Von der Volkszählung zur Speicherung von Verbindungsdaten - 25 Jahre informationelle Selbstbestimmung

Professor Dr. h. c. Hans-Jürgen Papier, Präsident des Bundesverfassungsgerichts

Sehr geehrte Damen und Herren, am 15. Dezember letzten Jahres wurde auf einer Veranstaltung in Karlsruhe – einige von Ihnen haben daran teilgenommen – der 25. Jahrestag des Volkszählungsurteils des Bundesverfassungsgerichts feierlich begangen, das gemeinhin als der Urknall des Datenschutzes gilt.

Die Geschichte des Datenschutzes begann jedoch schon früher – und zwar hier in Wiesbaden im Hessischen Landtag mit der Verabschiedung des Hessischen Datenschutzgesetzes von 1970 als erstem Datenschutzgesetz weltweit1. Damit gebührt eigentlich dem Land Hessen und nicht

dem Bundesverfassungsgericht die Ehre, Erfinder des Datenschutzes und

somit – wie Sie verehrter Herr Kollege Ronellenfitsch in meiner Einladung zur heutigen Veranstaltung formulierten – „Mutterland des Datenschutzes“ zu sein.

Gleichwohl hat das Volkszählungsurteil des Bundesverfassungsgerichts herausragende Bedeutung für den Datenschutz, weil es ihn dort von der einfach-rechtlichen Ebene in den Olymp des Verfassungsrechts erhob und aus dem Grundgesetz ein "Grundrecht auf informationelle Selbstbestimmung" ableitete2.

I. Zum Hintergrund des „Volkszählungsurteils“

Wie kam es jedoch dazu, dass ausgerechnet die für das Jahr 1983 geplante Volkszählung zu einer solchen Entscheidung führte?

Volkszählungen waren bereits vor 2.000 Jahren – denken wir nur an die im Weihnachtsevangelium erwähnte Volkszählung unter Kaiser Augustus – ein übliches Mittel, mit dem Regierungen Informationen über ihre Bevölkerung gewannen. Insbesondere im Römischen Reich galt der sogenannte "Zensus", die Volks- und Vermögensschätzung, als ein notwendiges Instrument der Steuererhebung. In den Vereinigten Staaten sind Volkszählungen im Zehnjahresrhythmus sogar von der Verfassung vorgeschrieben3. Auch in der Bundesrepublik Deutschland gab es bereits vor dem Jahr 1983 Volkszählungen4 und für das Jahr 2011 ist ein EU-weiter Zensus geplant, der in Deutschland – anders als im Jahr 1983 – hauptsächlich registergestützt durchgeführt werden soll5. Diese Erhebungen dienen heute aber nicht mehr in erster Linie steuerlichen Zwecken, sondern sie verschaffen dem Staat die statistische Grundlage für gesellschaftspolitische, soziale, wirtschaftliche und ökologische Planungen und Entscheidungen6.

Dies war auch bei der für das Jahr 1983 geplanten Volkszählung so. Gleichwohl hat damals das die Datenerhebung anordnende Gesetz auch in solchen Teilen der Bevölkerung Beunruhigung ausgelöst, die – ich zitiere das „Volkszählungsurteil" – als loyale Staatsbürger das Recht und die Pflicht des Staates respektierten, die für rationales und planvolles staatliches Handeln erforderlichen Informationen zu beschaffen7. Zu dieser Beunruhigung mag beigetragen haben, dass einige Sachkundige - wie etwa mein verehrter Kollege Spiros Simitis als Hessischer Landesdatenschutzbeauftragter8 – trotz einstimmiger Verabschiedung des Volkszählungsgesetzes in den gesetzgebenden Körperschaften von Anfang an die Auffassung vertraten, die dort geregelten

Möglichkeiten der Erhebung und Verwertung von Daten genügten nicht hinreichend unserer Verfassung9. Dies hat ja dann zum Teil mit der Entscheidung des Bundesverfas-sungsgerichts vom 15. Dezember 1983 auch eine Bestätigung erfahren.

Jedoch beruhte die Beunruhigung in der Bevölkerung darüber hinaus auch wesentlich darauf, dass sich im Laufe der 70er Jahre die Möglichkeiten der Datenverarbeitung erheblich weiterentwickelt hatten. Zur Datenverarbeitung wurden damals immer mehr Großrechner eingesetzt. Diese konnten aus Größen- und Kostengründen nur vom Staat und kapitalkräftigen Unternehmen betrieben werden. Die Datenverarbeitung fand deshalb in zentralen, in der Regel gut abgeschirmten Rechenzentren statt und wurde nur von einer kleinen Schicht hochspezialisierter Fachleute beherrscht10. Gerade dadurch sah wohl mancher das von George Orwell für das Jahr 1984 prognostizierte Menetekel zur Wirklichkeit werden, nämlich eine totale Beherrschung der Gesellschaft durch eine allwissende, selbst die Gedankenwelt kontrollierende Partei11.

