Erhard Denninger
Das Recht auf informationelle Selbstbestimmung und Innere Sicherheit

Folgerungen aus dem Volkszählungsgesetzurteil des Bundesverfassungsgerichts

A. Die gegenwärtige Situation

Anderthalb Jahre nach dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz (VZG) 1983[1] ist der parlamentarische wie außerparlamentarische Kampf um die notwendigen oder wünschenswerten gesetzgeberischen Konsequenzen des Karlsruher Spruches voll entbrannt. Wer die Datenschutz- und Amtshilfediskussion der letzten Jahre verfolgt hat, hat das nicht anders erwartet. Bezeichnenderweise scheint *die* Materie, die eigentlich Anlaß zu dem Grundsatzurteil gegeben hatte, nämlich das Volkszählungsgesetz, weniger kontrovers zu sein als die Novellierung des Datenschutzes[2], des Personalausweisrechts[3] und des allgemeinen Polizeirechts[4]. Die zahlreichen Stimmen in der Literatur, die sich beifällig oder kritisch vernehmen ließen[5], blieben meistens im Rahmen einer Analyse, riskierten nur selten Vorschläge zur konkreten, detaillierten Regelung entstehender Probleme, etwa im Bereich der Gefahrenabwehr oder zur Abstimmung von präventiver und repressiver Straftatbekämpfung usw. Die gesetzgebungspolitischen Reaktionen auf das Urteil lassen sich, etwas vergröbert, auf *drei Typen* zurückführen: a) Auf die Tendenz, die legislativen Auswirkungen des Urteils zu minimieren, einen umfassenden Gesetzesvorbehalt für die Erhebung und Verarbeitung personenbezogener Daten zu verneinen und die bestehenden, in den Sicherheits- und Ordnungsgesetzen zumeist generalklauselartig gefaßten Rechtsgrundlagen als auch verfassungsrechtlich ausreichend anzusehen. Man würde eine solche Haltung vor allem bei den Verwaltungspraktikern, zumal der Innenressorts, als dominant vermuten, bemerkenswerterweise trifft das keineswegs durchgängig zu (vgl. zu c). b) Die entgegengesetzte Tendenz leitet aus dem Urteil einen umfassenden Regelungsauftrag ab, der den Schutz der informationellen Selbstbestimmung sowohl im Verhältnis des Staates zum Bürger als auch im Verkehr zwischen ›Privaten‹ verwirklichen soll. Es überrascht nicht, diese Einstel-

1 BVerfGE 65, 1 ff., vom 15. 12. 1983.

2 Dazu liegt ein Gesetzentwurf der SPD dem Innenausschuß des Bundestages vor, BT-Drcks. 10/1180 vom 27. 3. 1984.

3 Vgl. dazu die Entwürfe eines Fünften Gesetzes zur Änderung des Gesetzes über Personalausweise a) der CDU/CSU und der FDP – BT-Drcks. 10/2177 und b) der Grünen, BT-Drcks. 10/1316.

4 Vgl. Vorentwurf zur Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes des Bundes und der Länder gemäß Beschluß der Innenministerkonferenz vom 25. November 1977 (Stand: 08.02. 1985).

5 Aus der Fülle der Literatur seien hervorgehoben:
Bull, Datenschutz oder die Angst vor dem Computer, 1984; *Heußner*, Das informationelle Selbstbestimmungsrecht in der Rechtsprechung des Bundesverfassungsgerichts, SGb. 7/84, 279 ff.; *Mückenberger*, Datenschutz als Verfassungsgebot, KJ 1984, 1 ff.; *Podlech*, Die Begrenzung staatlicher Informationsverarbeitung durch die Verfassung angesichts der Möglichkeit unbegrenzter Informationsverarbeitung mittels der Technik, Leviathan 1984, 85 ff. *Scholz/Pitschas*, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, 1984; *Simitis*, Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, 398 ff. Weitere Nachweise z. B. bei Scholz/Pitschas, FN. 1.

lung bei den Datenschutzbeauftragten vorzufinden; in deren Entschließung vom 27./28. März 1984 hat sie beredten Niederschlag gefunden.[6] c) Die dritte typische Antwort kann man als gesetzesförmlichen Grundrechtsleerlauf bezeichnen; sie kombiniert Teilelemente aus den beiden ersteren: ein formal detaillistischer Regelungsperfektionismus verbindet sich mit einer minimalen inhaltlichen Befugnisbegrenzung, die jedenfalls den status quo einer an der »Verwaltungseffizienz«[7] orientierten Praxis absichert, wenn sie nicht vielmehr noch deren Möglichkeiten erweitert. Auf dieser Linie bewegt sich der »Vorentwurf zur Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes des Bundes und der Länder«[8], wenn er in der Begründung (Teil A, 3.1.) davon ausgeht, daß die Datenerhebung und -verarbeitung der Polizei »im bisherigen Umfang zur Erfüllung der polizeilichen Aufgaben erforderlich ist und deshalb auch in Zukunft in diesem Ausmaß zulässig sein muß.« »Alle vorgesehenen Regelungen laufen daher im Prinzip auf eine präzisere gesetzliche Fixierung des ›Ist-Zustandes‹ hinaus.« Das ist zwar ehrlich, aber kaum im Sinne der Richter des VZG-Urteils.

