach § 26 der Geschäftsordnung der Bundesregierung ist es die ausdrückliche Aufgabe von Bundesjustizministerium und Bundesinnenministerium, alle von der Regierung in den Deutschen Bundestag einzubringenden Gesetzesentwürfe auf deren Übereinstimmung mit dem Grundgesetz zu prüfen.

Statt diesem früher einmal als ehren- und anspruchsvoll begriffenen Auftrag nachzukommen, erleben wir aber, dass selbst diejenigen Gesetzesvorhaben, die nicht von irgendeinem Fachministerium, sondern federführend vom Justiz- oder Innenministerium selbst erarbeitet wurden, immer häufiger gravierende verfassungsrechtliche Mängel aufweisen.

Reihenweise werden sie vom Bundesverfassungsgericht ganz oder in ihren wesentlichen Teilen für verfassungswidrig und nichtig erklärt.

Die in der Rechtsgeschichte der Bundesrepublik beispiellose Serie von Blamagen der Politik der inneren Sicherheit begann im März 2004 mit der Verfassungsgerichtsentscheidung zur akustischen Wohnraumüberwachung, zum Großen Lauschangriff.

Sie werden sich erinnern: Damals entschied das höchste deutsche Gericht, dass wesentliche Teile des Gesetzes zur Einführung der akustischen Wohnraumüberwachung mit dem Grundgesetz nicht vereinbar sind.

Das Gericht stellte fest, und darin kommen der Kern und die hohe Bedeutung dieses Gerichtsurteils zum Ausdruck, dass es einen sogenannten „Kernbereich der privaten Lebensgestaltung“ gibt, in den der Staat, wegen der Unantastbarkeit der Menschenwürde gemäß Art. 1 Abs. 1 GG grundsätzlich nicht, also selbst dann nicht eingreifen darf, wenn er mit seinem Eingriff höchststrangige Rechtsgüter zu schützen beabsichtigt.

Eine gegenseitige Abwägung der Rechtsgüter ist nicht statthaft.

Ein rechtswidriger Eingriff in den Kernbereich der privaten Lebensgestaltung liegt, so das Verfassungsgericht, nicht erst dann vor, wenn die Inhalte der heimlich belauschten kernbereichsrelevanten Gespräche gegen den Verdächtigen verwendet werden, sondern schon dann, wenn solche Gespräche heimlich belauscht werden.

Gespräche, die dem Kernbereich privater Lebensgestaltung zugerechnet werden müssen, unterliegen also nicht nur einem Verwertungs-, sondern einem strikten Erhebungsverbot.

Jedermann sollte anerkennen, dass das Urteil des Bundesverfassungsgerichts zum großen Lauschangriff, dem Staat erhebliche Schranken auch für andere staatliche Überwachungsmaßnahmen, wie etwa für die Telefonüberwachung, setzt. Im April 2006, musste die Politik der inneren Sicherheit eine weitere Niederlage vor dem Bundesverfassungsgericht hinnehmen.

Und zwar erklärte das Gericht am exemplarischen Fall Nordrhein-Westfalens die in der Folge der Terroranschläge von New York und Washington von einigen Landesregierungen vor allem an den Universitäten durchgeführten verdachtslosen Rasterfahndungen für nicht mit dem Grundgesetz vereinbar.

Eine präventive polizeiliche Rasterfahndung, so urteilte das Bundesverfassungsgericht, ist dann rechtswidrig und verstößt dann gegen das Grundrecht auf informationelle Selbstbestimmung, wenn nicht zumindest eine konkrete Gefahr für hochrangige Rechtsgüter wie den Bestand des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person gegeben ist.

So jedenfalls, wie sie in Nordrhein-Westfalen und anderen Bundesländern angeordnet und durchgeführt worden war, nämlich als verdachtslose Vorfeldmaßnahme, die erst der Verdachtsschöpfung dienen sollte, ist eine Rasterfahndung mit den vom Grundgesetz aufgestellten Anforderung unvereinbar, also rechtswidrig.

Am 27. Februar 2008 hatte das BVerfG über die Vorschriften zur Online-Durchsuchung des nordrhein-westfälischen Verfassungsschutzgesetzes zu entscheiden.

Anlässlich mehrerer Verfassungsbeschwerden gegen dieses Gesetz äußerte es sich in einer Grundlagenentscheidung zur Frage der Zulässigkeit von so genannten Online-Durchsuchungen, bei denen ohne Wissen des Betroffenen dessen Datenverarbeitungssysteme überwacht und Daten ausgelesen werden können.

