Entwicklungen des Rechts auf informationelle Selbstbestimmung seit dem Volkszählungsurteil des Bundesverfassungsgerichts

HANS-JÜRGEN PAPIER

„Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."[1]

Diese prägnante Zusammenfassung des Inhalts des Rechts auf informationelle Selbstbestimmung entstammt wortwörtlich dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983. Dieses Urteil muss der Ausgangspunkt unserer Betrachtungen sein, weil das Bundesverfassungsgericht das Recht auf informationelle Selbstbestimmung dort zum ersten Mal als besondere Ausprägung des allgemeinen Persönlichkeitsrechts entwickelt hat.[2] Erst seitdem lässt sich folglich von einem „Grundrecht auf informationelle Selbstbestimmung" sprechen. Rückblickend kann das Volkszählungsurteil daher – mit den Worten von *Wolfgang Hoffmann-Riem* – zu Recht als „Magna Charta" des deutschen Datenschutzrechts bezeichnet werden.[3]

Lassen Sie mich also zunächst die Grundaussagen des Volkszählungsurteils etwas detaillierter in Erinnerung rufen, bevor ich im Anschluss auf die weitere Entwicklung des Rechts auf informationelle Selbstbestimmung eingehen werde.

---

[1] BVerfGE 65, 1 (43).

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

[3] So *Hoffmann-Riem*, AöR 123 (1998), S. 513 (515).

I. Grundaussagen des Volkszählungsurteils

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 Persönlichkeitsrecht,[4] das unter anderem auch das Recht am eigenen Bild oder vor verfälschenden oder entstellenden Darstellungen der eigenen Person schützt.[5]

Die Ableitung eines Maßstabs für die staatliche Informationserhebung und -verarbeitung 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 so genannten „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.[6]

Neu war im „Volkszählungsurteil" vielmehr, dass das Bundesverfassungsgericht die Vorgaben des allgemeinen Persönlichkeitsrechts an die modernen Bedingungen der automatischen Datenverarbeitung angepasst hat.[7] Die freie Entfaltung der Persönlichkeit setzt hier den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Das

---

[4] Vgl. 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.

[5] Vgl. jüngst: BVerfGE 119, 1 (24) – „Esra".

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

[7] Vgl. BVerfGE 65, 1 (42).

Grundrecht auf informationelle Selbstbestimmung gewährleistet daher dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[8]

Damit wurde die zuvor vom Bundesverfassungsgericht verwendete „Sphärenkonzeption" zum Teil aufgegeben.[9] 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 von vornherein „belangloses Datum" mehr. Vielmehr bedarf es nun zur Feststellung der persönlichkeitsrechtlichen Bedeutung eines Datums der Kenntnis seines Verwendungszusammenhangs.[10]

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, gefährdet.[11]

Das Recht auf informationelle Selbstbestimmung hat nach dem „Volkszählungsurteil" allerdings nicht zur Folge, dass der Einzelne ein eigentumsgleiches Recht an „seinen Daten" hat.[12] 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 führt zugleich dazu, dass der

---

[8] Vgl. BVerfGE 65, 1 (43).

[9] 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).

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

[11] Vgl. BVerfGE 65, 1 (42 f.); zuletzt erneut bestätigt durch: BVerfGE 120, 274 (311 f.).

[12] Forderungen wie „Meine Daten gehören mir" (vgl. *Künast,* ZRP 2008, S. 201) sind daher fragwürdig.