Das ›menschlich‹ verständliche Bestreben der Verwaltungspraxis, nach Überwindung einer ersten Phase der rechtlichen Verunsicherung durch das Urteil möglichst bald wieder zum business as usual zurückzukehren, hat in so charakteristischer Weise theoretische Rückendeckung erfahren, daß dies einen Augenblick Aufmerksamkeit verdient: Die Rede ist von dem Versuch von *R. Scholz* und *R. Pitschas*, das soeben erst erblühte Grundrecht der informationellen Selbstbestimmung in der Konfrontation mit einer neu erfundenen verfassungsrechtlichen Figur, der »staatlichen Informationsvorsorge« und »Informationsverantwortung«, zu neutralisieren und es wieder verblassen zu lassen.

Die »*Informationsvorsorge*«, die ganz pauschal »aus dem Grundsatz der sozialen Rechtsstaatlichkeit (Art. 20 I, 28 I GG)« und einer daraus abzuleitenden »Aktionsvollmacht« »des Staates zur Sozialgestaltung schechthin«[9] verfassungsrechtlich legitimiert sein soll, findet prompt ihre polizeirechtliche Entsprechung und »Konkretisierung« in der polizeilichen Datenverarbeitung zum Zwecke der »*Gefahrenvorsorge*«: »Die Polizei kann personenbezogene Daten erheben, speichern, verändern und nutzen, soweit dies die Vorsorge zur Gefahrenabwehr erfordert«.[10] Eine ausgreifendere, schwammigere, stärker zum Mißbrauch einladende Generalklausel ist kaum formulierbar.

Der Ausgangspunkt – bei *Scholz/Pitschas* – ist ebenso zustimmungswürdig wie trivial: Die öffentliche Verwaltung könne ihre Aufgaben nur erfüllen, wenn sie über die dazu erforderlichen Informationen verfüge.[11] Aber schon der zweite Gedankenschritt impliziert die verhängnisvolle Weichenstellung, deren verfassungsrechtliche Haltlosigkeit allerdings aufgedeckt werden kann und muß: Der triviale Ansatz wird zu einer »prinzipalen Informationsfunktion der öffentlichen Verwaltung«, zu einer »*eigenständigen staatlichen Aufgabe der Informationsvorsorge*« überhöht.[12] Als ob es nicht eben genügte zu sagen, die Verwaltung solle diejenigen Daten erhalten, die sie – je nach gesetzlich umschriebener oder zugelassener (Art. 20 Abs. 3 GG!) Aufgabenstellung – für ihre Arbeit benötigt! Hat man erst einmal mit einem modisch klingenden Terminus eine Verwaltungsbanalität zur »genuinen Staatsauf-

6 Vgl. DÖV 1984, 504 ff.
7 Bejahend *Scholz/Pitschas*, S. 120, die im übrigen dem Typus a) zuzurechnen sind.
8 S. Anm. 4.
9 *Scholz/Pitschas*, S. 104.
10 So: Alternative B des Vorentwurfes (s. Anm. 4) zu § 72, der mit »Gefahrenvorsorge« überschrieben ist.
11 *Scholz/Pitschas*, S. 103.
12 Hervorhebung von *Scholz/Pitschas*, S. 104.

gabe« (S. 198) verfassungsrechtlich hochstilisiert, hat man diese ›Erfindung‹ außerdem mit einer weiteren Erfindung, nämlich dem »Grundrecht auf Sicherheit«[13], das in dieser Vagheit und Allgemeinheit auch nirgends im Grundgesetz steht, pseudorechtsstaatlich abgesichert, dann läuft alles weitere wie am Schnürchen. Am Ende sind die entscheidenden Erkenntnis- und Grundrechtsschutzgewinne des VZG-Urteils aufgezehrt: das Prinzip der bereichsspezifischen und präzisen Zweckbestimmung, das Verbot der Datensammlung auf Vorrat, das Verbot der Zweckentfremdung bzw. das Gebot des »amtshilfefesten« Schutzes gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote.[14] Es gibt dann »keinen allgemeininformations(hilfe-)rechtlichen Gesetzesvorbehalt« mehr[15], obschon das Bundesverfassungsgericht gerade in diesem Punkt[16] eine deutliche Sprache spricht. Beschränkungen des Rechts – und dazu gehören auch zweckvariierende Datenweitergaben – bedürfen einer gesetzlichen Grundlage. Und an die Stelle der bereichsspezifischen und präzisen gesetzlichen Zweckbestimmung[17] tritt – noch eine weitere Kompetenzen hervorzaubernde black box! – die »durch den grundsätzlichen Verwaltungszweck konstituierte Funktionseinheit behördlichen Handelns«.[18] Wen wundert es da noch, daß z. B. auch Polizei und Verfassungsschutz unter dem Topos einer »Funktionsidentität der Sicherheitsbehörden«[19], die jedenfalls einen »Zweckverbund« garantiert, zu unbeschränktem Informationsaustausch (»Vorsorge«-Prinzip!) verpflichtet und befugt sind und daß die geltenden Rechtsgrundlagen dafür eigentlich vollkommen ausreichen.[20] –

Wer sein datenschutz- und sicherheitsrechtliches Feld auf so kunstvoll gedüngtem und gepflügtem Boden des Grundgesetzes bestellen will, sollte die folgenden Ausführungen nicht mehr lesen. Sie sind der sicherlich unvollkommene erste Versuch eines seit zwei Jahrzehnten um rechtsstaatliche Präzision und Normenklarheit bemühten Polizeirechtlers, in diesem Bereich Konsequenzen aus dem VZG-Urteil zu ziehen. Der ursprüngliche Gutachten-Text wurde hier, besonders im Analyse-Teil (B.) aus redaktionellen Gründen erheblich gekürzt.

