Burkhard Hirsch

Zu den Anforderungen eines modernen Datenschutzes*

Datenschutz und die sich aus ihm ergebenden Rechte des Einzelnen stehen heutzutage in einem Spannungsfeld von Sicherheit und Freiheit. Um der Freiheit und Privatheit willen sind Grenzen der staatlichen und privaten Datenverarbeitung zu fordern, sei es nach nationalem Recht oder nach dem Recht der Europäischen Union.

I. Gesellschaftliche und gesetzgeberische Entwicklungslinien im Umgang mit dem Datenschutz

Datenschutz war einst anrüchig. Er galt als Täterschutz. „Wer nichts zu verbergen hat, der hat auch nichts zu befürchten". Der Staat solle künstlich dumm gemacht werden. Dabei wollten wir ihn nur daran hindern, allwissend zu werden. Es wurde streitlos akzeptiert, dass das Bundesverfassungsgericht der staatlichen Verwaltung einen „Kernbereich exekutiver Eigenverantwortung"[1] einräumte, der selbst parlamentarischen Untersuchungsausschüssen nicht offenbart werden muss, wenn das die staatliche Entscheidungsfähigkeit beeinträchtigen könnte. Aber es führte zu langen Debatten, als das Bundesverfassungsgericht einen absolut unantastbaren „Kernbereich privater Lebensführung"[2] erklärte.

Als Reisende mit ihren Handys ganze ICE-Abteile mit ihrem Privatkram unterhielten oder junge Leute im Fernsehen ihre Privatheiten ausbreiteten, wurde das erleichtert als das Ende des Datenschutzes und der Privatheit gewertet. Aber wird denn das Eigentumsrecht obsolet, wenn es Leute gibt, die ihre Wertsachen leichtfertig derelinquieren? So hat es denn manche Kritiker überrascht, dass sich plötzlich zehntausende junger Leute an den Verfassungsbeschwerden gegen den sog. Bundestrojaner, gegen die Vorratsdatenspeicherung und gegen das Datenvorratssystem ELENA beteiligten. Da empörten sich ganz normale Bürger über Verletzungen der privaten Vertraulichkeit, von denen sie selbst betroffen werden. Andere erkannten, dass bis dahin geschmähte Verschlüsselungstechniken für Staat und Wirtschaft notwendig sind, um die Ausspähung oder Lähmung ganzer Netze mit höchst empfindlichen politischen und wirtschaftlichen Folgen zu verhindern. Wir sind also mitten in einer technischen Entwicklung, die die Welt verändert hat und die sie weiter verändern wird, ob wir wollen oder nicht.

Ich habe in Nordrhein-Westfalen Mitte der 70er Jahre die Datenverarbeitung in der staatlichen und kommunalen Verwaltung und in der Polizei nach Kräften gefördert und ausgebaut. Eine rationelle Verwaltung und eine wirksame Kriminalitätsbekämpfung ohne Datenverarbeitung sind unmöglich. Das war so und das wird so bleiben. Aber wir müssen aufpassen, dass unser Staat nicht den Charme eines blankgeputzten Räderwerks entwickelt. Wir müssen verstehen, warum das Bundesverfassungsgericht in der Vor-

* Der Beitrag basiert auf einem Vortrag, der im Forum Justiz am 24. Januar 2011 in Erfurt gehalten wurde. Der Vortragsstil wurde bewusst beibehalten.

1 BVerfGE 67, 100 ff, 139.

2 BVerfGE 109, 219 ff.

ratsdaten-Entscheidung warnend erklärt, dass die lückenlose Erfassung der Freiheitswahrnehmung der Bürger der verfassungsrechtlichen Identität unseres Staates widersprechen würde und dass die Politik verpflichtet ist, diesen Gedanken in der Europäischen Union wirksam zu vertreten.[3]

Ich möchte an die Bemerkung des Kirchenvaters Augustinus erinnern, dass der eigentliche Unterschied zwischen einem Staat und einer organisierten Räuberbande die Gerechtigkeit ist.[4] Uns verbindet mit unserem Staat nicht seine pure Durchsetzungsfähigkeit, seine Effektivität, die „Herrschaftsgewalt kraft eigenen Rechts", wie einst Laband lehrte, sondern seine Gerechtigkeit und damit die Freiheit, die uns sein gutes Recht gewähren und sichern soll.

Dieser Zusammenhang ist in der Terrorismus-Debatte völlig verdrängt worden, die die Innenpolitik der Bundesrepublik seit Anfang der vergangenen 80er Jahre beherrscht und bei der das Attentat vom 11. September 2001 auch in Europa wie ein Brandbeschleuniger gewirkt hat. Diese Debatte wird fast ausschließlich unter dem Gesichtspunkt der „Sicherheit", mit wahltaktischer Berechnung, mit der bewussten Erfindung einer die Wirklichkeit verharmlosenden Sprache und mit der Forderung geführt, sofort immer neue, natürlich stets unverzichtbare Gesetze zu beschließen. Das hat uns eine Vielfalt intensiver staatlicher Kontroll- und Eingriffsrechte beschert, an die wir noch vor wenigen Jahren nicht zu denken gewagt hätten. Es gilt nicht dem Anfang, sondern dem bitteren Ende zu wehren, haben zwei Verfassungsrichterinnen bei der Entscheidung über den Großen Lauschangriff formuliert.

Wir erleben die Einführung einer verharmlosenden Sprache. Da mutierte die „Wanze" zum „Großen Lauschangriff" und schließlich zum aseptischen „Abhören des nichtöffentlich gesprochenen Wortes mit technischen Mitteln ohne Kenntnis des Betroffenen".[5] Im LuftSiG wurden der Abschuss eines zivilen Passagierflugzeugs und die Tötung aller Insassen als „unmittelbare Einwirkung mit Waffengewalt auf ein Luftfahrzeug" bezeichnet. Menschen kommen in dieser Formel nicht mehr vor. „Trojaner" nannte man die technische Möglichkeit, einen privaten PC heimlich zu verwanzen, seinen Inhalt auszulesen oder zu verändern und jede weitere Benutzung durch einen „key logger" mitzulesen. Der Bonner Staatsrechtler Günther Jacobs forderte die Einführung eines „Feindstrafrechts" und wollte damit in Wirklichkeit den Staat gegen seine „Feinde" vom lästigen geschriebenen Polizei- und Strafprozeßrecht befreien. Aus dem „finalen Todesschuss" wurde der „Rettungsschuss". Das so sympathische Wort „Sicherheitsarchitektur" soll verstärkte staatliche Eingriffs- und Kontrollrechte umschreiben. Die Erfindung des Begriffes „passive Bewaffnung" ist geradezu von genialer Hinterhältigkeit. Ich könnte die Aufzählung fortsetzen.