Einzelne Einschränkungen seines Rechts auf informationelle Selbstbestimmung im überwiegenden Allgemeininteresse hinnehmen muss.[13]

2. Datenschutzrechtliche Folgerungen

Welche konkreten Folgerungen zog das „Volkszählungsurteil" aus der genannten Einordnung des Datenschutzes als Grundrechtsschutz?[14] Eingriffe in das Recht auf informationelle Selbstbestimmung bedürfen nach dem „Volkszählungsurteil" zunächst einer hinreichend bestimmten gesetzlichen Grundlage.[15] Dabei muss der Gesetzgeber den Verwendungszweck der zu erhebenden Daten bereichsspezifisch und präzise festlegen.[16] 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 darf.[17] Zwar schließt die Zweckbindung erhobener Daten eine Zweckänderung nicht aus, diese bedarf jedoch ihrerseits einer verfassungskonformen gesetzlichen Grundlage.[18] Erforderlich sind zudem verfahrensrechtliche Schutzvorkehrungen wie Aufklärungs-, Auskunfts- und Löschungspflichten sowie im Interesse eines vorgezogenen Rechtsschutzes die Beteiligung eines unabhängigen Datenschutzbeauftragten.[19]

II. Weitere Entwicklung des Datenschutzes

Die Vorgaben des „Volkszählungsurteils" führten dann im Jahr 1990 zu einer Novellierung des aus dem Jahr 1977 stammenden Bundesdatenschutzgesetzes.[20] Damit war die Entwicklung des Datenschutzes

---

[13] Vgl. BVerfGE 65, 1 (44).

[14] Siehe dazu: *Simitis*, in: *Simitis* (Hrsg.), BDSG, 6. Aufl. 2006, Einleitung Rn. 30 ff.

[15] Vgl. BVerfGE 65, 1 (44).

[16] Vgl. BVerfGE 65, 1 (46).

[17] Vgl. BVerfGE 65, 1 (46).

[18] Vgl. BVerfGE 100, 313 (360).

[19] Vgl. BVerfGE 65, 1 (46).

[20] Gesetz 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 Daten-

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 EU-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 existierten[21] – die Freiheit des Verkehrs von Waren, Personen, Dienstleistungen und Kapital beeinträchtigten. Die deshalb im Jahr 1995 erlassene allgemeine Datenschutz-Richtlinie[22] kombinierte unterschiedliche juristische Ansätze und Rechtskulturen und beschränkte sich nicht – wie man annehmen könnte – auf den kleinsten gemeinsamen Nenner, sondern zielte auf ein hohes Schutzniveau ab.[23]

---

schutzrecht, 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.

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

[22] Richtlinie 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.

[23] Vgl. 10. Erwägungsgrund der Richtlinie 95/46/EG; *Abel,* in: *Roßnagel* (Hrsg.), Handbuch Datenschutzrecht, 2003, 2.7 Rn. 45 f.; *Simitis*, in: *Simitis* (Hrsg.), BDSG, 6. Aufl. 2006, Einleitung Rn. 205 ff.

Darüber hinaus erfordert nicht nur die gemeinsame Verwaltung des Binnenmarktes,[24] sondern auch die Abschaffung der Grenzkontrollen an den Binnengrenzen der Europäischen Union durch das Schengener-Durchführungsübereinkommen[25] und die in der Folge verstärkte Zusammenarbeit in den Bereichen Justiz und Inneres[26] einen Informationsaustausch zwischen den vielen mitgliedstaatlichen Verwaltungen und der Kommission.[27] 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 existieren.[28]

Die europäischen Organe und Einrichtungen selbst sind durch eine Verordnung an datenschutzrechtliche Regeln gebunden.[29] Darüber

---

[24] Vgl. *Wettner*, Die Amtshilfe im Europäischen Verwaltungsrecht, 2005, S. 45 ff.

[25] BGBl II vom 23. Juli 1993 S. 1013.

[26] Vgl. *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.

[27] Vgl. 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.

[28] Vgl. 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 Ratsdokument 9260/08 sowie KOM(2005) 475.