Die Karlsruher Richter haben dabei verfassungsdogmatische Grundlagenarbeit geleistet, indem sie aus dem allgemeinen Persönlichkeitsrecht auch ein neues Grundrecht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ableiteten.

Für die Zulässigkeit eines heimlichen Eingriffs, wie er etwa im Wege der Online-Durchsuchung erfolgt, stellt das BVerfG hohe Hürden auf: Die heimliche Infiltration eines informationstechnischen Systems ist nur zulässig, wenn tatsächliche Anhaltspunkte für eine konkrete Gefahr im Hinblick auf ein überragend wichtiges Rechtsgut bestehen. Zu diesen Rechtsgütern zählt das BVerfG neben Leib und Leben auch solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand der Existenz des Staates berührt.

Anknüpfend an seine Rechtsprechung zum Schutz des Kernbereichs der privaten Lebensgestaltung vor staatlichen Überwachungsmaßnahmen fordert das BVerfG auch für die Online-Durchsuchung, dass jede diesbezügliche gesetzliche Ermächtigungsgrundlage dem Schutz dieses Kernbereichs ausreichend Rechnung tragen muss. Außerdem ist es zwingend erforderlich, derartige Maßnahmen unter den Vorbehalt richterlicher Anordnung zu stellen. Die Regelungen zur Online-

Durchsuchung im nordrhein-westfälischen Verfassungsschutzgesetz genügten diesen strengen Anforderungen nicht und wurden daher vom BVerfG für nichtig erklärt.

Außerdem äußerte sich das BVerfG in der Entscheidung auch zu der Frage, inwieweit ein heimliches Aufklären des Internets zulässig ist. So kann eine Maßnahme, welche auf Daten aus der laufenden Telekommunikation im Rechnernetz zugreift, als Eingriff in den Schutzbereich des Art. 10 GG zu qualifizieren sein, wenn die staatliche Stelle nicht durch Kommunikationsbeteiligte zur Kenntnisnahme autorisiert ist. Ein Grundrechtseingriff liegt laut BVerfG jedoch dann nicht vor, wenn der Staat lediglich im Internet öffentlich zugängliche Kommunikationsinhalte wahrnimmt, etwa wenn die Behörde nicht Zugangsgesicherte Webseiten oder Blogs einsieht.

Besonders erfreulich ist, dass das BVerfG durch die Etablierung eines Grundrechts auf die Vertraulichkeit von Informationssystemen eine Möglichkeit geschaffen hat, Lücken im Grundrechtsschutz zu schließen, die durch die neuen Informationstechnologien entstanden sind. Dem Datenhunger und Überwachungseifer staatlicher Sicherheitsbehörden kann dadurch nunmehr ein handfestes subjektives Grundrecht entgegengesetzt werden.

Nach einem Gesetz, das CDU, CSU und SPD am 9. November 2007 gegen die Stimmen der Opposition beschlossen haben, wurden die Anbieter von Kommunikationsdiensten und Kommunikationsnetzen gesetzlich verpflichtet, alle bei der Festnetztelefonie, der Mobilfunktelefonie sowie beim Email- und Internet-Verkehr anfallenden Bestands- und Verkehrsdaten mindestens ein halbes Jahr lang zu speichern. Zu Zwecken der Ermittlung und Verfolgung von Straftaten sollten diese Daten zur Verwendung durch die Sicherheitsbehörden bereit gehalten werden.

Bislang war es so, dass diese bei der Telekommunikation betrieblich anfallenden Daten, wie Datum, Zeitpunkt und Dauer der Kommunikation, Rufnummern, Namen und Anschriften der Kommunikationsteilnehmer, Benutzerkennungen und Internetprotokolladressen sowie Daten zum Standort der Handynutzer usw. aus Datenschutzgründen zu keinem anderen Zwecke als zur Gebührenabrechnung gespeichert werden durften und nach vollzogener Abrechnung unverzüglich zu vernichten waren.

Von der nun erlassenen sogenannten Vorratsdatenspeicherung, deren Einführung wegen verfassungsrechtlicher Bedenken sowohl von der Bundesregierung als auch vom Deutschen Bundestag jahrelang und wiederholt abgelehnt worden war, sind alle Teilnehmer an der Telekommunikation, also im Grunde alle Menschen betroffen.

Ihre lange Zeit hindurch ablehnende Haltung hat die Bundesregierung erst im letzten Jahr aufgegeben und daran mitgewirkt, dass im März 2006 eine entsprechende Richtlinie zur Vorratsdatenspeicherung auf europäischer Ebene erlassen wurde, die bis in nationales Recht umgesetzt werden muss.