Die Vielzahl neuer Kontrollen und Möglichkeiten – durch Wanze, Trojaner und Mikrokameras, über Bankkonten, Postdienste und Passagierdaten, die Rasterfahndung von Millionen moslemischer Einwohner der Bundesrepublik, das anlasslose Scannen von KFZ-Kennzeichen, die lückenlose Überwachung aller telekommunikativen Auslands-

3 BVerfG NJW 2010, 833 ff, Rdnr. 218.

4 vgl. R. Weber-Fas, Der Staat. (Neske 1977) Bd. 1, S. 96. „Was anders sind also Reiche, wenn ihnen Gerechtigkeit fehlt, als große Räuberbanden?".

5 Dem Innenministerium war das von ihm erfundene Wort Lauschangriff zu polemisch geworden. Der damalige BMI Kanther nannte das „Abhören von Ganovenwohnungen". Aber ab wann ist man ein „Ganove"?

kontakte aller Bürger und ihre computergesteuerte Auswertung nach Stichworten, ständig zunehmende Telefonkontrollen einschließlich der Standortdaten und der sog. Quellen-TKÜ, gemeinsame Verdachtsdateien von Polizei und Nachrichtendiensten, die Inhaltskontrolle aller Telekommunikationskontakte mit Bundesbehörden, die Vorratsdatenspeicherung aller Telekommunikationsdaten aller Europäer – und die Flut neuer Bundes- und Landesgesetze brauche ich eigentlich nicht aufzuzählen. Dabei würde man allenfalls von der CSU-Landesgruppe überboten, die diese Kette nun erneut verlängern will[6] und dabei völlig außer Acht lässt, dass wir schon heute bei Telefonüberwachungen und Kontoabfragen geradezu traumhafte jährliche Steigerungsraten von 20 bis 30 % haben.

Dem Anti-Terrorismusgesetz von 1976 folgte das Gesetz zur Bekämpfung des Terrorismus von 1986, das umfangreiche Gesetz zur Bekämpfung der Organisierten Kriminalität von 1992, das Verbrechensbekämpfungsgesetz von 1994, das Gesetz zur Verbesserung der Bekämpfung der Organisierten Kriminalität von 1998 mit der Einführung des ‚Großen Lauschangriffs', die Terrorismusbekämpfungsgesetze von 2002 und 2003 (sog. Schily I und II) und das Terrorismusbekämpfungsergänzungsgesetz von 2006 mit jeweils umfangreichen Änderungen des Straf- und Strafprozessrechts, des Passgesetzes, mit äußerst rücksichtslosen Verschärfungen des Ausländerrechts und mit immer weitergehenden Eingriffsbefugnissen der Nachrichtendienste. Das wurde ergänzt durch Veränderungen der Polizei- und Verfassungsschutzgesetze des Bundes und der Länder, durch verschiedene Strafrechtsänderungsgesetze, das Telekommunikationsgesetz von 1996, seine Novellierung und das Zuwanderungsgesetz von 2004, das Luftsicherheitsgesetz von 2005, das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen von 2007 und die Novelle zum BKAG von 2008.[7]

Das gemeinsame Ziel all dieser Maßnahmen ist es, schon das Vorbereitungsstadium zur Straftat zu machen und die Prävention auf das unbegrenzbare „Vorfeld" zu erstrecken. Man will möglichst frühe Informationen über Handlungen, Planungen und Kommunikationen nicht nur verdächtiger Personen gewinnen, sondern auch von Personen, von denen die Polizei annimmt, dass sie zukünftig Straftaten vorhaben könnten, die Überwachung ihres persönlichen Umfelds und schließlich auch völlig anlasslose Kontrollen, um möglichst vor der Tat am Tatort zu sein. Vorbeugung kennt keine Grenzen. Für den, der Angst hat, raschelt es überall.

Wenn der Staat das Recht bekommen soll, auf die Vermutung böser Gedanken hin oder gar ohne konkreten Anlaß in Grundrechte einzugreifen, gerade dann, wenn er auf den leisen Sohlen des gutmeinenden Beschützers daherkommt, dann ist äußerste Vorsicht geboten. Der damalige Innenminister Wolfgang Schäuble fühlte sich schon 1996 durch die Verfassung behindert und disqualifizierte sich selbst mit der Bemerkung: „Die Verfassung ist immer weniger das Gehege, in dem sich die demokratisch legitimierte

6 CSU-Landesgruppe, „Sicher in Deutschland leben." 35. Klausurtagung Wildbad Kreuth vom 5.-7.1.2011.

7 Eine Evaluierung der Wirksamkeit dieser Gesetze steht aus bzw. hat beim sog. Großen Lauschangriff zu höchst ernüchternden Ergebnissen geführt. Schily II läuft im Januar 2012 aus.

Gesetzgebung entfalten kann, sondern immer stärker die Kette, die den Bewegungsspielraum der Politik lahmlegt."[8]

II. Der Datenschutz zwischen Privatheit und öffentlichem Interesse

Die Bundesrepublik hat die Grenze zum Präventionsstaat erreicht oder überschritten. Sie begibt sich damit auf ein gefährliches Gebiet. In den letzten 6 Jahren sind allein beim Bundesverfassungsgericht 14 Verfassungsbeschwerden im Bereich der Innenpolitik ganz oder teilweise erfolgreich gewesen, eine in der deutschen Verfassungsgeschichte einmalige Serie.

Es sind die Entscheidungen zum Großen Lauschangriff[9] und zu den Befugnissen des Zollkriminalamts,[10] zur präventiven Telefonüberwachung nach dem niedersächsischen Polizeirecht,[11] zur Rasterfahndung,[12] zur Pressefreiheit mit dem Cicero-Urteil,[13] zur Auskunft über Telefonverbindungsdaten von Journalisten,[14] zum Luftsicherheitsgesetz,[15] zur Beschlagnahme von Datenträgern in Anwaltskanzleien,[16] zur Beschlagnahme von Kommunikationsdaten einer Richterin,[17] zur Abfrage von Kontostammdaten,[18] zum Europäischen Haftbefehl,[19] zum sog. Scannen von KFZ-Kennzeichen,[20] zur Online-Durchsuchung von PCs[21] und zur Vorratsdatenspeicherung,[22] zur Durchsuchung einer Redaktion.[23] Zum bayerischen Polizeiaufgabengesetz ist eine Kostenentscheidung zugunsten der Beschwerdeführer ergangen.[24] Zum BKA-Gesetz,[25] zu einer Reihe von Bestimmungen der StPO und zu ELENA[26] sind Verfassungsbeschwerden anhängig. Ein Teil dieser Verfassungsbeschwerden ist von vielen zehntausenden Beschwerdeführern unterstützt worden. Es hat mich verwundert, dass liberale Abgeordnete in den 80er Jahren begannen, sich mit einem „Paradigmenwechsel" zu rechtfertigen, dass nun der Staat den Bürger zu schützen habe, obwohl das nun schon seit über 500 Jahren – seit dem Mainzer Ewigen Landfrieden von 1495 – völlig unbestritten ist. Und man zitierte Wilhelm von Humboldt`s Ideen zu einem Versuch, die Grenzen der Wirksamkeit des Staates