Zunächst wird eine Analyse des »juristischen Gehalts« des Urteils versucht und sodann in ausgewählten Anwendungsbereichen auf die notwendigen oder eventuell nur wünschenswerten Folgerungen für den Gesetzgeber und die Verwaltungspraxis eingegangen. Das Interesse konzentriert sich dabei auf das Aufgabenfeld der inneren Sicherheit, insbesondere den Bereich der Polizei. Die Notwendigkeit einer Novellierung der Datenschutzgesetze des Bundes und der Länder soll damit nicht geleugnet werden; ihre Bedeutung als bereichsübergreifender »Allgemeiner Teil« des Datenschutzrechtes steht außer Frage. Doch liegen wesentliche Folgeprobleme des Urteils gerade in der aufgabenspezifischen Umsetzung der mit generellem Geltungsanspruch entwickelten Kriterien. Besondere Aufmerksamkeit verdient dabei die Frage, ob und bis zu welchem Grade den Äußerungen des Gerichts der Charakter unmittelbar anwendbaren, zwingenden Rechts zukommt und inwiefern sie vielmehr nur als »soft law« oder gar nur als die Beschreibung eines idealen datenschutzrechtlichen Zielzustandes anzusehen sind.

13 *Dieselben*, S. 198, diese Erfindung stammt von *Isensee*, Das Grundrecht auf Sicherheit. Zu den Schutzpflichten des freiheitlichen Verfassungsstaates, 1983.
14 S. dazu im einzelnen unten B. III., BVerfGE 65, 1, 46 u. ö.
15 *Scholz/Pitschas*, S. 199.
16 Vgl. nur BVerfGE 65, 1, 44.
17 BVerfGE 65, 1, 46.
18 *Scholz/Pitschas*, S. 147.
19 *Dieselben*, S. 188.
20 *Dieselben*, S. 201, so als gäbe es keinen Grundsatz der Trennung von Verfassungsschutz und Polizei, dazu statt vieler *Denninger*, ZRP 1981, 231 ff.

Analyse und Folgenbetrachtung bleiben auch dort, wo sie in praktische Verwirklichungsvorschläge einmünden, im Rahmen einer normativen Untersuchung; der Verfasser versteht sich als Verfassungsrechtler, nicht als Informatik-Technologe. Er geht davon aus, daß rechtlich gebotene Kommunikationsschranken technisch auch realisierbar sind.

B. Analyse

I. Das Recht auf informationelle Selbstbestimmung (RiS); Inhalt und Funktion

1. Das Urteil zum Volkszählungsgesetz ist »*nicht* die *Geburtsstunde eines neuen Grundrechts*; und insbesondere nicht eines »Grundrechts auf Datenschutz«[21]. Weder der Sache noch der Bezeichnung nach ist das RiS eine »Erfindung« des Bundesverfassungsgerichts. In der Sache führt das Urteil die differenzierte Rechtsprechung des Gerichts zum allgemeinen Persönlichkeitsrecht weiter: Nachdem im Mikrozensus-Beschluß[22] das »Selbstbestimmungsrecht im innersten Lebensbereich« der menschlichen Persönlichkeit, im Lebach-Urteil[23] das Selbstbestimmungsrecht, »ob und inwieweit andere (s)ein Lebensbild im ganzen oder bestimmte Vorgänge aus (s)einem Leben öffentlich darstellen dürfen«, im Eppler-Beschluß[24] der Schutz gegen das Unterschieben nicht getaner Äußerungen und im Gegendarstellungsrecht-Beschluß[25] der Schutz vor Herabwürdigung zum bloßen Objekt öffentlicher Erörterung als Dimensionen des allgemeinen Persönlichkeitsrechts erkannt und anerkannt worden sind, werden nunmehr die Konsequenzen mit Bezug auf die elektronische (wie auf die herkömmliche aktenmäßige) Datenverarbeitung entwickelt. Der Ansatz dieser seit Jahrzehnten gefestigten (und sich ausdifferenzierenden) Rechtsprechung – vgl. nur etwa das Investitionshilfegesetz-Urteil 1954 oder das Lüth-Urteil 1958[26] – bei »Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt«[27], wird konsequent durchgehalten und im Schrifttum, unbeschadet der Kritik am »Wertordnungs-Denken« im einzelnen, im wesentlichen gebilligt[28].

Auch die Bezeichnung dieser Teilausprägung des allgemeinen Persönlichkeitsrechts als »Recht auf informationelle Selbstbestimmung« ist nicht neu. Seine wesentlichen Strukturen haben Steinmüller u. a. bereits 1971 in einem Gutachten im Auftrage des Bundesministers des Innern ausführlich beschrieben, wobei sie Termini wie »informationelles Selbstbestimmungsrecht über das eigene Person- bzw. Gruppenbild« oder »Selbstbestimmungsrecht des Bürgers über sein informationelles Personenmodell« einführten[29]. 1975 spricht Schwan von der »Freiheit vor staatlicher Informationssammlung«[30]; 1976 findet sich der Terminus »informationelles Selbstbestimmungsrecht« als Kapitelüberschrift bei C. Mallmann[31], das »informationelle Selbstbestimmungsrecht« erörtern Schatzschneider[32] und Podlech[33] 1979, Simon und Taeger[34] 1981. Im gleichen Jahr behandelt Denninger »Die Trennung von Verfassungsschutz und Polizei und das Grundrecht auf informationelle Selbstbestimmung«[35].