[29] Verordnung (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.

hinaus verleiht die seit Inkrafttreten des Vertrages von Lissabon verbindliche Charta der Grundrechte der Europäischen Union in ihrem Art. 8 dem Recht auf Schutz personenbezogener Daten deutlich sichtbar den Status des Grundrechtsschutzes.[30]

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".[31] In Verfolgung dieses Konzepts wurde in den letzten Jahren mit der deutschen Arkantradition gebrochen, nach der Behördenakten – außer für die Beteiligten – grundsätzlich der Geheimhaltung unterlagen.[32] Nun gibt es auf Bundes- oder Landesebene Gesetze, die jedermann den Zugang zu Umweltinformationen, zu gesundheitsbezogenen Verbraucherinformationen oder allgemein zu jeder amtlichen Information gewährleisten.[33] Diese Entwicklung hin zu einem „gläsernen Amt"[34] wurde unter anderem durch Vorschriften der Europäischen Union[35] sowie durch Vorbilder in anderen Staaten wie den USA[36] oder Schweden angestoßen. In letzterem ist das Öffentlichkeitsprinzip bereits im Jahr 1766 eingeführt worden.[37]

Das „Konzept der informierten Öffentlichkeit" zielt in erster Linie darauf ab, die „res publica" Wirklichkeit werden zu lassen,[38] das heißt durch mehr Transparenz der Verwaltung und einen verbesserten Informationszugang der Bürger den demokratischen Meinungs- und

---

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

[31] Vgl. *Roßnagel*, MMR 2007, S. 16 ff.; *Kloepfer*, DÖV 2003, S. 221 ff.

[32] Vgl. § 29 VwVfG, dazu: *Sydow*, NVwZ 2008, S. 481 ff.

[33] Vgl. Umweltinformationsgesetz vom 22. Dezember 2004, BGBl I S. 3704; Verbraucherinformationsgesetz vom 5. November 2007, BGBl I S. 2558; Informationsfreiheitsgesetz vom 5. September 2005, BGBl I S. 2722.

[34] Vgl. *Reinhart*, DÖV 2007, S. 18.

[35] Vgl. 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.

[36] Freedom of Information Act von 1966, vgl. BTDrucks 15/4493, S. 6.

[37] Vgl. *Schoch*, DÖV 2006, S. 1 (5); *Gröschner*, VVDStRL 64 (2004), S. 344 (346).

[38] Vgl. *Gröschner*, VVDStRL 64 (2004), S. 344 (353); *Masing*, VVDStRL 63 (2004), S. 377 (384).

Willensbildungsprozess zu stärken.[39] Damit korrespondiert das Informationszugangsrecht für jedermann – jedenfalls auf einer abstrakten Ebene – mit dem Recht auf informationelle Selbstbestimmung.[40] Wie bereits erwähnt, hat ja gerade auch das „Volkszählungsurteil" den Zusammenhang zwischen Datenschutz und Ausübung demokratischer Freiheitsrechte deutlich aufgezeigt.[41] 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 wurden.[42] Ich denke jedoch, dass diese Konflikte durch eine sorgfältige und differenzierende Abwägung der jeweiligen Rechtspositionen gelöst werden können.[43]

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",[44] und es wurden die Befugnisse des BND zur Überwachung der Telekommunikation ausgeweitet.[45] Und nach den Terroranschlägen vom 11. September 2001 in den USA und vom

---

[39] Vgl. 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).

[40] Vgl. *Roßnagel*, MMR 2007, S. 16 (18); *Schoch*, DÖV 2006, S. 1 (2 f.).

[41] Vgl. BVerfGE 65, 1 (43).

[42] Vgl. BVerwG, NJW 2002, S. 1815 ff. – „Fall Helmut Kohl".

[43] *Roßnagel*, MMR 2007, S. 16 (19 f.); *Masing*, VVDStRL 63 (2004), S. 377 (410 ff.).

[44] Das 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).

[45] Vgl. das Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses 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.