8 Schäuble: "Weniger Demokratie wagen? Die Gefahr der Konstitutionalisierung der Tagespolitik" in FAZ vom 13.9.1996, S. 12.
9 BVerfGE 109, 279 ff.
10 BVerfGE 110, 33 ff.
11 BVerfGE 113, 348 ff.
12 BVerfGE 115,320 ff.
13 BVerfGE 117, 244 ff.
14 BVerfGE 107, 330 ff.
15 BVerfGE 115, 118 ff.
16 BVerfGE 113, 29 ff.
17 BVerfGE 105, 365 ff, 115, 166 ff.
18 BVerfGE 118, 168 ff.
19 BVerfGE 113, 273 ff.
20 BVerfGE 120, 378 ff.
21 BVerfGE 120, 274 ff.
22 BVerfG NJW 2010, 833 ff.
23 BVerfG Beschluss 1 BvR 1739/04 vom 10.12.2010
24 BVerfG Beschluss 1 BvR 661/06 vom 4.11.2010
25 BKA-Gesetz i. d. F. vom 25.12.2008, BGBl. I 3083 ff.
26 ELENA-VerfahrensG vom 28.3.2009, BGBl. I 634 ff.

zu bestimmen: „Es ist keine Freiheit ohne Sicherheit“. Man sollte ihn nicht zitieren, ohne ihn gelesen zu haben. Denn natürlich war er nicht so töricht anzunehmen, dass man mit immer mehr Sicherheit auch immer mehr Freiheit schaffe, im Gegenteil. Selbst bei der Prävention zieht Humboldt dem Staat enge Grenzen – um der Freiheit willen.[27]

Natürlich muss der Staat den Bürger schützen. Aber er darf nur die Mittel einsetzen, die ihm die Verfassung dazu gibt. Es ist das Verdienst des Bundesverfassungsgerichts, gerade bei seiner Volkszählungsentscheidung von 1983[28] das Recht auf informationelle Selbstbestimmung mit der überlieferten Freiheitsidee unserer Rechtstradition zu verbinden. Es betont, dass die informationelle Selbstbestimmung nicht allein zur Förderung des individuellen, privaten Wohls gewährleistet werde. Sie ist „eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen demokratischen Gemeinwesens.“[29] Das ist der Grundgedanke einer langen kontinuierlichen Rechtsprechung des Gerichts, die schon frühzeitig die Notwendigkeit der Mitwirkungsmöglichkeit des Bürgers für den politischen Willensbildungsprozess hervorgehoben und die Notwendigkeit der „Chance zur Identifikation“ mit dem Staat erkannt hat.[30]

Dazu gehört nach meiner Überzeugung auch eine möglichst großzügige Regelung der Informationsfreiheit, also die frühzeitige Einbeziehung der Bürger bei großflächigen Planungen und ein Akteneinsichtsrecht, das nur drei Grenzen kennen sollte: die Handlungsfähigkeit bei noch nicht getroffenen Entscheidungen, die aktuelle Gefahrenabwehr und Strafverfolgung sowie die Rechte dritter Personen.[31]

Das Volkszählungsurteil hat das Grundrecht auf Datenschutz nicht erfunden, sondern war die konsequente Weiterentwicklung einer Rechtsprechung, die der Menschenwürde, der Privatheit und der Selbstbestimmung den Vorrang vor Effektivität und Perfektionismus gab.[32] Auch die Bezeichnung „informationelles Selbstbestimmungsrecht“ wurde schon lange Jahre vor der Entscheidung von Steinmüller und anderen Autoren geprägt[33] und ist sogar schon einmal in einem Urteil des Bundesverfassungsgerichts verwendet worden.[34] Der Gedanke eines allgemeinen Rechts auf Datenschutz und Privatheit ist übrigens von den amerikanischen Juristen Warren, Cooley und Brandeis schon 1890 publiziert worden, das Recht auf „privacy“ und das „right to be let alone“,

27 Sicherheit bedeutete für ihn „die Gewißheit der gesetzmäßigen Freiheit“. Darum könne zur Erhaltung der Sicherheit „das nicht notwendig sein, was gerade die Freiheit und mithin auch die Sicherheit aufhebt“. Wilhelm v. Humboldt, Ideen zu einem Versuch, die Grenzen der Wirksamkeit des Staates zu bestimmen. Reclam 1991, S. 118 f.

28 BVerfGE 65, 1 ff, vom 15.12.1983.

29 Vgl. BVerfGE 65, 43; vgl. dazu auch Denninger, Der gebändigte Leviathan, NOMOS 1990, S. 375 ff, 381.

30 Vgl. Denninger a.a.O. S. 381, und BVerfGE 5, 85, 205; 20, 56, 103; 40, 237, 251.

31 Vgl. dazu das IFG vom 5.9.2005 (BGBl. I 2722), und das IFG NRW vom 27.11.2001 (GVBl 2005, 351).

32 Vgl. BVerfGE 54,148(153) Eppler; E 27, 1 Mikrozensus; E 27, 344(350) Scheidungsakten; E 32, 373(379) Arztkartei; E 34, 238(245) Heiml. Tonbandaufnahme; E 34, 238 (246) Recht am gesprochenen Wort; E 34, 269 (282) Soraya; E 56, 37(41) Selbstbezichtigung; E 63, 131(142) Gegendarstellung.

33 Von Steinmüller, Mallmann, Schatzschneider, Podlech, Simon und Taeger, vgl. die Nachweise bei Denninger, a.a.O. S.378,379.

34 BVerfGE 57, 170 ff, 201.

sind Gedanken, die sich im Common Law allerdings erst allmählich, aber doch erheblich schneller durchsetzten[35] als bei uns.

Dieser strukturelle Gegensatz zwischen Privatheit und informationeller Selbstbestimmung auf der einen und dem Interesse des Staates an größerer Effektivität der Verwaltung, der Strafverfolgung und der Prävention auf der anderen Seite ist durch zwei Entwicklungen drastisch verschärft worden: durch die technische Entwicklung der Datenverarbeitung und durch die sich aus ihr ergebenden ungeahnten ökonomischen Interessen.