21 So zutreffend *Simitis*, NJW 1984, 398, 399; ebenso *Basten*, Prot. des Landtags Rheinland-Pfalz, 16. Sitzung 20. Januar 1984, Drcks. 10/802.

22 BVerfGE 27, 1, 7.

23 BVerfGE 35, 202, 220.

24 BVerfGE 54, 148, 153, 155; weitere einschlägige Entscheidungen s. BVerfGE 54, 154; 63, 131, 142; EuGRZ 1983, 588 = BVerfGE 65, 42.

25 BVerfGE 63, 131, 142 vom 8. 2. 1983.

26 BVerfGE 4, 7, 15 f.; 7, 198, 205 u. a. m.

27 EuGRZ 1983, 588 = BVerfGE 65, 41.

28 Vgl. statt vieler *Stern*, Staatsrecht I, 1977, S. 428.

29 *Steinmüller/Lutterbeck/Mallmann u. a.*, Grundfragen des Datenschutzes, Gutachten im Auftrag des BMI, 1971, BT-Drcks. VI/3826, bes. S. 81 ff., 88, 93.

30 *Schwan*, Datenschutz, Vorbehalt des Gesetzes und Freiheitsgrundrechte, Verwaltungsarchiv 1975, 120 ff., 131.

31 *C. Mallmann*, Datenschutz in Verwaltungs- und Informationssystemen, 1976, S. 47 ff.

32 *Schatzschneider*, Ermittlungstätigkeit der Ämter für Verfassungsschutz und Grundrechte, Frankfurter jur. Diss. 1979, S. 135/136.

33 *Podlech*, Das Recht auf Privatheit, in: Perels (Hrg.), Grundrechte als Fundament der Demokratie, 1979, S. 55.

34 *Simon/Taeger*, Rasterfahndung, 1981, S. 84.

35 *Denninger*, Die Trennung von Verfassungsschutz und Polizei und das Grundrecht auf informationelle

2. Verfügungsbefugnis über persönliche Daten als Bedingung autonomer Verhaltenssteuerung

Das Grundgesetz und seine Interpreten gehen davon aus, daß der Mensch »eine mit der Fähigkeit zu eigenverantwortlicher Lebensgestaltung begabte ›Persönlichkeit‹« ist[36]. Diese Lebensgestaltung kann nur gelingen, wenn der Einzelne nicht nur – abstrakt gesehen – sein eigenes Verhalten steuern kann, sondern wenn er dies tun kann, indem er zugleich die Verhaltenserwartungen und Verhaltensweisen der Mitmenschen in bezug auf seine Person zu beeinflussen vermag. Oder anders gesagt: Der Einzelne muß auf seine soziale Umwelt einwirken können, indem er selbst darüber entscheidet, ob, wo, wann und wie und in welchen Beziehungen er sich selbst seiner sozialen Umwelt darstellen will. In diesem Sinne hat N. Luhmann bereits 1965 die Freiheit- und Würde-Garantien des Grundgesetzes als »die äußeren und inneren Vorbedingungen der Selbstdarstellung als individuelle Persönlichkeit im Kommunikationsprozeß« analysiert[37].

3. Schutz der Entscheidungsfreiheit

Die hier gemeinte, durch Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geschützte Freiheit der Selbstdarstellung hat nichts mit einem theatralisch-pathetischen Sich-in-Szene-setzen-Wollen zu tun, auch nichts mit schauspielerischer Verstellung oder mit einem Rollenspiel, hinter dem sich ein »wahres Ich« zu verbergen suchte. Es geht vielmehr darum, daß der Einzelne seine Entscheidungen in komplexen sozialen Beziehungen, z. B. als Ehemann, Vater (bzw. Ehefrau, Mutter usw.), als Arbeitnehmer, Vereinsmitglied, Krankenkassenpatient, Subventionsempfänger, Steuerzahler, kommunalpolitisch oder auf anderer Ebene aktiver Bürger usw. »frei«, »autonom«, »selbstbestimmt«, »eigenverantwortlich« und letztlich: erfolgreich nur treffen kann, wenn er von möglichst zutreffenden Informationen und Einschätzungen über den Informations- und Wertungshorizont seiner Interaktionspartner ausgehen kann. Der Schutz der Freiheit der Selbstdarstellung durch das informationelle Selbstbestimmungsrecht hat insofern instrumentellen Charakter: Weil die Freiheit der Entscheidung des Einzelnen in sozialen Beziehungen, sein »Auch-anders-können« geschützt werden soll, muß der Einzelne in seiner »informationellen Selbstbestimmung« geschützt werden[38]. Deshalb wären mit dem RiS – hier übernimmt das Gericht eine Formulierung A. Podlechs[39] – »eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß«.

Das Gericht entnimmt dem Grundrecht der freien Entfaltung der Persönlichkeit die Befugnis des Einzelnen, »grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen«[40]. Überträgt man die – wohl bewußt untechnisch formulierten – Modalitäten der Datenpreisgabe und Datenverwendung in die rechtstechnische Sprache der Datenschutzgesetze, so unterliegt es keinem Zweifel, daß die Ausdrücke alle Phasen der Datenerhebung und der Datenverarbeitung (also das Speichern, Übermitteln, Verändern und Löschen, vgl. § 1 Abs. 1 BDSG) umfassen.