Mittlerweile haben sich die technischen Möglichkeiten der Datenverarbeitung freilich so sehr revolutioniert, dass der „Große Bruder“ George Orwells aus heutiger Sicht über die damals, gewissermaßen in der informationstechnischen Steinzeit bestehenden Möglichkeiten der Überwachung nur noch mitleidig lächeln könnte. Die technischen Möglichkeiten von heute befinden sich allerdings nicht mehr in den Händen weniger Einzelner oder gar nur von Staaten. Die Privatisierung der Informationstechnologie hat im Zusammenwirken mit der Globalisierung die Zahl potentieller „Big Brother“ so unübersichtlich werden lassen, dass aus datenschutzrechtlicher Sicht anarchische Zustände eher zu drohen scheinen als ein totalitärer Überwachungsstaat.

Doch lassen Sie mich, bevor ich auf die heute durch den Staat und durch Private drohenden Gefahren für das Recht auf informationelle Selbstbestimmung sowie weitere den Datenschutz betreffende Entwicklungen eingehen werde, zunächst die Grundaussagen des „Volkszählungsurteils“ in Erinnerung rufen.

II. Grundaussagen

1. Herleitung des Rechts auf informationelle Selbstbestimmung

Das Bundesverfassungsgericht verankerte das mit dem „Volkszählungsurteil“ anerkannte „Recht auf informationelle Selbstbestimmung“ im Mittelpunkt unserer grundgesetzlichen Ordnung, nämlich im Wert und der Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt. Ihrem Schutz dient – neben speziellen Freiheitsverbürgungen wie dem Grundrecht auf Unverletzlichkeit der Wohnung oder dem Brief-, Post- und Fernmeldegeheimnis – das allgemeine Persönlichkeitsrecht12, das unter anderem auch das Recht am eigenen Bild oder vor verfälschenden oder entstellenden Darstellungen der eigenen Person schützt.13

Die Ableitung eines Maßstabs für die staatliche Informationserhebung und ver-arbeitung unter Bezugnahme auf die Menschenwürde und das allgemeine Persönlichkeitsrecht war freilich nicht neu. So hatte das Bundesverfassungsgericht bereits im Jahre 1970 in seiner Entscheidung zum sogenannten „Mikrozensus“ – das ist die Erstellung einer Repräsentativstatistik der Bevölkerung und des Erwerbslebens – festgestellt, dass es mit der Menschenwürde nicht zu vereinbaren wäre, wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich sei.14

Neu war im „Volkszählungsurteil“ vielmehr, dass das Bundesverfassungsgericht die Vorgaben des allgemeinen Persönlichkeitsrechts an die modernen Bedingungen der automatischen Datenverarbeitung angepasst hat15. Die freie Entfaltung der Persönlichkeit setzt hier den Schutz des

Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Das Grundrecht auf informationelle Selbstbestimmung gewährleistet daher dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen16.

Damit wurde die zuvor vom Bundesverfassungsgericht verwendete „Sphärenkonzeption“ zum Teil aufgegeben17. Seit dem „Volkszählungsurteil“ hängt die Beurteilung der Frage, inwieweit ein Datum als sensibel zu beurteilen ist, nicht mehr allein davon ab, ob es einen intimen Vorgang betrifft. Unter den Bedingungen der modernen Informationstechnologie gibt es nämlich kein vornherein „belangloses Datum“ mehr. Vielmehr bedarf es nun zur Feststellung der persön-lichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines Verwendungszusammenhangs18.

Die modernen Mittel der Datenverarbeitung geben zudem die Möglichkeit, einmal erlangte Informationen beliebig zusammenzufügen, ohne dass der Einzelne die Richtigkeit und Verwendung kontrollieren könnte. Wer jedoch nicht mehr überschauen kann, wer in einer Gesellschaft was wann und bei welcher Gelegenheit über einen weiß, wird in seiner Persönlichkeit und in der Ausübung von Freiheitsrechten, die auch für die Mitwirkung in einem demokratischen Gemeinwesen von Bedeutung sind, gefährdet19.

Das Recht auf informationelle Selbstbestimmung hat nach dem „Volkszählungsurteil“ allerdings nicht zur Folge, dass der Einzelne ein eigentumsgleiches Recht an „seinen Daten“ hat20. Denn der Mensch ist Teil einer miteinander kommunizierenden Gemeinschaft. Eine Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann. Dies hat zugleich zur Folge, dass der Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen muss21.

2. Datenschutzrechtliche Folgerungen

Welche konkreten Folgerungen zog das „Volkszählungsurteil“ aus der genann-ten Einordnung des Datenschutzes als Grundrechtsschutz?22 Eingriffe in das Recht auf informationelle Selbstbestimmung bedürfen nach dem „Volkszählungsurteil“ zunächst einer hinreichend bestimmten gesetzlichen Grundlage23. Dabei muss der Gesetzgeber den Verwendungszweck der zu erhebenden Daten bereichsspezifisch und präzise festlegen24. Eine Weitergabe von Daten kommt grundsätzlich nur zu dem gleichen Zweck in Betracht, zu dem die Daten erhoben wurden. Die öffentliche Verwaltung ist keine „Informationseinheit“, innerhalb derer im Wege der Amtshilfe jede Information beschafft werden darf25. Erforderlich sind zudem verfahrensrechtliche Schutzvorkehrungen, wie Aufklärungs-, Auskunfts- und Löschungspflichten sowie im Interesse eines vorgezogenen Rechtsschutzes die Beteiligung eines unabhängigen Datenschutzbeauftragten26.