Konrad Zuse hat mit seinem Z 3, dem 1941 gebauten ersten Computer, eine technische Entwicklung eingeleitet, die unser Leben ebenso veränderte wie die Erfindung des Rades. Wir können nahezu unbegrenzte Datenmengen unbegrenzt lange speichern, sie aus ihren Zusammenhängen lösen, nach Belieben miteinander verbinden, sie zu Entscheidungsgrundlagen machen, über Grenzen hinweg abrufen. Der PC ist zu einem ausgelagerten Gehirn geworden, das nichts vergisst, mit dem wir schreiben, telefonieren, Nachrichten austauschen, Geschäfte abwickeln und unsere Bankkonten führen. Er ist Ablage, Briefkasten, Terminkalender, Adressregister, unsere Erinnerung. Seine Speicherkapazität wird durch Auslagerung an Provider, durch das sog. Cloud-computing[36] unbegrenzt erweitert.

Aus unseren Handys werden internetfähige Smartphones. Sie werden demnächst wie Video-Anlagen mit einem Gesichtserkennungsprogramm und Geo-Datensystemen verbunden werden können. Sie werden uns mitteilen, wem wir begegnen und was über ihn gespeichert ist. Sie werden uns sagen, wer in dem Haus wohnt, auf das wir die integrierte Webcam richten. Man wird diese Informationen unbemerkbar in die Brille einspiegeln können, in der sich die Webcam befindet, die mit dem Smartphone verbunden ist. Der Anwendungsbereich sog. RFID-Chips, die über Meter hinweg berührungsfrei ausgelesen werden können, ist unübersehbar. Und mit jeder neuen Anwendungsmöglichkeit wächst das Interesse von Staat, Unternehmen und Bürgern an den Daten für heilige und unheilige Zwecke aller Art.

Bei den Unternehmen geht es nicht nur um die Ersetzung menschlicher Arbeitskraft oder eine bessere Steuerung der Materialflüsse. Es geht um die heimliche Sammlung individueller persönlicher Daten über Gebrauchsgewohnheiten oder Interessen für Werbezwecke, für die Bewertung der Kreditwürdigkeit eines potentiellen Kunden bis hin zu schwarzen Listen. Es geht auch um Leistungskontrolle, allgemeine Verhaltenskontrolle und darum, die Daten, die in StudiVZ, Facebook oder andern sozialen Netzwerken gespeichert sind, für Personalentscheidungen von der Einstellung bis hin zur Entlassung zu nutzen. Darum sind die politischen Widerstände gegen ein Arbeitnehmerdatenschutzgesetz enorm.

Für den Bürger ist entscheidend, dass er sich diesen Entwicklungen nicht entziehen kann, wenn er nicht allmählich als etwas komisch gelten und zum Robinson werden will. Die Datenschutzgesetzgebung hat diese Entwicklungen nicht gesteuert, sondern ist ihnen eher zögernd gefolgt. Es ging nicht immer darum, die Datennutzung zu begrenzen, sondern die jeweils bestehende Praxis zu legitimieren. In einzelnen Länder-

35 Zitiert nach Bull, Datenschutz oder die Angst vor dem Computer, Piper 1984, S. 78

36 Datenverarbeitung über Internet, bei der sich Software, Ressourcen und Informationen auf anderen irgendwo stationierten Servern befinden.

verfassungen, beginnend mit Hessen und Nordrhein-Westfalen konnten wir den Datenschutz relativ früh zum Verfassungsrecht erheben. Im Grundgesetz sind wir immer wieder gescheitert, während die Aufnahme in Art. 8 der Europäischen Menschenrechtskonvention und Art. 8 der Grundrechtecharta der Europäischen Union ohne Debatte akzeptiert wurde. Die Europäische Datenschutzrichtlinie[37] hat im Bundestag keine gesteigerte Beachtung gefunden, obwohl die Praxis des Datenschutzes gerade in der Überschreitung der nationalen Grenzen einem besonderen Problem begegnet. Der Datenschutz richtet sich gem. § 1 Abs. 5 BDSG auch bei Datenerhebung und Verarbeitung nach dem Recht des Landes, in dem der Provider seinen Sitz hat.[38]

III. Die Rechtsprechung des Bundesverfassungsgerichts zu datenschutzrechtlichen Fragestellungen im Einzelnen

Das Bundesverfassungsgericht hat den Gesetzgeber wiederholt aufgefordert, aus der sprunghaften technischen Entwicklung gesetzgeberische Konsequenzen für das notwendige Gleichgewicht zwischen neuen Eingriffsmöglichkeiten und traditionellen Bürgerrechten zu ziehen.[39] Das blieb erfolglos und führte schließlich zu den Entscheidungen des Gerichts, die wir nun etwas näher betrachten müssen, weil sie Grundrechte einführen, die auch den Landesgesetzgeber binden.

1. Das Volkszählungsurteil

Das Volkszählungsurteil des Bundesverfassungsgerichts von 1983 erklärt das informationelle Selbstbestimmungsrecht als subsidiär gegenüber den geschriebenen Persönlichkeitsrechten. Es wird aus Art. 1 und 2 GG hergeleitet und gibt jedermann das Recht, „selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden."[40] Dadurch wird ein lückenloser Schutzmechanismus etabliert, der auch bei neuen technischen Entwicklungen gilt.

Das Selbstbestimmungsrecht kann durch Gesetz eingeschränkt werden. Es muss aber ein normenklares, präzise formuliertes Gesetz sein, das dem Verhältnismäßigkeitsgrundsatz entsprechen muss. Die Freiheit des Einzelnen soll nicht im Ermessen der Verwaltung liegen. Darum sollen „der Anlass, der Zweck, und die Grenzen des Eingriffs bereichsspezifisch, präzise und normenklar festgelegt werden."[41] Das Gericht definiert, dass schon die Erhebung personenbezogener Daten und nicht erst ihre weitere Verarbeitung in das Grundrecht eingreift. Es verlangt die Zweckbindung der Daten, die nicht

37 Richtlinie 95/46/EG vom 24.10.1995 (ABl. L 281 vom 23.11.1995, S. 31).

38 Es sei denn, dass er seinen Sitz in einem Drittland oder in der Bundesrepublik eine Niederlassung hat, die die Datenverarbeitung vornimmt. Bei der Behandlung des sog. Swift-Abkommens mit den USA über die Übermittlung von Bankdaten an amerikanische Behörden ist in der deutschen Diskussion völlig unbeachtet geblieben, dass das US -amerikanische Datenschutzrecht nur für amerikanische Staatsangehörige gilt.

39 BVerfGE 90, 145 (191); 112, 304 (316 f.).

40 BVerfGE 65, 1 (43); 118, 168 (184).

41 BVerfGE 100, 313 (359 f, 372); sehr eingehend 110, 33 ff. und 120, 274 (315 ff.).

zu beliebiger späterer Verwendung auf Vorrat erhoben und aufbewahrt werden dürfen. Es verlangt die definitive Trennung von Statistik und vollziehender Verwaltung.