Selbstbestimmung, ZRP 1981, 231. Auch schon *derselbe*, JA 1980, 280. Vgl. ferner *Preis*, Verfassungsschutz und öffentlicher Dienst, 1982, S. 20ff.

36 Statt vieler: BVerfGE 5, 85, 204.

37 *Luhmann*, Grundrechte als Institution, 1965, S. 70, 77.

38 Klar herausgearbeitet von *W. Schmidt*, Die bedrohte Entscheidungsfreiheit, JZ 1974, 241.

39 *Podlech*, AK-GG Art. 2 I, Rz. 45. EuGRZ 1983, 588 = BVerfGE 65, 43.

40 EuGRZ 1983, 588 = BVerfGE 65, 43.

4. Relativierung der Sphärentheorie.

Mit dem Verständnis des RiS als grundsätzliche Verfügungsbefugnis über die eigenen persönlichen Daten hat das Gericht in der theoretischen und (verfassungsrechtlichen) Fundierung des Datenschutzes eine wichtige Weiche gestellt: Informationelle Selbstbestimmung ist nicht daten-, sondern verarbeitungsorientiert[41]. Nicht die abstrakte kategoriale Einordnung eines Datums je nach der größeren oder geringeren Nähe zum »innersten Lebensbereich« einer Person, nicht die Frage, ob es »von Natur aus Geheimniscbarakter« hat oder nicht[42], entscheidet über die Datenschutzwürdigkeit, sondern der konkrete *Verwendungszusammenhang*[43]. Das Zensus-Urteil geht von einem Nebeneinander beider Kriterien aus: Auf die »Art der Angaben« soll es nicht »allein« ankommen. »Entscheidend« seien vielmehr ihre Nutzbarkeit und Verwendungsmöglichkeit.

Der verarbeitungs- oder funktionsorientierte Schutz der informationellen Selbstbestimmung, von dem das Gericht nunmehr ausgeht, bildet die Grundlage für zwei wichtige Folgerungen, auf die noch näher einzugehen ist: 1. Der Gesetzesvorbehalt, dem Beschränkungen des RiS unterliegen, ist verwendungsspezifisch, d. h. anwendungsbereichsspezifisch auszufüllen; nur im Hinblick auf die typisierte Verwendungssituation kann die gesetzgeberische »Abwägung« zwischen einer Verarbeitung persönlicher Daten im Allgemeininteresse und dem Einzelinteresse an einer Kommunikationsbarriere erfolgen. Und 2.: Für jede individualisierte Datenwiedergabe muß grundsätzlich das Prinzip strenger Zweckbindung beachtet werden. Datenübermittlung soll dadurch nicht ausgeschlossen werden, sie darf aber nicht zur Aushöhlung der informationellen Selbstbestimmung führen (können). Eine fehlende oder generalklauselartig weite Zweckbindung bei der Datenübermittlung – wie sie etwa § 10 Abs. 1 Satz 1 BDSG vorsieht – könnte dazu führen, daß persönliche Daten zwar nur zu einem eng begrenzten Zweck erhoben und erstmalig gespeichert werden, danach aber für alle möglichen Verwaltungszwecke abgefragt und weitergegeben werden könnten, ohne daß der Betroffene noch irgend einen Einfluß darauf hätte.

5. Funktionsbedingung der freiheitlichen Demokratie

Informationelle Selbstbestimmung wird dem Einzelnen nicht allein zur Förderung seines privaten individuellen Wohles gewährleistet. Das Gericht begreift sie vielmehr auch als »eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens«[44]. Es unterstreicht damit die Bedeutung der Integrität der politisch bedeutsamen Kommunikationsgrundrechte wie der Versammlungs-, Demonstrations- oder Vereinigungsfreiheit, Art. 8, 9 GG, jener Grundrechte also, die zusammen mit der Meinungsfreiheit und den Rechten aus Art. 33, 38 GG den status constituens des Bürgers, seine staatshervorbringende Rechtsstellung umreißen[45].

Die Demokratie- und Gemeinwohlrelevanz des RiS ist nicht als ein beiläufig-

41 *Simitis*, NJW 1984, 402; ebenso schon *derselbe* in *Simitis/Dammann/Mallmann/Reh*, Kommentar zum BDSG, 3. Aufl. 1981, Einleitung, Rz. 28.

42 Vgl. aber BVerfGE 27, 7.

43 BVerfG EuGRZ 1983, 589 = BVerfGE 65, 45, *Simitis* (o. Anm. 41).

44 EuGRZ 1983, 588 re.Sp. = BVerfGE 65, 43. Vgl. die ganz ähnliche frühere Formulierung von *Simitis*, Datenschutz: Voraussetzung oder Ende der Kommunikation?, in: FS für H. Coing, Band II, 1982, S. 495 ff., 512.

45 Zum status constituens s. *Denninger* in *Denninger/Lüderssen*, Polizei und Strafprozeß im demokratischen Rechtsstaat, 1978, S. 9 f., 116 ff. Ferner *derselbe*, VVDStRL Heft 37, 1979 S. 26 ff. Dazu *Preu* (s. Anm. 35) S. 22. Zur Bedeutung des RiS für die Erhaltung des notwendigen kulturellen, wirtschaftlichen und politischen Innovationspotentials in einer demokratischen Gesellschaft vgl. den Bericht der

ornamentaler Hinweis des Gerichts abzutun. Vielmehr wird damit eine Linie der Rechtsprechung weiter ausgezogen, die früh mit grundsätzlichen Aussagen zur verantwortlichen Mitwirkungsmöglichkeit des Einzelnen in Angelegenheiten der res publica beginnt[46], die die Bedeutung der Urteilskraft und der Aktivität der Bürger für den politischen Willensbildungsprozeß hervorgehoben[47] und die Notwendigkeit der »Chance zur Identifikation« des Bürgers mit der Demokratie erkannt hat[48].