11. März 2004 in Madrid wurden in Deutschland sowie auf EU-Ebene Maßnahmen durchgeführt oder beschlossen, wie die präventive polizeiliche Rasterfahndung nach so genannten „Schläfern",[46] die „Online-Durchsuchung"[47] oder die Vorratsspeicherung von Telekommunikationsverbindungsdaten.[48]

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 kann.[49] Gleichwohl dürfen bei der Ausbalancierung von Freiheit und Sicherheit die Gewichte nicht grundlegend verschoben werden.[50]

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 ihrer Gefährdung.[51] 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 vereinbaren.[52]

Darüber hinaus darf – dies hat das Bundesverfassungsgericht seit seiner Anfangszeit immer wieder betont[53] – der Kernbereich privater

---

[46] Vgl. dazu: BVerfGE 115, 320.

[47] Vgl. dazu: BVerfGE 120, 274.

[48] Vgl. 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 verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. Nr. L 105 vom 13. April 2006, S. 54; vgl. dazu: BVerfGE 122, 120.

[49] Vgl. BVerfGE 120, 274 (319 f.); BVerfGE 120, 378 (428 f.).

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

[51] Vgl. BVerfGE 115, 320 (360).

[52] Vgl. BVerfGE 115, 320 (360 ff.); BVerfGE 120, 378 (430).

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

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 möchte.[54]

Schließlich hat das Bundesverfassungsgericht mit seiner Entscheidung zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten vom März diesen Jahres in einer weiteren Hinsicht einen verfassungsrechtlichen „Grenzpfahl" errichtet: Eine flächendeckende, vorsorgliche Erfassung und Speicherung von Daten, die praktisch alle Aktivitäten des Bürgers rekonstruierbar macht, ist mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar.[55] Eine solche staatliche Datensammlung bedeutete vielleicht ein zusätzliches Maß an Sicherheit; dies darf aber nicht auf Kosten einer totalen Überwachung der Bürger gehen, die die Freiheitsausübung empfindlich einschränken würde. Die gesetzlich vorgeschriebene anlasslose Speicherung aller Telekommunikationsverkehrsdaten durch die Telekommunikationsdiensteanbieter für den Zeitraum von sechs Monaten ist daher vor allem deshalb noch mit dem Grundgesetz vereinbar, weil sie eben nur die Verkehrsdaten, nicht aber die Inhalte der Kommunikation umfasst. Zugleich hob das Bundesverfassungsgericht hervor, dass die Existenz dieser Art der Vorratsdatenspeicherung den Spielraum für die Schaffung weiterer ähnlicher Datensammlungen aus dem oben genannten Grund stark beschränkt; derartige Vorratsdatenspeicherungen müssen die Ausnahme bleiben. Darüber hinaus hat das Bundesverfassungsgericht in der Entscheidung zur Vorratsdatenspeicherung die sich aus dem Verhältnismäßigkeitsgrundsatz ergebenden verfassungsrechtlichen Anforderungen an die konkrete Ausgestaltung des Eingriffs in das Recht auf informationelle Selbstbestimmung nochmals präzisiert: Angesichts der Schwere des Eingriffs muss ers-

[54] Vgl. BVerfGE 120, 274 (338 f.).
[55] BVerfG NJW 2010, S. 833 (839).

tens ein besonders hoher Standard der Datensicherheit gewährleistet sein.[56] Zweitens dürfen die Daten nur zur Ahndung von Straftaten, die überragend wichtige Rechtsgüter bedrohen oder zur Abwehr von Gefahren für solche Rechtsgüter verwendet werden.[57] Drittens schließlich muss der Gesetzgeber hinreichende Vorkehrungen zur Transparenz der Datenverwendung sowie zur Gewährleistung eines effektiven Rechtsschutzes treffen.[58] Die Entscheidung zur Vorratsdatenspeicherung betraf zwar den Anwendungsbereich von Art. 10 GG; dieser stellt aber insoweit nur eine spezielle Normierung des Rechts auf informationelle Selbstbestimmung für den Bereich des Telekommunikationsverkehrs dar, so dass sich die verfassungsrechtlichen Vorgaben des Bundesverfassungsgerichts auf das allgemeine Recht auf informationelle Selbstbestimmung übertragen lassen.[59]

Insgesamt scheint mir angesichts dieser alten und neuen grundrechtlichen Grenzen für die sicherheitsrechtliche Tätigkeit des Staates 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 halten.[60] Zudem verfügt unser Gemeinwesen über rechtsstaatliche und demokratische Kontrollmechanismen, 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 heute jedenfalls mehr darum, dass wir uns zu einer privaten Überwachungsgesellschaft internationalen Ausmaßes verwandeln und dies weitgehend auch noch völlig freiwillig. Durch den andauernden technischen Fortschritt der Informations- und Kommunikationstechnologie und die internationale Vernetzung der Informa-

---

[56] BVerfG NJW 2010, S. 833 (840).