Insbesondere der Begriff der Verhältnismäßigkeit eines Eingriffs wurde z. T. erst in der folgenden Rechtsprechung immer präziser definiert. Je massiver der Eingriff ist, umso höher sind auch die Anforderungen an die Anerkennung der Verhältnismäßigkeit. Es müssen die „Streubreite", die Eingriffsintensität und die Veranlassung des Eingriffs bewertet werden. Bei der Strafverfolgung muss die Straftat auch im Einzelfall der Schwere des Eingriffs entsprechen. Sie ist durch einen Katalog oder eine entsprechend hohe Strafdrohung vom Gesetzgeber zu qualifizieren. Eine Ermittlung ins Blaue ist grundsätzlich verfassungswidrig.[42] Es muss vielmehr ein auf dem Einzelfall beruhender Tatverdacht vorliegen und bei der Gefahrenabwehr eine konkrete Gefahr für besonders hohe Rechtsgüter. Dabei lässt es das Bundesverfassungsgericht allerdings genügen, dass ihr Eintritt nicht unmittelbar bevorstehen muss.

Zur Verhältnismäßigkeit gehören auch der Richtervorbehalt und die Transparenz, also die Benachrichtigung des Betroffenen und seine Möglichkeit, die Rechtmäßigkeit des Eingriffs kontrollieren zu lassen. Eine Verschiebung der Benachrichtigung wird nur bei einer Gefährdung des Erfolges der Maßnahme und bei Gefahr für Leib und Leben eines verdeckt ermittelnden Beamten akzeptiert, nicht aber schon dann, wenn das Interesse an der weiteren Einsatzmöglichkeit eines verdeckten Ermittlers besteht. So abwägungsfähig das klingen mag, diese Vorgaben sind jedenfalls präzise.[43]

2. Das Urteil zum „Großen Lauschangriff"

Die Entscheidung zum Großen Lauschangriff[44] erklärt den Kernbereich privater Lebensführung ausdrücklich für unantastbar und bestandsfest gegenüber allen sonstigen privaten oder öffentlichen Interessen. Alle Aufzeichnungen, die den Kernbereich verletzen, müssen gelöscht werden. Ihre Verwertung ist schlechthin ausgeschlossen.[45] Das ist ständige Rechtsprechung geworden und gilt nicht nur beim Lauschangriff. Der Grundsatz der absoluten Schutzwürdigkeit der reinen Privatsphäre gilt als Rechtssatz auch außerhalb einer Wohnung bei staatlichen Eingriffen aller Art.

Der akustische Eingriff in die Wohnung nach Art. 13 GG wird im Wesentlichen nur als ultima ratio bei schweren, enumerativ aufgezählten Delikten zugelassen, wenn zuvor geklärt wurde, dass der Kern des Privatbereichs voraussichtlich nicht berührt werden wird. Er setzt eine richterliche, zeitlich begrenzende Entscheidung voraus und sieht zwingend eine nachträgliche Information der Betroffenen sowie einen jährlichen Bericht an das Parlament vor.

Für die richterliche Entscheidung schreibt das Gericht bestimmte Mindestbedingungen vor, die nach den bisherigen empirischen Untersuchungen überwiegend nicht beachtet wurden, immer wieder zu Aufhebungen durch das Bundesverfassungsgericht geführt und den Senat nun endlich veranlasst haben, eine ausdrückliche gesetzliche Re-

42 BVerfGE 115, 320, 361.
43 Vgl. Schlink, Abwägungen im Verfassungsrecht, 1976; Leisner, Der Abwägungsstaat., 1997, S. 96 ff, 144 ff.
44 BVerfGE 109, 279 ff.
45 BVerfGE 109, 279 ff., (313).

gelung anzuraten.[46] Alle Berufsgruppen des § 53 StPO werden gem. § 100 c Abs. 6 StPO vom Lauschangriff ausgenommen, wenn sich die Ermittlungen nicht gegen sie selbst richten. Aus einer missverständlichen Formulierung glaubte der Gesetzgeber bei der Berücksichtigung des Zeugnisverweigerungsrechts nach § 160 a StPO eine Unterscheidung zwischen Verteidigern und Rechtsanwälten machen zu können. Das hat der Bundesgesetzgeber inzwischen durch ein Gesetz korrigiert, das in diesen Tagen in Kraft getreten ist.[47] Anwälte und Verteidiger sind nun Abgeordneten und Geistlichen – nur der öffentlich-rechtlichen Religionsgemeinschaften? – gleichgestellt. Hinsichtlich der anderen Berufsgruppen, insbesondere der Journalisten, sind Verfassungsbeschwerden weiter anhängig.

3. Das Urteil zur sog. „online-Durchsuchung"

Die Entscheidung des Bundesverfassungsgerichts im Jahr 2008 zur sog. Online-Durchsuchung[48] eines PCs durch eine Computerwanze formuliert ein „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme". Es enthält wesentliche Hinweise zu der Tiefe eines solchen Eingriffs und zu der sich daraus ergebenden Bewertung der Verhältnismäßigkeit.[49] Es lässt einen Eingriff in den PC nur bei einer konkreten Gefahr für Leib, Leben und Freiheit einer Person, für den Bestand des Bundes oder eines Landes und bei der Gefährdung der Funktionsfähigkeit öffentlicher Versorgungseinrichtungen zu, die für die menschliche Existenz erforderlich sind.

Die Polizei darf nicht in eine Wohnung mit dem Ziel eindringen, den PC zu verwanzen. Das Gericht stellt fest, dass man mit einer solchen Wanze auch den Inhalt eines PCs ohne Wissen des Betroffenen verändern könnte. Darum wird man mit Recht die forensische Verwendbarkeit der erhobenen Erkenntnisse bezweifeln können. Das Gericht befasst sich auch eingehend mit dem Problem, dass bei einer Infiltration des PCs auch Dinge erfasst werden, die zum Kernbereich der privaten Lebensführung gehören. Darum muss es gesetzgeberisch gesichert werden, dass die Ergebnisse zunächst in einem angemessenen zweistufigen Verfahren auf die Zulässigkeit ihrer Verwendung geprüft werden.[50]

In § 20 k Abs. 7 BKA-Gesetz hat das zu der lächerlichen Variante geführt, dass die Prüfung durch drei BKA-Beamte erfolgt, von denen einer die Befähigung zum Richteramt haben müsse. Das ist natürlich Gegenstand einer anhängigen Verfassungsbeschwerde.[51] Ebenso kunstvoll ist die um sich greifende Regelung, dass ein Gespräch nur dann nicht aufgenommen werden darf, wenn „allein" Erkenntnisse aus dem Kernbereich aufgenommen werden würden, § 100 a Abs. 4 StPO, § 201 Abs. 6 BKA-Gesetz,

46 Vgl. statt aller Albrecht, Dorsch, Krüpe, Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation, MPI, Freiburg 2003., und BVerfG NJW 2010, S. 833 ff, Rdnr. 284

47 Gesetz zur Stärkung des Schutzes von Vertrauensverhältnissen zu Rechtsanwälten im Strafprozessrecht vom 17.12.2010,.BGBl I., S. 2261. das am 1. 2. 2011 in Kraft getreten ist.