II. Allgemeine verfassungsrechtliche Kriterien für die Schrankenziehung gegenüber dem RiS

Als Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) unterliegt das RiS den gemäß Art. 2 Abs. 1 GG zugelassenen Freiheitsbeschränkungen; die beschränkende staatliche Gewalt (Legislative oder Exekutive) unterliegt ihrerseits den verfassungsmäßigen, hier besonders den aus dem Rechtsstaatsprinzip (Art. 20 Abs. 3, 19 Abs. 1 GG) sich ergebenden Schranken.

1. Ohne auch nur mit einem Wort etwa auf die »Wesentlichkeitstheorie« einzugehen, geht das Gericht hier von der Existenz eines *Gesetzesvorbehalts* aus. Auf der Basis der umfassenden Definition des RiS – Schutz gegen Preisgabe und Verwendung persönlicher Daten – ist das schlüssig. Jede Begrenzung der umfassenden individuellen Verfügungsbefugnis wirkt sich als »Eingriff« aus und fordert von daher eine gesetzliche Ermächtigung. Auf alte Streitfragen, z. B. unter welchen Voraussetzungen ein Informationseingriff anzunehmen sei[49], brauchte das Gericht nicht näher einzugehen, zumal nicht im Hinblick auf den eigentlichen Streitgegenstand: das Volkszählungsgesetz, vgl. § 6 Abs. 1 BStatG. Gleichwohl wären der Datenschutz- wie der Verwaltungsrechtler überhaupt gerade in diesem Punkte für eine kleine Zugabe an Deutlichkeit dankbar gewesen. Nach den Darlegungen des Gerichts steht einer weitgefaßten Datenverfügungsbefugnis des Einzelnen eine ebenso weitgefaßte, aber dem Gesetzesvorbehalt unterworfene Beschränkungsbefugnis des Staates im überwiegenden Allgemeininteresse gegenüber.

2. Eine rechtsstaatliche, gesetzlich normierte Schrankenziehung muß a) dem Grundsatz der *Normklarheit*, b) dem *Übermaßverbot* und c) den Erfordernissen des *Grundrechtsschutzes* durch organisatorische und verfahrensrechtliche Vorkehrungen genügen. Das Gericht erwähnt diese drei Prinzipien unter Hinweis auf Rechtsprechungsbelege, ohne die Einzelfolgerungen für die Ausgestaltung der Volkszählung unmittelbar hieran zu knüpfen. Vielmehr entwickelt es eine Reihe von kommunikationsspezifischen Kriterien, aus denen sich zum Teil konkrete Forderungen an den Gesetzgeber ableiten lassen.

III. Kommunikationsspezifische Ausprägungen der allgemeinen Grundsätze für eine grundrechtsgewährleistende Konkretisierungs- und Schrankengesetzgebung

Das Gericht erörtert die Kriterien für drei mögliche Arten der Erhebung persönlicher Daten[50]:

a) die Erhebung individualisierter[51], nicht anonymer Daten für Zwecke des »Verwaltungsvollzuges«,

Sachverständigenkommission »Staatszielbestimmungen/Gesetzgebungsaufträge«, hrg. vom BMI und BMJ, 1983, Rz. 222.

46 Vgl. BVerfGE 5, 85, 205.

47 BVerfGE 20, 56, 103.

48 BVerfGE 40, 237, 251.

49 Vgl. *Schwan*, o. Anm. 30; ferner *Schlink*, Die Amtshilfe, 1982, S. 169 ff., m. w. N. zum Streitstand.

50 BVerfGE 65, 45 ff.

51 »Individualisierung« meint hier die Möglichkeit der Zuordnung des Datums zu einem namentlich

b) die Erhebung, sei es anonymer, sei es nicht anonymer Daten für statistische Zwecke und
c) die Zulässigkeit einer »kombinierten Erhebung«, bei der gleichzeitig, aber auf verschiedenen Bögen Daten teils für Vollzugszwecke, teils für statistische Zwecke abgefragt werden.

Da die Verwendung anonymisierter Daten in aller Regel, jedenfalls soweit sie nicht nachträglich wieder individualisiert werden können, das RiS nicht verletzen kann, ist sie wesentlich weniger strengen Anforderungen unterworfen als die Erhebung und Verarbeitung individualisierter Daten.

1. Kriterien der Erhebung und Verarbeitung nicht anonymisierter personenbezogener Daten

a) Eine Beschränkung des RiS darf in jedem Falle nur zur Befriedigung eines überwiegenden Allgemeininteresses erfolgen. Unter diesem Gesichtspunkt scheiden solche Daten als Erhebungsobjekt aus, an deren Kenntnis »die Allgemeinheit«, d. h. der Staat, kein legitimes Interesse haben kann. Das Gericht nennt Daten ohne jeden »Sozialbezug«, »unzumutbare intime Angaben« und Selbstbezichtigungen. Da der »Sozialbezug« nicht erst vor der Wohnungstür beginnt, sondern natürlicherweise familieninterne Beziehungen einschließt, kommen in erster Linie innerpsychische Tatsachen als Daten ohne Sozialbezug in Betracht. Aber selbst diese gewinnen häufig einen Sozialbezug, so z. B., wenn die Glaubensüberzeugung sich in der Zugehörigkeit zu einer Religionsgemeinschaft niederschlägt und diese, wie Art. 136 Abs. 3 WRV i. V. m. Art. 140 GG zeigt, einer gesetzlich angeordneten Erhebung zugänglich gemacht wird.