[57] BVerfG NJW 2010, S. 833 (840 ff.).

[58] BVerfG NJW 2010, S. 833 (843 f.).

[59] BVerfG NJW 2010, S. 833 (836).

[60] Besonders 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; BVerfGE 120, 274 (315 ff.); BVerfGE 120, 378 (407 ff.).

tionswege 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. In Zukunft könnte – wofür es sicherlich gute Gründe gibt – auch noch unsere Krankenakte digital gespeichert und versendet werden.[61]

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 der im „Volkszählungsurteil" für unzulässig befundene „Super-GAU des Datenschutzes" Wirklichkeit werden,[62] allerdings herbeigeführt durch die Hände Privater. 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 in letzter Zeit aufgetretenen Skandale betreffend den „Datendiebstahl" oder die Überwachung von Arbeitnehmern geradezu auf.[63] 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 programmiert.[64]

Das Grundrecht auf informationelle Selbstbestimmung im Sinne des „Volkszählungsurteils" fordert auch diesbezüglich den Schutz der Bürger. Denn es verpflichtet den Staat auch, im Ausgleich mit

---

[61] Vgl. *Geyer*, FAZ vom 25. November 2008, S. 33.

[62] Vgl. BVerfGE 65, 1 (42). S. dazu auch BVerfG NJW 2010, S. 833 (839).

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

[64] Vgl. auch: *Steidle/Pordesch*, DuD 2008, S. 324 ff.

konkurrierenden Freiheitsrechten ein angemessenes Schutzregime zu schaffen und durchzusetzen sowie sich auf internationaler Ebene für ein solches Regime einzusetzen.[65] Im Bereich der Schutzpflichten hat der Staat selbstverständlich eine größere Ausgestaltungsfreiheit als es bei der oben dargestellten Abwehrdimension des Rechts auf informationelle Selbstbestimmung der Fall ist. Dennoch muss er einen effektiven Schutz gegen Eingriffe von privater Seite sicherstellen. Mindestanforderungen sind dabei insbesondere, dass der Zweck der Datenerhebung in einem angemessenen Verhältnis zu der Eingriffsintensität steht und dass die zu diesem bestimmten Zweck erhobenen Daten nicht ohne weiteres zu einem anderen Zweck benutzt werden dürfen. Darüber hinaus hat der Staat Private dazu zu verpflichten, die Sicherheit erhobener personenbezogener Daten zu gewährleisten. Schließlich muss bei heimlicher Datenerhebung grundsätzlich ein Anspruch des betroffenen Bürgers auf Benachrichtigung bzw. auf Auskunft bestehen, das heißt, es muss für eine hinreichende Transparenz der Datenerhebung gesorgt werden.

Um einen ausreichenden Schutz des Rechts auf informationelle Selbstbestimmung auch in diesem Bereich zu sichern, 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. Denn nur auf der Grundlage gesetzlicher Regelungen sind effiziente Rechtsschutzmöglichkeiten gegeben. Bezeichnenderweise bezogen sich die letzten Novellen des Bundesdatenschutzgesetzes aus dem Jahr 2009 ganz überwiegend auf den privaten Bereich und haben beispielsweise den Adresshandel erschwert.[66]

---

[65] Vgl. 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).