48 BVerfGE 120, 274 ff

49 BVerfG a.a. O. Rdnr. 198 ff.

50 BVerfG. a.a.O. Rdnr. 273 ff.

51 Das BKA hat übrigens diese Ermittlungsmöglichkeit bei der Bekämpfung des internationalen Terrorismus zwar für unverzichtbar erklärt, für ihre technische und personelle Vorbereitung etwa 900.000 € aufgewendet, sie aber seit Verabschiedung des Gesetzes noch nie eingesetzt.

§ 34 b Abs. 1 ThürPAG, eine Eingrenzung, deren Mangel an Ernsthaftigkeit nicht verkannt werden kann.

Bei der sog. Quellen-TKÜ, also bei dem Abhören von Telefonaten, die mit dem PC verschlüsselt über das Internet geführt werden, kann mit derselben Wanze, mit der das Telefonat vor seiner Verschlüsselung mitgehört wird, auch der Rest des PCs ausgelesen werden. Das Bundesverfassungsgericht geht erkennbar davon aus, dass dafür eine besondere Rechtsgrundlage geschaffen werden müsste. Dazu habe ich vor kurzer Zeit jedoch feststellen müssen, dass sich der Zollfahndungsdienst dieser Technik zwar ohne eine besondere Rechtsgrundlage, aber mit richterlichen Entscheidungen bedient.

4. Das Urteil zur Vorratsdatenspeicherung

Die vierte Entscheidung des Bundesverfassungsgerichts ist die zur Vorratsdatenspeicherung.[52] Ihre Vorgeschichte ist voller Merkwürdigkeiten. Ursprünglich hatte der Bundestag eine Vorratsdatenspeicherung ausdrücklich abgelehnt. Die dann mit Zustimmung der Bundesregierung erlassene Europäische Richtlinie 2006/24/EG[53] hätte nur als Rahmenbeschluss der sog. Dritten Säule, also ohne zwingende Verbindlichkeit für die Mitgliedstaaten der Union beschlossen werden können, da die Union auf dem Gebiet der polizeilichen und sicherheitspolitischen Zusammenarbeit keine Kompetenz zur unmittelbaren Rechtsetzung besaß. Der EuGH[54] rechtfertigte aber die zwischen der Kommission und den nationalen Regierungen abgesprochenen Richtlinie mit der Begründung, dass damit die Wettbewerbsgleichheit der Provider gesichert werden solle – ein offenkundiges Scheinargument.[55] Der Inhalt der Richtlinie war dazu weder bestimmt noch geeignet. Die Vereinbarkeit mit Art. 8 EMRK hat der EuGH ausdrücklich nicht behandelt, weil das nicht vom Kläger, der Republik Irland, sondern nur von der Slowakei vorgetragen worden war. Inzwischen hat allerdings der Oberste Gerichtshof Irlands die Klage einer Bürgerrechtsorganisation gegen die Richtlinie dem EuGH vorgelegt, der sich nun mit der Vereinbarkeit der Richtlinie mit der Grundrechtecharta und der EMRK befassen muss.[56] Schweden, Irland, Deutschland, Österreich, Griechenland und Bulgarien haben die Richtlinie bisher nicht umgesetzt, Luxemburg nur teilweise.

Das Bundesverfassungsgericht hat die Vorratsdatenspeicherung entgegen seiner bisherigen Rechtsprechung, wenn auch nur in engsten Grenzen und unter detaillierten Voraussetzungen, für verfassungsgemäß gehalten und damit erneut eine Vorlage zum EuGH vermieden. Wegen der außerordentlichen Tiefe des Eingriffs in das informationelle Selbstbestimmungsrecht verlangt das Bundesverfassungsgericht äußerste gesetzliche Maßnahmen von Bund und Ländern, erklärte das bisherige nationale Umsetzungs-

52 BVerfG NJW 2010, 833 ff. vgl. dazu Hornung/Schnabel, "Verfassungsrechtlich nicht schlechthin verboten. Das Urteil des Bundesverfassungsgerichts zur Vorratsdatenspeicherung." DVBl. 2010, 824 ff, Simitis, NJW 2009, 1782 ff.

53 RiLi des Europ. Parlaments und des Rates vom 15.3.2006 über die Vorratsspeicherung von Daten u. d. Änderung der RiLi 2002/58/EG (ABl.L 105 vom 13.4.2006, S. 54 ff).

54 EuGH Urteil vom 10.2.2009, C-301/06.

55 Die Kommission hat in ihrem Zwischenbericht vom 28.6.2006 zum sog. Haager Programm die Vorratsdatenspeicherung selbst als Maßnahme zur Terrorismusbekämpfung bezeichnet, vgl. Kom (2006) 333 Tzif. 38.

56 Vgl. http://www.mcgarrsolicitors.ie/2010/05/05/digitals-rights-ireland-update.

gesetz für nichtig und ordnete die Löschung der bisher vorsorglich gesammelten Daten an. Es formuliert unmissverständlich: Es handele sich „um einen besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt. […] Die Speicherung bezieht sich auf Alltagshandeln, das im täglichen Miteinander elementar und für die Teilnahme am sozialen Leben in der modernen Welt nicht mehr verzichtbar ist.“ Der Bürger habe keine Ausweichmöglichkeit. „Die Aussagekraft der Daten ist weitreichend. Je nach Nutzung von Telekommunikationsdiensten seitens der Betroffenen lassen sich schon aus den Daten selbst – und erst recht, wenn diese als Anknüpfungspunkte für weitere Ermittlungen dienen – tiefe Einblicke in das soziale Umfeld und die individuellen Aktivitäten eines jeden Bürgers gewinnen“, auch wenn der Inhalt der Kommunikation nicht erfasst werde. Aus den Daten „lassen sich jedoch bei umfassender und automatisierter Auswertung bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse über gesellschaftliche und politische Zugehörigkeiten“ ziehen sowie über „persönliche Vorlieben, Neigungen und Schwächen derjenigen, deren Verbindungsdaten ausgewertet werden.“ Eine solche Speicherung kann „die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers ermöglichen. Bezogen auf Gruppen und Verbände erlauben die Daten überdies unter Umständen die Aufdeckung von internen Einflussstrukturen und Entscheidungsabläufen.“ Dieser schwerwiegende Eingriff erhöhe das Risiko drastisch, zum Gegenstand weiterer Ermittlungen zu werden, ohne selbst Anlass dazu gegeben zu haben.