III. Weitere Entwicklung des Datenschutzes

Die Vorgaben des „Volkszählungsurteils“ führten dann im Jahr 1990 zu einer Novellierung des aus dem Jahr 1977 stammenden Bundesdatenschutzgesetzes27. Damit war die Entwicklung des Datenschutzes freilich nicht abgeschlossen. Für die Folgezeit lassen sich vielmehr vier wichtige Entwicklungslinien identifizieren, die – wie ich meine – auch für die zukünftige Entwicklung maßgeblich sein werden.

1. Europäische Integration

Eine Entwicklungslinie wurzelt in der Europäischen Integration. Die Einführung des Binnenmarktes brachte die Notwendigkeit mit sich, die Regeln der EG-Mitgliedstaaten über den Schutz der Privatsphäre bei der Datenverarbeitung zu vereinheitlichen. Denn die Datenverarbeitung machte fortan nicht mehr an den Ländergrenzen Halt, wohingegen die unterschiedlichen Datenschutzregeln –sofern denn überhaupt welche existierten28 – die Freiheit des Verkehrs von Waren, Personen, Dienstleistungen und Kapital beeinträchtigten. Die deshalb im Jahr 1995 erlassene allgemeine Datenschutz-Richtlinie29 kombinierte unter-schiedliche juristische Ansätze und Rechtskulturen und beschränkte sich nicht –wie man annehmen könnte –- auf den kleinsten gemeinsamen Nenner, sondern zielte auf ein hohes Schutzniveau ab.30 Darüber hinaus erfordert nicht nur die gemeinsame Verwaltung des Binnenmarktes31, sondern auch die Abschaffung der Grenzkontrollen an den Binnengrenzen der Europäischen Union durch das Schengener-Durchführungsübereinkommen32 und die in der Folge verstärkte Zusammenarbeit in Bereichen Justiz und Inneres33 einen Informationsaustausch zwischen den vielen mitgliedstaatlichen Verwaltungen und der Kommission34. Dabei ist aus datenschutzrechtlicher Sicht positiv hervorzuheben, dass für die deshalb errichteten Systeme für den Datenaustausch zwischen den Mitgliedstaaten – wie etwa das Schengener Informationssystem – spezielle Regeln über den Rechtsschutz des Betroffenen und die Amtshaftung existieren35.

Die europäischen Organe und Einrichtungen selbst sind durch eine Verordnung an datenschutzrechtliche Regeln gebunden36. Darüber hinaus würde die Charta der Grundrechte der Europäischen Union - sollte sie mit dem Vertrag von Lissabon in Kraft treten - dem Recht auf Schutz personenbezogener Daten – unabhängig von ersten Ansätzen hierzu in Entscheidungen des Gerichtshofs der Europäischen Gemeinschaften37 – deutlich sichtbar den Status des Grund-rechtsschutzes verleihen38.

2. Konzept der informierten Öffentlichkeit

Lassen Sie mich zu einer weiteren Entwicklungslinie kommen, die allerdings dem staatlichen Datenschutz zu widersprechen scheint: Sie beruht auf dem „Konzept der informierten Öffentlichkeit“39. In Verfolgung dieses Konzepts wurde in den letzten Jahren mit der deutschen Arkantradition gebrochen, nach der Behördenakten – außer für die Beteiligten –- grundsätzlich der Geheimhaltung unterlagen40. Nun gibt es auf Bundes- oder Landesebene Gesetze, die jedermann den Zugang zu Umweltinformationen, zu gesundheitsbezogenen Verbraucherinformationen oder allgemein zu jeder amtlichen Information gewährleisten41. Diese Entwicklung hin zu einem "gläsernen Amt"42 wurde unter anderem durch Vorschriften der Europäischen Union43 sowie durch Vorbilder in anderen Staaten wie den USA44 oder Schweden angestoßen. In letzterem ist das Öffentlichkeitsprinzip bereits im Jahr 1766 eingeführt worden45.

Das „Konzept der informierten Öffentlichkeit“ hat nicht nur zur Folge, dass der Bundesbeauftragte für den Datenschutz jetzt auch für die Informationsfreiheit zuständig ist46. Nein, es zielt vielmehr darauf ab, die „res publica“ Wirklichkeit werden zu lassen47, dass heißt, durch mehr Transparenz der Verwaltung und einen verbesserten Informationszugang der Bürger den demokratischen Meinungs- und Willensbildungsprozess zu stärken48. Damit korrespondiert das Informationszugangsrecht für Jedermann - jedenfalls auf einer abstrakten Ebene - mit dem Recht auf informationelle Selbstbestimmung49. Wie bereits erwähnt, hat ja gerade auch das "Volkszählungsurteil" den Zusammenhang zwischen Datenschutz und Ausübung demokratischer Freiheitsrechte deutlich aufgezeigt50. Dennoch ist auch unübersehbar, dass es im konkreten Fall durchaus zu einem Konflikt zwischen Informationsfreiheit und Datenschutz kommen kann, und zwar nicht nur dann, wenn wie im Sonderfall des Stasi-Unterlagen-Gesetzes personenbezogene Daten durch rechtsstaatswidrige Ausspähung erlangt wurden51. Ich denke jedoch, dass diese Konflikte durch eine sorgfältige und differenzierende Abwägung der jeweiligen Rechtspositionen gelöst werden können52.