Damit bedient sich auch die neue Bundesregierung einer von der alten Bundesregierung wiederholt geübten Praxis, Gesetzesverschärfungen im Bereich der inneren Sicherheit, die im Deutschen Bundestag auf breite Ablehnung stoßen, über den Umweg einer entsprechenden europarechtlichen Regelung durchzusetzen.

Da diese EU-Richtlinie wegen der Klage Irlands vom Europäischen Gerichtshof überprüft wird, hätte die Bundesregierung diese Entscheidung abwarten sollen.

Folgt man nun der einschlägigen verfassungsgerichtlichen Rechtsprechung und der weit überwiegenden Meinung der juristischen Fachöffentlichkeit, dann ist schon jetzt abzusehen, dass - wie so viele Gesetzgebungsvorhaben der Vergangenheit - auch die Vorratsdatenspeicherung einer Überprüfung durch das Bundesverfassungsgericht nicht standhalten wird. Die Sachverständigenanhörung im Bundestag hat dies bestätigt.

In vielen Entscheidungen hat nämlich das Bundesverfassungsgericht betont, dass nicht erst die staatliche Verarbeitung und Verwendung, sondern schon die Erhebung und Speicherung personenbezogener Daten einen Eingriff in das Recht auf informationelle Selbstbestimmung und in das Fernmeldegeheimnis gemäß Art. 10 GG darstellt, der unter verfassungsrechtlicher Perspektive einer Rechtfertigung bedarf.

Das heißt vor allem, dass der mit der Vorratsdatenspeicherung zu erzielende Nutzen für die innere Sicherheit in einem angemessenen Verhältnis zum Umfang und der Tiefe des mit der Vorratsdatenspeicherung verbundenen Eingriffs in die verfassungsrechtlich geschützten Grundrechtspositionen der Bürgerinnen und Bürger stehen muss.

An dieser Verhältnismäßigkeit bestehen erhebliche Zweifel.

Auch hat das Bundesverfassungsgericht immer wieder betont, (ich zitiere aus dem Volkszählungsurteil), dass „der Zwang zur Angabe personenbezogener Daten voraussetzt, dass der Gesetzgeber den Verwendungszweck dieser Daten bereichsspezifisch und präzise bestimmt und, dass die Angaben für diesen Zweck geeignet und erforderlich sind“.

Mit diesen verfassungsrechtlichen Bedingungen wäre, so das Bundesverfassungsgericht weiter, „die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbar Zwecken nicht zu vereinbaren“ (Zitat Ende)

Also, sehr geehrte Damen und Herren, es besteht begründeter Anlass anzunehmen, dass eine verfassungsgerichtliche Prüfung die geplante Vorratsdatenspeicherung als grundgesetzwidrig verwerfen würde.

Da sich nun die Bundesregierung mit ihrem Vorhaben dahinter versteckt, dass sie europarechtlich zur Umsetzung der existierenden EU-Richtlinie zur Vorratsdatenspeicherung verpflichtet war, wobei sie natürlich verschweigt, dass sie an dem Zustandekommen dieser EU-Richtlinie kräftig mitgewirkt hat, ist zunächst die Frage völlig offen, ob das Bundesverfassungsgericht die Verfassungsbeschwerde gegen die Vorratsdatenspeicherung überhaupt zur Entscheidung annehmen wird.

Denn das Bundesverfassungsgericht hat besonders in seiner so genannten Solange-Rechtssprechung und seiner Entscheidung zur europäischen Bananenmarktordnung betont (ich zitiere), dass „Verfassungsbeschwerden (...), die eine Verletzung von Grundrechten des Grundgesetzes durch sekundäres Recht der Europäischen

Gemeinschaften geltend machen, von vorneherein unzulässig (sind), wenn ihre Begründung nicht darlegt, dass die europäische Rechtsentwicklung einschließlich der Rechtsprechung des Europäischen Gerichtshofs (.....) unter den erforderlichen Grundrechtsstandard abgesunken ist“ (Zitat Ende)

Sie sehen also, sehr geehrte Damen und Herren, es ist durchaus eine Situation denkbar, in der die Vorratsdatenspeicherung - obgleich grundgesetzwidrig - dennoch im nationalen Recht Verankerung findet, weil es keine Gerichtsinstanz gibt, die diese Grundgesetzwidrigkeit feststellt.