Zu den Daten aus der »Intimsphäre«, deren »Preisgabe« in einer staatlichen Erhebung unzumutbar ist, gehören Daten des Sexualverhaltens, die im allgemeinen auch durch eine Schamschwelle besonders geschützt sind. Andererseits kann keineswegs das gesamte geschlechtliche Verhalten unter allen Umständen gegen jede Offenbarungspflicht geschützt sein; man denke hier nur an die Feststellung der Vaterschaft eines nichtehelichen Kindes, § 1600a BGB. Der Schutz vor dem Zwang zur Selbstbezichtigung entspricht einem wichtigen Grundsatz des Strafprozeßrechts, § 243 Abs. 4 StPO.

b) Neben das (organisationsrechtliche) Gebot der gesetzlichen Eingriffsermächtigung tritt als wichtigstes materiellrechtliches Kriterium das Übermaßverbot in Gestalt der Grundsätze der Zweckbestimmtheit, der Geeignetheit und der Erforderlichkeit. Der Grundsatz der »bereichsspezifischen und präzisen« Zweckbestimmung, den das Gericht aufstellt, ist zusammen mit den organisations- und verfahrensrechtlichen Vorkehrungen zu seiner Sicherung der wichtigste Grundsatz zum Schutze des RiS überhaupt. Er zwingt Gesetzgeber und Verwaltung, von einer mißverstandenen Vorstellung von der »Einheit der Staatsgewalt« endgültig Abschied zu nehmen, von der Vorstellung nämlich, nach der das Wissen einer bestimmten Behörde zugleich das (fiktive) Wissen aller anderen Zweige der Verwaltung bedeute[52].

Auch in diesem Punkt bringt das Zensus-Urteil keine »Kehre«, »Wende« oder auch nur sensationelle Neuigkeit gegenüber der bisherigen Rechtslage, sondern es zieht notwendige Konsequenzen aus der Anerkennung des Grundrechtsschutzes.

Die gefestigte Rechtsprechung des Bundesverwaltungsgerichts zur Bedeutung des Art. 35 GG geht seit langem davon aus, daß der Amtshilfegrundsatz des Grundgesetzes über Inhalt und Umfang der im Einzelfall zu leistenden Amtshilfe, auch qua »Informationshilfe«, nichts aussagt, sondern daß diese nur unter Berücksichtigung der bereichsspezifischen Vorschriften

bekannten Individuum, das ohne erheblichen Aufwand identifiziert werden kann. Ein »Hans Müller« oder »Franz Meier, Bundesrepublik Deutschland« wäre in diesem Sinne noch nicht individualisiert.

52 Zur Kritik schon *Denninger*, VVDStRL Heft 37, 1979, 40 f. Anm. 127. Vgl. ferner BVerfGE 31, 43, 46. Die Gegenkritik von *Scholz/Pitschas*, S. 114 FN. 390 unter dem Begriff der »Einheit der Verwaltung« geht fehl.

und der etwa einschlägigen Grundrechte bestimmt werden können[53]. Das Grundrecht auf informationelle Selbstbestimmung rangiert hier systematisch an erster Stelle.

Der Grundsatz der präzisen Zweckbindung ist die normative Antwort auf mehrere verfassungsrechtsdogmatisch zu trennende Anforderungen: Einerseits verwirklicht er das aus dem Rechtsstaatsprinzip abzuleitende Gebot der Normklarheit[54]: Der Bürger muß aus der gesetzlichen Regelung klar erkennen können, »für welche konkreten Zwecke des Verwaltungsvollzuges seine personenbezogenen Daten bestimmt und erforderlich sind«[55]. Andererseits trägt das Zweckbindungsprinzip den Elementen des Übermaßverbotes Rechnung: Die Zweckbestimmung muß soweit konkretisiert werden, daß ein Urteil darüber möglich wird, a) ob die Informationserhebung und -verarbeitung zur Zweckerreichung überhaupt tauglich ist (»Geeignetheitstest«), und b) ob sie nicht über das notwendige Mindestmaß hinausgeht (»Erforderlichkeitstest«). Gerade unter dem letztgenannten Gesichtspunkt werden zahlreiche Fälle des Datenverbunds durch »On-Line-Zugriff«, »Direktzugriff«, einer kritischen Überprüfung bedürfen, denn schon nach den Begriffsbestimmungen des BDSG, § 2 Abs. 2 Nr. 2, gilt das zum Abruf Bereithalten eines Datenbestandes als Datenübermittlung und damit als Datenverarbeitung.