3. Innere Sicherheit

Freilich wurde der Staat in den Jahren nach dem "Volkszählungsurteil" nicht nur gläserner, er bekam auch selbst immer mehr Möglichkeiten zur Durchleuchtung Einzelner. So wurden in den 90er Jahren insbesondere zur Bekämpfung der Organisierten Kriminalität neue Ermittlungsmethoden eingeführt, wie der „kleine“ und der „große Lauschangriff“53, und es wurden die Befugnisse des BND zur Überwachung der Telekommunikation ausgeweitet54. Und nach den Terror-anschlägen vom 11. September 2001 in den USA und vom 11. März 2004 in Madrid wurden in Deutschland sowie auf EU-Ebene Maßnahmen durchgeführt oder beschlossen, wie die präventive polizeiliche Rasterfahndung nach sogenannten „Schläfern“55, die „Online-Durchsuchung“56 oder die Vorratsspeicherung von Telekommunikationsverbindungsdaten57.

Damit steht das Recht auf informationelle Selbstbestimmung im Vergleich zur Zeit des „Volkszählungsurteils“ vor neuen Herausforderungen. Sie haben ihren Grund allerdings nicht nur in der Art der drohenden Gefahren, sondern auch in den revolutionären Veränderungen der Informations- und Kommunikationstechnologie. Es ist dabei anzuerkennen, dass der Staat – schon um seiner grundrechtlichen Pflicht zum Schutz von Leib, Leben oder Freiheit zu genügen – diese technischen Veränderungen bei der Gefahrenbekämpfung und Verfolgung von Straftaten nicht unberücksichtigt lassen kann58. Gleichwohl dürfen bei der Ausbalancierung von Freiheit und Sicherheit die Gewichte nicht grundlegend verschoben werden59.

Für Eingriffe in das Recht auf informationelle Selbstbestimmung stellt zunächst der Verhältnismäßigkeitsgrundsatz Anforderungen an den Rang der zu schützenden Rechtsgüter sowie die Art und Intensität von deren Gefährdung60. So sind beispielsweise präventive polizeiliche Rasterfahndungen ohne Vorliegen einer konkreten Gefahr für hochrangige Rechtsgüter oder automatische Kfz-Kennzeichenüberwachungen ohne konkreten Anlass und ohne jede Konkretisierung der Verwendungszwecke mit dem Verhältnismäßigkeitsgrundsatz nicht zu vereinbaren61.

Darüber hinaus darf - dies hat das Bundesverfassungsgericht seit seiner Anfangszeit immer wieder betont62 – der Kernbereich privater Lebensgestaltung, der sich letztlich aus der Menschenwürde ableitet, durch staatliche Überwachungsmaßnahmen nicht angetastet werden. Die Menschenwürde und der Menschenwürdegehalt spezieller Freiheitsrechte sind nämlich nicht gegenüber anderen Freiheitsrechten und den aus ihnen folgenden Schutzpflichten des Staates abwägbar oder gar „wegwägbar“. Gleichwohl stellt sich in der Praxis oft das Problem, dass vor einer Datenerhebung nicht geklärt werden kann, ob sie den Kernbereich betreffen wird. Für diese Situationen hat das Bundesverfassungsgericht in seiner Entscheidung zur „Online-Durchsuchung“ ein zweistufiges Schutzkonzept durch die Unterscheidung von Erhebungs- und Auswertungsphase entwickelt, auf das ich jetzt aber nicht näher eingehen möchte63.

Vielmehr möchte ich noch erwähnen, dass das Recht auf informationelle Selbstbestimmung nach Maßgabe des „Volkszählungsurteils“ im Alter von fast 25 Jahren mit der genannten Entscheidung zur „Online-Durchsuchung“ gewissermaßen eine „Schwester“ bekommen hat, nämlich das „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“. Die Geburt dieser neuen „Tochter“ des allgemeinen Persönlichkeitsrechts war notwendig, weil weder die speziellen Freiheitsrechte noch die übrigen Ausprägungen des allgemeinen Persönlichkeitsrechts gegen die Gefahren hinreichend Schutz gewähren, die sich aus der für die Persönlichkeitsentfaltung bedeutsamen Nutzung der Informationstechnik ergeben64. Das neue Grundrecht sichert den persönlichen Bereich nämlich auch dann, wenn auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten65. Zudem schützt es die Vertraulichkeit und Integrität dieser Systeme insbesondere dann, wenn der

Einzelne wegen ihrer technischen Komplexität gar nicht mehr in der Lage ist, über ihre Vertraulichkeit und Integrität selbst bestimmen zu können66. Das Recht auf informationelle Selbstbestimmung liefe hier von seinem Ansatz her ins Leere.

Angesichts dieser alten und neuen grundrechtlichen Grenzen für die sicherheitsrechtliche Tätigkeit des Staates scheint mir seine Verwandlung in einen Überwachungsstaat „Orwell'scher Prägung“ eine eher fernliegende Möglichkeit zu sein. Denn jenseits aller verfassungsrechtlichen Unzulänglichkeiten der bisher vom Bundesverfassungsgericht beanstandeten Maßnahmen versuchen - nach meiner Beobachtung - die derzeit maßgeblichen politischen Akteure zumindest, sich an diese Vorgaben zu halten67. Entscheidend ist jedoch, dass unser Gemeinwesen über rechtsstaatliche und demokratische Kontrollmechanismen verfügt, die es von totalitären Überwachungsstaaten unterscheidet, wie wir sie auch aus unserer jüngeren Geschichte kennen.