Eins ist aber sicher: Der öffentliche Widerstand gegen die Vorratsdatenspeicherung ist groß. Zehntausende Bürger haben bereits gegen die staatliche Überwachung demonstriert. Allein die Sammelklage des AK Vorratsdatenspeicherung zählt knapp 35,000 Beschwerdeführer.

Wie das Bundesverfassungsgericht entscheiden wird, ob es die Beschwerde zur Entscheidung annehmen oder als unzulässig verwerfen wird, ist eine ebenso spannende, wie offene Frage. Bisher hat es zumindest eine einstweilige Anordnung erlassen, die die Vorratsdatenspeicherung stark einschränkt. Die gespeicherten Daten dürfen nur noch zur Verfolgung schwerer Straftaten und nach richterlichem Beschluss herausgegeben werden.

Diese Anordnung wurde mittlerweile auch verlängert.

Zuversichtlich stimmt außerdem eine Eilentscheidung des Verwaltungsgerichts Berlin, die im Juli bekanntgegeben wurde. Danach sind die Regelungen der Vorratsdatenspeicherung auch unter finanziellen Gesichtspunkten unverhältnismäßig. Die Telekommunikationsanbieter erhalten für den Mehraufwand, der mit der halbjährigen Speicherung einhergeht, keine finanzielle Entschädigung vom Staat. Das Gericht hegt dahingehende Zweifel an der Verfassungsmäßigkeit des Gesetzes, muss es aber zunächst dem Bundesverfassungsgericht vorlegen, da nur Karlsruhe die Kompetenz hat Gesetze wegen Verfassungswidrigkeit zu verwerfen.

Wir werden abwarten müssen.

Wenn man die Folgen der eben aufgezählten Urteile des Verfassungsgerichts nimmt und die Beschwerden einiger Innenpolitiker und Sicherheitsbeamten hört, kann tatsächlich der Eindruck entstehen, der Datenschutz und ihm verwandte Freiheitsrechte stünden der Terrorismusbekämpfung im Weg.

Die rechtspolitische Wirklichkeit muss aber differenzierter betrachtet werden. Fakt ist nun mal: Der Datenschutz hat Grundrechtsrang. Aus dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG entwickelte Karlsruhe einen grundrechtlichen Schutz der Privatsphäre sowie das Grundrecht auf informationelle Selbstbestimmung. Auch das neue IT-Grundrecht schützt persönliche Daten, die in informationstechnischen Systemen gespeichert oder verarbeitet werden.

Das mit der Bekämpfung des Terrorismus verfolgte Ziel ist, zweifelsohne mehr Sicherheit zu schaffen. Die öffentliche Sicherheit und Ordnung ist zweifellos ein bedeutendes Rechtsgut, Grundrechtsrang hat es aber nicht.

Allerdings gilt der grundrechtliche Datenschutz nicht absolut. Im konkreten Fall bedarf es der Abwägung zwischen Interesse des Betroffenen an Geheimhaltung und Schutz der Privatsphäre und dem öffentlichen Informationsinteresse. Im Fall eines konkreten terroristischen Bedrohungsszenarios dürfte das öffentliche Interesse an Datenerhebung überwiegen. Die entscheidende Frage ist aber, wie die Abwägung bei einer abstrakten Gefährdungslage vorzunehmen ist. Eine solche Gefährdungslage wird seit dem 11. September fast durchgängig von Innenpolitikern und Sicherheitsbehörden beschworen.

Dafür ist mit entscheidend, welche Qualität dem internationalen Terrorismus beigemessen wird. Ist die Terrorismusbekämpfung tatsächlich Teil eines groß angelegten „Krieges gegen den Terror“, wie ihn der amerikanische Präsident ausgerufen hat? Oder handelt es sich dabei ‚nur‘ um die Bekämpfung besonders heimtückischer, politisch motivierter Verbrechen?

Eine Einstufung der Terrorismusbekämpfung als Notstand oder „kriegsähnlich“ könnte unter Umständen eine Einschränkung von Freiheitsrechten, wie dem Datenschutz, rechtfertigen. Doch wenn überhaupt, ist die Bekämpfung des Terrorismus nicht mit einem konventionellen, „heißen“ Krieg vergleichbar, sondern eher mit dem Kalten Krieg.