Daraus ergeben sich besondere Voraussetzungen für eine noch akzeptierbare verfassungsgemäße Regelung: Der Staat darf die Daten nicht selbst speichern. Sie müssen anonymisiert, gegen Missbrauch jeweils nach dem neuesten Stand der Technik besonders geschützt werden und dürfen sowohl zur Strafverfolgung wie zur Gefahrenabwehr nur bei im Einzelfall schwersten Delikten genutzt werden. Die Nutzung setzt eine richterliche Entscheidung voraus, die auf einer eigenständigen Prüfung beruhen muss. Datensicherheit, Datenverwendung, Transparenz, Rechtsschutz des Einzelnen und Sanktionen bei Missbrauch sind normenklar und anspruchsvoll zu regeln. Datensicherheit und Verwendungszweck muss der Bundesgesetzgeber auch für die Fachbereiche regeln, für die die Länder zuständig sind. Zur Datensicherheit gehört die getrennte Speicherung, Verschlüsselung und Anonymisierung, Abruf nach dem 4-Augen-Prinzip, eine revisionssichere Kennzeichnung und Protokollierung von Nutzung und Löschung. Zur Datenverwendung gehören die Art der Delikte, die Eingriffsschwelle, die entsprechenden Präzisierungen bei der Gefahrenabwehr durch Polizei oder Nachrichtendienste – Gefahr für Leib, Leben, Freiheit einer Person, Bestand und Sicherheit des Bundes oder eines Landes, Gemeingefahr. Für die Länder verbleiben in ihren Zuständigkeitsbereichen die Regelung der Modalitäten des Einzelabrufs, die Transparenz für den Betroffenen und sein Rechtsschutz.

Das Gericht warnt den Gesetzgeber, dass eine Gesetzgebung, „die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielte, […] von vornherein mit der Verfassung unvereinbar“ sei. Die Vorratsdatenspeicherung „zwinge den Gesetzgeber zu größter Zurückhaltung. Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, für deren Wahrung sich die Bundesrepublik auch in europäischen und internatio-

nalen Zusammenhängen einsetzen muss."[57] Dabei folgt das Gericht dem Gedanken, dass der Staat mit dem gleichen Recht wie bei den Telekommunikationsdaten ohne Anlass alle Fahrkarten, Bücher, Zeitungen, Mietverträge, und was immer wir kaufen, leihen oder tun, zentral auf Vorrat speichern könnte.

Man kann lange darüber streiten, was das konkret bedeutet, etwa für ELENA und andere Speicherwerke. Ich erinnere daran, dass der Nationale Normenkontrollrat in einem Gutachten[58] festgestellt hat, dass ELENA erst dann rentabel arbeiten könne, wenn man zu den bisherigen 5 Verdienstbescheinigungen nunmehr 11 weitere Sozialbereiche in diese vorsorgliche Datensammlung einbeziehe, ein System, das auf einer Scheinfreiwilligkeit der erfassten Personen beruht und zu dem bereits eine Verfassungsbeschwerde anhängig ist.

Die praktische Bedeutung der Vorratsdatenspeicherung ist streitig. Wirklich verlässliche und ausreichende Tatsachenfeststellungen gibt es dazu noch nicht. Ein Gutachten des BKA[59] lässt erkennen, dass die polizeiliche Tätigkeit durch den Wegfall der Vorratsdatenspeicherung nur in begrenztem Umfang ernsthaft berührt wurde, überwiegend bei der Aufklärung von Kinderpornographie über die Internetaufrufe. In den Ländern, die die Richtlinie umgesetzt haben, ist eine Erhöhung der Aufklärungsquote nicht erkennbar.

Gegen das von der Justizministerin vorgeschlagene Quick-Freeze-Verfahren – also sofortige Sistierung der Verkehrsdaten bei konkretem Verdacht – wird eingewendet, dass die Verkehrsdaten bei den sog. Flat-Rates höchstens zwei Tage gespeichert werden und das Verfahren daher leerlaufe. Das ist jedoch unzutreffend. Die Daten werden auch bei Flatrate-Tarifen – je nach der Größe des Providers – bis zu 80 Tagen gespeichert, weil die Provider auch untereinander abrechnen müssen. Außerdem wird bei der organisierten oder gewerblichen Kriminalität die fortlaufende Tätigkeit einer kriminellen oder terroristischen Vereinigung nicht in dem Augenblick beendet, in dem die Polizei einen konkreten Verdacht fasst und die entsprechenden Teledaten einfrieren lässt. Ihr wachsen also immer weitere Daten zu, die fortlaufend eingefroren werden können.

IV. Der Datenschutz nach dem Recht der Europäischen Union

Inzwischen hat sich die europäische Rechtslage allerdings verändert. Durch den Lissabonner Vertrag hat die Europäische Union gemäß Art. 39 EUV, Art. 16 Abs. 2, 67 ff AEUV Entscheidungskompetenzen auch für die Datenverarbeitung im Bereich der polizeilichen und justiziellen Zusammenarbeit erhalten. Ebenso ist die Europäische Grundrechtecharta in Kraft getreten, die in Art. 7 und 8 das Recht auf Privatheit und den Schutz der persönlichen Daten enthält.

In einer Konferenz auf EU-Ebene Anfang Dezember 2010 zur Vorratsrichtlinie hat die für die Innenpolitik zuständige Kommissarin Malmström in einer Art erweitertem Grußwort[60] zu erkennen gegeben, dass sie an der Richtlinie im Grundsatz festhalten und sie durchsetzen will, wenn auch mit konkreteren Regelungen über Art und Dauer der

57 BVerfG NJW 2010, 833(839 f), Rdnr. 218.
58 Gutachten vom Sept. 2010, http://www.normenkonrtrollrat.bund. de.
59 BTInnenA DrS. 17(4)139 vom 30.11.2010.
60 Vgl. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/723.

zu speichernden Daten, über Zweckbestimmung, Richtervorbehalt, Missbrauchsverhütung und Kostentragung. Das berührt den Kern der Richtlinie nicht, kann aber durchaus mit den zwingenden Bedingungen des Bundesverfassungsgerichts über die Vereinbarkeit der Vorratsdatenspeicherung mit dem Grundgesetz kollidieren. Die Kommissarin betrachtet es als Erfolg, dass der Abruf von Vorratsdaten mit 148000 Abrufen pro Jahr und Mitgliedsstaat und 2,6 Mio. Anfragen zu Internetdaten ein Routineverfahren geworden ist, das in einzelnen Staaten bei bis zu 86 % der polizeilichen Vorgänge benutzt wurde. Sie hat das Problem offenbar überhaupt nicht begriffen, dass bei einer so gewaltigen Streuung persönlicher Daten ein Missbrauch überhaupt nicht verhindert werden kann.