4. Gefahren für den Datenschutz durch Private

Ich sorge mich jedenfalls mehr davor, dass wir uns zu einer privaten Überwachungsgesellschaft internationalen Ausmaßes verwandeln, und dies weitge-hend auch noch völlig freiwillig. Durch den andauernden technischen Fortschritt der Informations- und Kommunikationstechnologie und die internationale Vernetzung der Informationswege haben wir alle – zumindest diejenigen von uns, die sich diesen laufenden technischen Veränderungen stellen wollen oder können – im Vergleich zur Zeit vor 25 Jahren unglaublich viele neue Handlungsmöglichkeiten hinzugewonnen. Wir können über das Internet Briefe schreiben, die in Sekundenschnelle ankommen, Bücher und Bahntickets kaufen sowie unsere Bankgeschäfte erledigen. Wir freuen uns darüber, wenn wir beim Einkauf Bonuspunkte bekommen, für die wir später ein „Geschenk“ erhalten oder geben im Internet ohne größeres Nachdenken auf verschiedensten Seiten unsere intimsten Gedanken, Gefühle oder Bilder einem uns unbekannten Publikum preis.

Würden alle diese irgendwo auf der Welt über uns gespeicherten Informationen zusammengeführt, ließe sich sehr leicht ein „Persönlichkeitsprofil“ von jedem von uns erstellen. Dadurch würde – herbeigeführt durch die Hände Privater und nicht den Staat – ein Szenario Wirklichkeit werden, das im „Volkszählungsurteil“ für unzulässig befunden wurde und das als „Super-Gau des Datenschutzes“ bezeichnet werden kann68. Auch eine weitere, bereits eingangs zitierte Aussage des „Volkszählungsurteils“ scheint auf privatem Sektor neue Aktualität zu bekommen. Die Aussage lautete: „Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über einen weiß“. Diesbezüglich drängt sich der Gedanke an die im letzten Jahr aufgetretenen Skandale betreffend den „Datendiebstahl“ oder die Überwachung von Arbeitnehmern geradezu auf69. Wenn man noch berücksichtigt, dass das Internet – wie es heißt – „nichts vergisst“, erscheint eine zweckwidrige Verwendung von heute im Internet kommunizierten Daten in der Zukunft geradezu programmiert70.

Das Grundrecht auf informationelle Selbstbestimmung im Sinne des „Volkszählungsurteils“ und seine junge „Schwester“, das Grundrecht auf Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme, fordern auch diesbezüglich den Schutz der Bürger. Denn die genannten Grundrechte verpflichten den Staat, im Ausgleich mit konkurrierenden Freiheitsrechten ein angemesse-nes Schutzregime zu schaffen und durchzusetzen sowie sich auf internationaler Ebene für ein solches Regime einzusetzen71. Dabei wird sich der Staat häufig nicht mit bloßen Selbstverpflichtungen Privater begnügen dürfen, sondern wird selbst eine verbindliche Ordnung konstituieren müssen, um der grundrechtlichen Werteordnung auch im Privatrechtsverkehr Geltung zu verschaffen. In der Folge der jüngsten „Datenschutzskandale“ hat der Gesetzgeber kürzlich gleich drei Novellen zum Bundesdatenschutzgesetz verabschiedet72, die vor allem der unzureichenden

Transparenz und Rechtssicherheit im Auskunfteiwesen und beim sogenannten Kreditscoring73 sowie dem illegalen Adresshandel und Fällen ausufernder Mitarbeiterkontrolle abhelfen sollen74. Ganz zum Schluss der Legislaturperiode wurde vom Bundesministerium für Arbeit und Soziales sogar noch ein eigener Gesetzentwurf zum Arbeitnehmer-Datenschutz vorgestellt75. Eine verfassungsrechtliche Bewertung dieser erlassenen oder vorgeschlagenen Neuregelungen möchte ich an dieser Stelle freilich nicht vornehmen.