Auch dieser zeichnete sich durch eine abstrakte Gefährdungslage aus, die über Jahrzehnte andauert hat. Damals konnte man nicht abschätzen, wie lange der Kalte Krieg dauern würde, wodurch eine Abwägung zugunsten der Sicherheit und auf Kosten der Freiheit unverhältnismäßig und unangebracht gewesen wäre. Sie hätte ja auch endgültig sein können und käme damit einer Aufgabe unserer tradierten Rechtsstaatlichkeit gleich.

Außerdem waren die von der westlichen Welt genossenen Freiheiten eine der effizientesten „Waffen“ gegen die totalitären Widersacher. Indem er den moderaten Kräften und Dissidenten als Leitbild gedient hat, hat der freiheitlich-demokratische Rechtsstaat wesentlich dazu beigetragen, dass der Kalte Krieg nicht auf dem Schlachtfeld, sondern an einem runden Tisch beendet wurde.

Der islamistische Terrorismus ist ausgesprochen gefährlich, keine Frage. Und ich brauche auch nicht betonen, wie verabscheuungswürdig er ist. Rechtfertigt das alleine schon die Analyse, die moderne Welt sei jetzt im Krieg mit dem islamistischen Terrorismus? Reichen wirklich die Mittel der Gefahrenabwehr und Strafverfolgung nicht aus, wie behauptet wird?

Maßnahmen zur Bekämpfung des Terrorismus müssen wie alle anderen staatlichen Eingriffe die Grundrechtschranken, gerade auch des Datenschutzes, beachten. Diese Sichtweise ist durch die vorhin skizzierte Rechtsprechung unstrittig bestätigt worden.

Anrede,

eine von Grundrechtswängen befreite Terrorismusbekämpfung macht nicht zwangsläufig sicherer. Die Bewahrung des Datenschutzes und eines Kernbereichs der Privatsphäre liegt nicht nur im elementaren Interesse des Einzelnen, sondern ist ein unverzichtbarer Teil unserer liberalen Rechtsordnung. Ohne die Freiheit des einzelnen Bürgers wird es auch keine gesellschaftliche Freiheit geben.

Die Frage, ob der Datenschutz der Terrorismusbekämpfung im Weg steht, kann nur bejaht werden, wenn man unsere Grundrechtstradition ausblendet. Diese Sichtweise ist einseitig und stark vereinfacht. Sie geht davon aus, dass Datenschutz mit Täterschutz gleichzusetzen ist.

Daher ist „im Weg stehen“ nicht die richtige Formulierung. Sie impliziert, dass der Datenschutz ein minderwertiges Rechtsgut ist, welches illegitimerweise das Streben nach Sicherheit behindert. Tatsächlich hat der Datenschutz aber Grundrechtsrang und Grundrechte haben eine Schrankenfunktion. Man könnte daher eher die These umdrehen und behaupten, dass die Terrorismusbekämpfung dem Datenschutz im Weg steht.

Der Datenschutz setzt der Terrorismusbekämpfung Schranken. Schranken, die rechtsstaatlich geboten sind und sich aus unserem Grundgesetz ergeben. Insoweit steht der Datenschutz der Terrorismusbekämpfung genauso im Weg wie habeas corpus, Prozessrechte und das Folterverbot. Auch wenn die Terroristen sich an keine Regeln halten, bedeutet das nicht, dass wir uns bei ihrer Bekämpfung dasselbe erlauben dürfen.

Doch darf bei alledem nicht vergessen werden, dass Freiheit - in Form des Datenschutzes - und Sicherheit sich nicht gegenseitig ausschließen. Das Verhältnis ist komplizierter.

Der Einzelne kann in einer Diktatur, von einer staatlichen Gewalt um seine Freiheit gebracht wird, nie wirklich sicher sein. Er kann immer der Willkür ausgesetzt sein, ist abhängig von der Gnade der Obrigkeit. Andererseits kann Freiheit in einer lebensbedrohlichen Lage auch nicht wirksam ausgeübt werden.

Es kommt auf die Balance zwischen Freiheitsrechten und Maßnahmen zur Erhaltung der Sicherheit an. Doch diese Balance verschiebt sich in letzter Zeit zunehmend zugunsten der Sicherheit und auf Kosten der Freiheit. Der Einsatz für Freiheitsrechte wie den Datenschutz ist heute so wichtig, weil die elektronischen Datensammlungen stetig wachsen. Dadurch wachsen auch die Begehrlichkeiten staatlicher Überwachung.

Freiheit lässt sich nicht mit deren Einschränkung verteidigen. Wie Bundespräsident Köhler am Dienstag auf dem Juristentag in Erfurt sagte: „Unser Streben nach Sicherheit darf uns nicht unsere Freiheit kosten.“