[66] Zu den Novellen s. *Scheuring*, NVwZ 2010, 809 ff. u. *Kühling/Bohnen*, JZ 2010, 600 (601 ff.). Im Hinblick auf den Datenschutz von Arbeitnehmern sollte der neue § 32 BDSG keine materiell-rechtlichen Änderungen herbeiführen, sondern lediglich die bestehenden Regelungen klarstellend zusammenfassen (*Kühling/Bohnen*, JZ 2010, 600 [605]; kritisch zu § 32 BDSG *Thüsing*, NZA 2009, 865 ff.); eine Novellierung des Arbeitnehmerdatenschutzrechts ist jedoch in Planung, s. den Regierungsentwurf für ein Beschäftigungsdatenschutzgesetz vom 25.8.2010, der umfassende Neuregelungen für das BDSG vorsieht.

Allerdings befürchte ich auch, dass der grundrechtliche Schutzauftrag des Rechts auf informationelle Selbstbestimmung angesichts des ständigen Fortschritts der Technik wohl nie wird abgeschlossen werden können.[67] Dies hat sich zuletzt wieder an der Diskussion um „Google Street View" gezeigt – ein Internet-Programm, das für jeden frei zugänglich ist und eine detailgetreue, dreidimensionale Darstellung ganzer Städte ermöglicht. Das Privatunternehmen Google hat sich zwar unter anderem dazu bereit erklärt, auf Widerspruch von Hauseigentümern und Mietern auf die Darstellung von deren Gebäuden zu verzichten,[68] es ist jedoch zumindest umstritten, ob nach der derzeitigen Rechtslage eine wirksame *rechtliche* Handhabe gegen eine Veröffentlichung der Bilder bestünde.[69] Man muss sich hier schon die Frage stellen, ob damit der Gesetzgeber seiner grundrechtlichen Schutzpflicht im hinreichenden Maße entspricht.

III. Schluss

Wir haben gesehen, dass der Ausgangspunkt des „Volkszählungsurteils" erhebliche Veränderungen und Entwicklungen erfahren hat. Gleichwohl haben die Aussagen des „Volkszählungsurteils" nichts von ihrer Aktualität verloren. Ich habe hervorgehoben, dass die technologische Entwicklung erhebliche Gefahren für das Recht der informationellen Selbstbestimmung gerade auch für das Verhältnis

---

[67] Zum weiteren grundlegenden Reformbedarf des Datenschutzrechts s. *Kutscha*, ZRP 2010, 112 ff.; *Kühling/Bohnen*, JZ 2010, 600, 601 (607 ff.).

[68] S. hierzu die Selbstverpflichtungserklärung „Zusagen von Google zum Internetdienst Google Street View", abrufbar unter http://www.hamburg.de/datenschutz/aktuelles/1569338/google-street-view-zusage.html.

[69] S. dazu bspw. *Caspar*, DÖV 2009, 965 ff.; *Spiecker gen. Döhmann*, CR 2010, 311 ff.; *Lindner*, ZUM 2010, 292 ff. Umstritten ist dabei bereits, ob es sich bei der Darstellung von Gebäuden um personenbezogene Daten handelt und damit überhaupt der Anwendungsbereich des BDSG eröffnet ist. Selbst wenn das BDSG anwendbar ist, dann dürfte sich die Zulässigkeit der Erhebung und Übermittlung der Daten nach § 29 Abs. 1 und 2 BDSG richten; ausschlaggebend ist dabei insbesondere, ob das schutzwürdige Interesse des von der Datenerhebung bzw. -übermittlung Betroffenen offensichtlich überwiegt. Nicht geklärt ist, ob ein einfacher Widerspruch gegen die Veröffentlichung der Daten bereits dazu führt, dass das Interesse des Betroffenen an der Nichterhebung bzw. -übermittlung überwiegt.

zwischen Privaten birgt. Umso mehr begrüße ich es, dass wir auf den 1. Bitburger Gesprächen in München die Gelegenheit haben, einen zentralen Bereich dieser Problematik – den Datenschutz im Arbeitsverhältnis – vertiefender zu betrachten.