5. Schluss

Meine Damen und Herren, lassen Sie mich vielmehr zum Schluss festhalten, dass der Ausgangspunkt des „Volkszählungsurteils“ in den letzten 25 Jahren erhebliche Veränderungen und Entwicklungen erfahren hat. Gleichwohl haben die Aussagen des Urteils nichts von ihrer Aktualität verloren. Das Recht der informationellen Selbstbestimmung muss sich bewähren im Spannungsfeld des behördlichen Umgangs mit neuen europarechtlichen Freiheiten, dem Konzept der informierten Öffentlichkeit hinsichtlich beim Staat vorhandener Daten, neuer Anforderungen der inneren Sicherheit sowie Bedrohungen des Datenschutzes durch Private. Hier ist es die Aufgabe des Datenschutzes, mit kritischer Wachsamkeit die weitere Entwicklung zu verfolgen und im demokratischen Streit die beste Lösung zu finden. Warnen möchte ich allerdings davor, in diesem Zusammenhang das nahe Heraufziehen eines Überwachungsstaates Orwell'scher Prägung zu beschwören und durch einen Vergleich unseres demokratischen Rechtsstaats mit anderen aktuellen oder historischen Gemeinwesen kategoriale Unterschiede zu verwischen. Vielleicht sollten wir dabei einen – jüngst von Ulrich Clauß in der Welt zitierten – Satz von Karl Popper in einem seiner letzten Interviews Anfang der neunziger Jahre bedenken, der meinte, dass Menschen, die in freiheitlichen Gesellschaften aufgewachsen sind, oft nur schwer begreifen können, worin der fundamentale Unterschied zu unfreien besteht, zu Gesellschaften in denen jedermann einfach nachts abgeholt werden kann und spurlos verschwindet76. In einem solchen Staat leben wir nicht und werden wir hoffentlich auch nie wieder leben müssen. Für den Staat des Grundgesetzes gilt das schon im Jahre 1670 von dem großen niederländischen Philosophen de Spinoza geprägte Wort: „Der Zweck des Staates ist in Wahrheit die Freiheit“ in besonderem Maße. Deshalb verlangen aber auch die in meinem Vortrag geschilderten Gefahren für den elementaren Persönlichkeitsschutz entschiedene und vor allem auch rechtzeitige Sanktionen.

_____

Fußnoten (bitte auf die Ziffer klicken, um zur Textstelle zurückzukehren):

1Hess. GVBl I 1970 S. 625; vgl. Simitis, BDSG, 6. Aufl. 2006, Einleitung Rn. 1.

2Vgl. BVerfGE 65, 1 (41 ff.).

3Vgl. Art. 1, Section 2 of the United States Constitution.

4Vgl. BVerfGE 65, 1 (12).

5Vgl. VO (EG) Nr. 763/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über Volks- und Wohnungszählungen, ABl. Nr. L 218 vom 13. August 2008, S. 14; Zensusvorbereitungsgesetz 2011 vom 8. Dezember 2007, BGBl I S. 2808 sowie BRDrucks 222/07.

6Vgl. BVerfGE 65, 1 (12, 47); VO (EG) Nr. 763/2008, a.a.O., Erwägung Nr. 2.

7Vgl. BVerfGE 65, 1 (3).

8Vgl. BVerfGE 64, 67 (68); 65, 1 (35).

9Vgl. BVerfGE 65, 1 (4).

10Dazu: Abel, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 2.7. Rn. 6.

11 George Orwell, 1984; siehe ferner: Simitis, in: Simitis (Hrsg.), BDSG, 6. Aufl. 2006, Einleitung Rn. 28.; Benda, in: Leibholz u.a. (Hrsg.), Festschrift für Geiger, 1974, S. 23 ff.

12Vgl. BVerfGE 65, 1 (41); dazu: Trute, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 2.5 Rn. 7 ff.; Albers, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2008, § 22 Rn. 58 ff.

13Vgl. jüngst: BVerfGE 119, 1 (24) - "Esra".

14Vgl. BVerfGE 27, 1 (6). Weitere Entscheidungen: BVerfGE 27, 344 (350 f.); 32, 373 (379); 44, 353 (372 f.).

15Vgl. BVerfGE 65, 1 (42).

16Vgl. BVerfGE 65, 1 (43).

17 Nur „zum Teil“ deshalb, weil das Bundesverfassungsgericht in der Folge daran festgehalten hat, dass wegen der besonderen Nähe zur Menschenwürde ein Kernbereich privater Lebensführung absolut geschützt bleibt, vgl. BVerfGE 109, 279 (310 ff.); BVerfGE 119, 1 (29).

18Vgl. BVerfGE 65, 1 (45); Trute, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 2.5 Rn. 10.

19. BVerfGE 65, 1 (42 f.); zuletzt erneut bestätigt durch: BVerfG, Urteil vom 27. Februar 2008, 1 BvR 370/07 und 1 BvR 595/07 - JURIS -, Rn. 180.

20Forderungen wie „Meine Daten gehören mir“ (vgl. Künast, ZRP 2008, S. 201) sind daher fragwürdig.

21. BVerfGE 65, 1 (44).

22Siehe dazu: Simitis, in: Simitis (Hrsg.), BDSG, 6. Aufl. 2006, Einleitung Rn. 30 ff.

23Vgl. BVerfGE 65, 1 (44).

24Vgl. BVerfGE 65, 1 (44).

25Vgl. BVerfGE 65, 1 (44).

26Vgl. BVerfGE 65, 1 (44).

27Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20. Dezember 1990, BGBl I S. 2954; Simitis, in: Simitis (Hrsg.), BDSG, 6. Aufl. 2006, Einleitung Rn. 52 ff.; Abel, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, 2.7. Rn. 40 ff. Das erste Datenschutzgesetz weltweit war übrigens das LDSG von Hessen aus dem Jahr 1970, Hess. GVBl 1970 S. 652.

28Über keine Datenschutzvorschriften verfügten zuvor zum Beispiel: Italien, Griechenland und Spanien, vgl. Simitis, in: Simitis (Hrsg.), BDSG, 6. Aufl. 2006, Einleitung Rn. 205.

29Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 vom 23. November 1995, S. 31. Siehe auch die später erlassenen bereichsspezifischen Richtlinien wie: Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember

1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, ABl. Nr. L 24 vom 30. Januar 1998, S. 1 sowie die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für die elektronische Kommunikation), ABl. Nr. L 201 vom 31. Juli 2002, S. 37.

30 Vgl. 10. Erwägungsgrund der Richtlinie 95/46/EG; Abel, in: Roßnagel (Hrsg.), Handbuch Da-enschutzrecht, 2003, 2.7. Rn. 45 f.; Simitis, in: Simitis (Hrsg.), BDSG, 6. Aufl. 2006, Einleitung Rn. 205 ff.

31Vgl. Wettner, Die Amtshilfe im Europäischen Verwaltungsrecht, 2005, S. 45 ff.

32BGBl II vom 23. Juli 1993 S. 1013.

33Vgl. Europol, Europol-Übereinkommen, ABl. Nr. C vom 27. November 1995, S. 2 ff.; Eurojust, Beschluss des Rates vom 28. Februar 2002, ABl. Nr. L 63 vom 6. März 2002, S. 1; sowie die Gemeinsame Visa-, Asyl- und Einwanderungspolitik nach Titel IV des EG-Vertrages.

34Vgl. zum Beispiel das Schengener Informationssystem, Europol, das Zollinformations-System oder Eurodac, dazu: Simitis, in: Simitis (Hrsg.), BDSG, 6. Aufl. 2006, Einleitung Rn. 233 ff.; J. Hofmann, Rechtsschutz und Haftung im Europäischen Verwaltungsverbund, 2004, S. 142 ff., 232 ff. und 345 ff.

35Vgl. für den die „Erste Säule“ betreffenden Teil des Schengener Informationssystems: Art. 40 ff. der Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II, ABl. Nr. L 381 vom 28. Dezember 2006, S. 4) und für den die „Dritte Säule“ betreffenden Teil des SIS II: Art. 56 ff. des Beschlusses des Rates 2007/533/JI vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), ABl. Nr. L 205 vom 7. August 2007, S. 63. Siehe auch: Simitis, in: Simitis (Hrsg.), BDSG, 6. Aufl. 2006, Einleitung Rn. 233 ff.; J. Hofmann, Rechtsschutz und Haftung im Europäischen Verwaltungsverbund, 2004, S. 142 ff., 232 ff. und 345 ff. Am 27. und 28. November 2008 hat der Rat der Innen- und Justizminister zudem einen Rahmenbeschluss für den Datenschutz im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verabschiedet, vgl. Pressemitteilung 16325/08 sowie Rats-dokument 9260/08 sowie KOM(2005) 475.

36Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. Nr. L 8 vom 12. Januar 2001, S. 1.

37Dazu: Albers, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Band II, 2008, § 22 Rn. 42 ff.; Rengeling/Szczekalla, Grundrechte in der Europäischen Union, 2004, § 16 Rn. 675 f.

38Vgl. dort Art. 8, ABl. Nr. C 303 vom 14. Dezember 2007, S. 1.

39Vgl. Roßnagel, MMR 2007, S. 16 ff.; Kloepfer, DÖV 2003, S. 221 ff.

40. § 29 VwVfG, dazu: Sydow, NVwZ 2008, S. 481 ff.

41 Vgl. Umweltinformationsgesetz vom 22. Dezember 2004, BGBl I S. 3704; Verbraucherinformationsgesetz vom 5. November 2007, BGBl I S. 2558; Informationsfreiheitsgesetz vom 5. Sep-tember 2005, BGBl I S. 2722.

42Vgl. Reinhart, DÖV 2007, S. 18.

43Vgl. Art. 255 EG-Vertrag; Art. 42 der Charta der Grundrechte der Europäischen Union, ABl. Nr. C 303 vom 14. Dezember 2007, S. 1, oder die Umweltinformations-Richtlinie 2003/4/EG vom 28. Januar 2003, ABl. Nr. L 41 vom 14. Februar 2003, S. 26.

44Freedom of Informations Act von 1966, vgl. BTDrucks 15/4493, S. 6.

45Vgl. Schoch, DÖV 2006, S. 1 (5); Gröschner, VVDStRL 64 (2004), S. 344 (346).

46Vgl. § 12 Informationsfreiheitsgesetz.

47Vgl. Gröschner, VVDStRL 64 (2004), S. 344 (353); Masing, VVDStRL 63 (2004), S. 377 (384).

48Vgl. BTDrucks 15/4493, S. 6; Roßnagel, MMR 2007, S. 16 (18); Schoch, DÖV 2006, S. 1 (2 f.). Siehe auch bereits: BVerfGE 7, 198 (208).

49Vgl. Roßnagel, MMR 2007, S. 16 (18); Schoch, DÖV 2006, S. 1 (2 f.).

50Vgl. BVerfGE 65, 1 (43).

51Vgl. BVerwG, NJW 2002, S. 1815 ff. - "Fall Helmut Kohl".

52Roßnagel, MMR 2007, S. 16 (19 f.); Masing, VVDStRL 63 (2004), S. 377 (410 ff.).