Da zieht eine Kontroverse herauf, deren Ausgang ungewiss ist. Wir werden sehen, ob die Kommission gegen säumige Staaten Sanktionen einleiten würde, bevor der EuGH über die erneut anhängige irische Klage zur Verletzung der Charta entschieden hat. Ich kann auch keineswegs ausschließen, erneut das Bundesverfassungsgericht anzurufen, wenn von der EU oder dem Bundestag Regelungen vorgeschrieben werden sollten, die mit den verfassungsmäßigen Mindestbedingungen des Bundesverfassungsgerichts nicht vereinbar sind. Immerhin hat sich das Bundesverfassungsgericht in den einschlägigen Entscheidungen auf Art. 1 und 2 GG berufen. Dann wird es vor der Frage stehen, ob es auch bei einer Verletzung des europafesten Art. 1 GG vor dem EuGH zurückweichen darf.[61]

Unabhängig von der Vorratsdatenspeicherung wird sich die Politik mit der am 4.11.2010 vorgelegten Gesamtkonzeption der Kommission der EU für den Datenschutz in der Union[62] befassen müssen. Mit ihr soll die Datenschutzrichtlinie von 1995[63] und die sie ergänzenden Regelungen durch präzisere und vor allem zwingende Bestimmungen ersetzt werden, nachdem die Europäische Union gem. Art. 16, 67 AEUV dazu die Kompetenz erhalten hat, und zwar, wie sie betont, auch für den nicht grenzüberschreitenden Datenverkehr. Zu den Neuregelungen sollen u. a. gehören: eine größere Transparenz und Anzeigepflichten auch bei der Verletzung von Datenschutzrechten, das Recht auf Vergessen und damit die Möglichkeit des Einzelnen, von ihm freigegebene Daten zeitlich zu befristen und auch aus sozialen Netzwerken wie Facebook zurückzuholen, die Möglichkeit von Verbandsklagen, einheitliche Regelungen auch für den Bereich der polizeilichen und justiziellen Zusammenarbeit sowie die Stärkung der Befugnisse und die „uneingeschränkte Durchsetzung der völligen Unabhängigkeit“ der nationalen Datenschutzbeauftragten.[64]

Über die Durchsetzung dieser Rechte gegenüber Providern, die ihren Sitz oder ihre Verarbeitung außerhalb der EU haben, sagt die Kommission naturgemäß nichts. Aber sie erklärt ausdrücklich, dass sie ihre Möglichkeiten ausschöpfen wird, die Mitgliedsstaaten zu entsprechenden Regelungen zu zwingen.

---

61 Vgl. dazu den äußerst vorsichtigen Honeywell-Beschluss des Bundesverfassungsgerichts, NZA 2010,995. Das Verhältnis des Art. 1 der Europäischen Grundrechtecharta zu Art. 1, 23 Abs. 1, 79 Abs. 3 GG kann hier nicht erörtert werden.

62 Vgl. KOM (2010) 609 endgültig DE.

63 RiLi 95/46/EG des Europäischen Parlaments u. d.Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten u. z. freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31).

64 Vgl. EuGH vom 9.3.2010, Kommission./.Deutschland, Rechtssache C – 518/07.

Schon im sog. Haager Programm vom 3.3.2005[65] und seiner Fortsetzung, dem Stockholmer Programm vom 2.11.2009[66] für die Weiterentwicklung der Zusammenarbeit der Europäischen Union von 2010 bis 2014, wird eine enge Zusammenarbeit im Bereich einer „Europäischen Sicherheitsarchitektur" gefordert, die Durchsetzung des Anerkennungs- und des Verfügbarkeitsprinzips,[67] interoperative Polizeidatenbanken, grenzüberschreitende Online-Durchsuchungen, ein zentrales Bevölkerungsregister, mehr Kontrolle im Internet, eine Europäische Gendarmerie, militärische Einsätze zur Migrationsabwehr.

Das führt zu einer letzten Überlegung: Zwar sind Kommission und Europäisches Parlament an Art. 7 und 8 der Grundrechtecharta gebunden, die den Schutz der Privatheit und der persönlichen Daten garantieren. Aber die in Art. 52 der Charta geregelte Möglichkeit, Grundrechte durch Gesetz einzuschränken, ist so erschreckend allgemein formuliert, dass man angesichts der bisherigen äußerst verwaltungsfreundlichen Rechtsprechung des EuGH nicht vorhersagen kann, ob das Grundrecht gegenüber Einschränkungen wirklich standhält. Das gilt leider auch für Art. 1 der Charta. Er hat zwar den gleichen Wortlaut wie der Art. 1 GG, ist aber vom EuGH in seiner bisherigen Rechtsprechung mehrfach in seiner rechtlichen Bedeutung eingeschränkt worden.[68] Es ist also durchaus denkbar, dass wir es gerade im Bereich der Harmonisierung der polizeilichen und justiziellen Zusammenarbeit mit Regeln zu tun haben werden, die der EuGH mit Art. 1, 7 und 8 der Grundrechtecharta für vereinbar hält, die aber der bisherigen Rechtsprechung des Bundesverfassungsgerichts zu Art. 1 GG widersprechen. Dann allerdings wird das Bundesverfassungsgericht Farbe dazu bekennen müssen, was nach unserer Überzeugung zur Menschenwürde und zu unserer Verfassungsidentität gehört.

Dem Gericht ist im Zusammenhang mit der Lissabon- Entscheidung[69] wiederholt vorgehalten worden, dass es die politische Bedeutung der Europäischen Union nicht ausreichend gewürdigt habe. Das ist falsch. Es ist nicht europafeindlich, darauf zu bestehen, dass die Union die verfassungsrechtlichen Grundüberzeugungen ihrer Mitgliedsstaaten zu respektieren hat, im Gegenteil. Europa ist nur dann der oft beschworene „Raum der Sicherheit, der Freiheit und des Rechts", wenn seine Bürger davon überzeugt sein können, dass ihre Freiheitsrechte dabei nicht zu kurz kommen und dass sie nicht verfassungswirksam beschnitten werden können, ohne dass das Volk das selbst beschlossen hätte. Bleibt zu hoffen, dass die Union diese Bewährungsprobe besteht.

65 Amtsbl. C 236 vom 24.9.2005.
66 Amtsbl. C 155 vom 4.5.2010.
67 D.h. einheitlichen Zugang zu sicherheitsbehördlich gespeicherten Datenbeständen der Mitgliedsstaaten und die Anerkennung der Rechtswirksamkeit polizeilicher Zwangsmaßnahmen eines Mitgliedsstaates in allen anderen Unionsstaaten ohne Rücksicht darauf, ob das Verhalten eines Bürgers im Vollstreckungsstaat überhaupt rechtswidrig ist.
68 Der EuGH vertritt in ständiger Rechtsprechung auch die Auffassung, dass das Grundgesetz für die deutschen Gerichte bei der Bewertung von Gemeinschaftsakten keine Bedeutung habe.
69 BVerfG 123, 267 ff.