53Das heißt, die Überwachung von Gesprächen außerhalb (vgl. § 100c Abs. 1 Nr. 2 StPO in der Fassung des Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität vom 15. Juli 1992, BGBl I S. 1302) und innerhalb von Wohnungen (vgl. Art. 13 Abs. 3 bis 6 GG; § 100c in der Fassung des Gesetzes zur Verbesserung der Bekämpfung der Organisierten Kriminalität vom 4. Mai 1998, BGBl I S. 845, dazu: BVerfGE 109, 279).

54Vgl. das Gesetz zur Beschränkung des Brief-, Post- und Fermmeldegeheimnisses vom 13. August 1968, BGBl I S. 949 in der Fassung des Begleitgesetzes zum Telekommunikationsgesetz vom 17. Dezember 1997, BGBl I S. 3108, vgl. dazu: BVerfGE 100, 313.

55Vgl. dazu: BVerfGE 115.

56 Vgl. dazu: BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 – 1 BvR 370/07 und 1 BvR 595/07 –, JURIS.

57Vgl. Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarverarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. Nr. L 105 vom 13. April 2006, S. 54; vgl. dazu: Beschlüsse des Ersten Senats vom 11. März 2008 und 28. Oktober 2008 – 1 BvR 256/08 –.

58Vgl. BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 – 1 BvR 370/07 und 1 BvR 595/07 –, JURIS Rn. 202; Urteil des Ersten Senats vom 11. März 2008 – 1 BvR 2074/05 und 1 BvR 1254/07 –, JURIS Rn. 169.

59Vgl. BVerfGE 115, 320 (360), siehe auch: Hohmann-Dennhardt, RDV 2008, S. 1 ff.; Buermeyer, RDV 2008, S. 8 ff.

60Vgl. BVerfGE 115, 320 (360).

61Vgl. BVerfGE 115, 320 (360 ff.); Urteil des Ersten Senats vom 11. März 2008 – 1 BvR 2074/05 und 1 BvR 1254/07 –, JURIS Rn. 172.

62Vgl. BVerfGE 6, 32 (41); 27, 1 (6); 109, 279 (311 ff.).

63Vgl. BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 – 1 BvR 370/07 und 1 BvR 595/07 –, JURIS Rn. 262 ff.

64Vgl. BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 – 1 BvR 370/07 und 1 BvR 595/07 –, JURIS Rn. 152 ff. Dazu: Hoffmann-Riem, JZ 2008, S. 1009 ff.; Petri, DuD 2008, S. 443 ff.

65Vgl. BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 – 1 BvR 370/07 und 1 BvR 595/07 –, JURIS Rn. 183.

66Vgl. Hoffmann-Riem, JZ 2008 S. 1009 (1013, 1018).

67Besonders häufig kommt es nämlich "nur" zu „handwerklichen Fehlern“ des Gesetzgebers. Dies gilt insbesondere, wenn man berücksichtigt, dass die betreffenden Gesetze häufig wegen Verletzung des Bestimmtheitsgrundsatzes beanstandet wurden: vgl. BVerfGE 118, 168; BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 – 1 BvR 370/07 und 1 BvR 595/07 –, JURIS Rn. 190 ff.; Urteil des Ersten Senats vom 11. März 2008 – 1 BvR 2074/05 und 1 BvR 1254/07 –, JURIS Rn. 93 ff.

68Vgl. BVerfGE 65, 1 (42).

69Vgl. Nachweise bei Hoffmann-Riem, JZ 2008, S. 1009 (1010); zur Arbeitnehmerüberwachung vgl. Schierbaum, Der Personalrat 2008, S. 180 ff.

70Vgl. auch: Steidle/Pordesch, DuD 2008, S. 324 ff.

71Vgl. auch Hoffmann-Riem, JZ 2008, S. 1009 (1011 f., 1013); ders., AöR 123 (1998), S. 513 (524 ff.); Petri, DuD 2008, S. 443 (446 f.); Hassemer, FAZ vom 5. Juli 2007, S. 6; Ronellenfitsch, RDV 2008, S. 55 (58).

72Gesetz zur Änderung des Bundesdatenschutzgesetzes vom 29. Juli 2009, BGBl I S. 2254; Art. 5 des Gesetzes zur Umsetzung der Verbraucherkreditrichtlinie, des zivilrechtlichen Teils der Zahlungsrichtlinie sowie zur Neuordnung der Vorschriften über das Widerrufs- und Rückgaberecht vom 29. Juli 2009, BGBl I S. 2355; Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14. August 2009, BGBl I S. 2814; vgl. zum Ganzen: Gola/Klug, NJW 2009, S. 2577.

73Gesetz zur Änderung des Bundesdatenschutzgesetzes vom 29. Juli 2009, BGBl I S. 2254; BTDrucks 16, 10529.

74Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14. August 2009, BGBl I S. 2814; BTDrucks 16/12011; BTDrucks 16/13657; siehe auch: Gola/Klug, NJW 2009, S. 2577 (2579 ff.).

75Vgl. dazu: Thomas Öchsner, "Mit aller Macht für den Arbeitnehmer", www.sueddeutsche.de vom 3. September 2009.

76Zitiert nach Ulrich Clauß, Welt vom 22. Juli 2009: „Die 'Zensurdebatte' im Internet wird immer absurder - Es gibt kein Grundrecht auf Hass“.