Auch hiervon abgesehen bereitet es nahezu unlösbare Schwierigkeiten, abstrakt-begriffliche Kriterien für die Frage anzugeben, wann dem Grundsatz der präzisen Zweckbindung Genüge getan ist und wann nicht. Die Rechtsprechung des Bundesverfassungsgerichtes erleichtert die Antwort nicht wesentlich, wenn sie einerseits die Verwendung unbestimmter, der Auslegung und Konkretisierung bedürftiger Gesetzesbegriffe zuläßt, andererseits aber fordert, der Betroffene müsse die Rechtslage erkennen und sein Verhalten danach einrichten können[56]. Die bloße generalklauselartige Bezugnahme der bisherigen Datenschutzvorschriften auf die »rechtmäßige Erfüllung der in der Zuständigkeit« einer XYZ-Behörde liegenden Aufgaben[57] wird, wenn diese Aufgabenumschreibung ihrerseits sehr umfassend ist (z. B. »Gefahrenabwehr« oder »Verfassungsschutz«) den begrifflichen Anforderungen an eine präzise und konkrete Zweckbindung nicht gerecht. Andererseits ist kaum abzusehen, wie der Gesetzgeber in manchen Bereichen zu größerer Konkretion vordringen könnte, ohne in eine mangelhafte Kasuistik zu verfallen. Hier werden zusätzliche Eingrenzungsmerkmale – Abstellen auf den Einzelfall, strenge Prüfung der Erforderlichkeit, Beschränkung auf wenige Daten (Name, Wohnanschrift, Geburtsdatum) – sowie verfahrensrechtliche Sicherungselemente zum Zuge kommen müssen.

c) Anders als bei einer Erhebung zu statistischen Zwecken soll bei einer Erhebung für Zwecke des Verwaltungsvollzuges »das strikte *Verbot der Sammlung personenbezogener Daten auf Vorrat*« gelten[58]. Eine solche Vorrats-Sammlung »zu unbestimmten oder noch nicht bestimmbaren Zwecken« wäre mit dem Grundsatz der präzisen Zweckbindung nicht zu vereinbaren. Auch das Gebot des Mindesteingriffs führt zu diesem Ergebnis.

53 BVerwGE 38, 336, 340 f.; 50, 301, 310. *P. Krause*, Datenschutz und Grundgesetz, DVR 1980, 229 ff., Anm. 131, zitiert beide Entscheidungen als Beleg für die »Einheit der Staatsgewalt« – bezüglich des Terminus zutreffend für E 38, 336 ff. Daß aber das Bundesverwaltungsgericht gerade – im Sinne der hier vertretenen Auffassung – die Konkretisierungsbedürftigkeit des Amtshilfeprinzips aus Art. 35 GG hervorhebt, wird bei *Krause* verdunkelt.

54 Vgl. BVerfGE 45, 400, 420 m. w. N.

55 EuGRZ 1983, 594 links o. = BVerfGE 65, 62.

56 BVerfGE 37, 132, 142; 45, 420.

57 Vgl. statt vieler § 10 Abs. 1 BDSG, § 72 SGB-X.

58 EuGRZ 1983, 589 re. Sp. = BVerfGE 65, 47.

So einleuchtend das Verbot auf den ersten Blick erscheinen mag, so notwendig und lohnend ist es doch, einen Augenblick über seine Bedeutung nachzudenken. Denn im Grunde genommen ist jede Datei, ja, jede Aktensammlung eine »Sammlung von Daten auf Vorrat«. Es ist gerade der Sinn jeder Art von Informationsspeicherung – auf Listen, in Karteien, Akten oder Dateien –, daß man die Daten für zukünftige Gebrauchsfälle rasch verfügbar, also in diesem Sinne »vorrätig« hält.

Das Verbot der Sammlung auf Vorrat muß also einen eingeschränkten Sinn haben, wenn nicht die eigentliche Funktion der Informationsspeicherung getroffen werden soll. Die Einschränkung muß sich aus der gesetzlichen Zweckbestimmung ergeben. Verhindert werden soll, daß personenbezogene Daten »einfach drauflos« »für alle Fälle« gespeichert werden, ohne daß ein aktueller oder zukünftiger Bedarfsfall gesetzlich klar umschrieben wäre.

Das Gericht hatte im Streit über das Volkszählungsgesetz unmittelbar nur über die Erhebung von Daten zu statistischen Zwecken, sodann aber auch über die Verbindung dieser Erhebung mit dem sog. Melderegisterabgleich (§ 9 Abs. 1 VZG) und einigen anderen Übermittlungstatbeständen zu entscheiden. Die Ausführungen über das Verbot einer Datensammlung auf Vorrat können daher, soweit rein statistische Erhebungen in Rede stehen, nicht zu den die Entscheidung tragenden Gründen, sondern nur als ein obiter dictum angesehen werden. Dies ist zwar für den Umfang der Bindungswirkung des Urteils gemäß § 31 Abs. 1 BVerfGG von Bedeutung, an welcher die bloßen obiter dicta nicht teilhaben. Doch darf hieraus nicht etwa gefolgert werden, daß diese Darlegungen jeglicher rechtlichen Bedeutung entbehrten. Sie machen das Prinzip deutlich, von dem für statistische Erhebungen eine Ausnahme gilt. Sie sind als ein Hinweis des Gerichts auf seine Einschätzung der materiellen Rechtslage anzusehen, auf die Grundlage, von der aus das Gericht gegebenenfalls judizieren würde. Insofern können auch derartige obiter dicta auf Gesetzgeber und Verwaltung mittelbar eine dirigierende Wirkung ausüben.

d) Die grundsätzliche Anerkennung des RiS, auf der die ganze Argumentation des Gerichts basiert und die deshalb zu den tragenden Gründen der Entscheidung zu rechnen ist, hat unmittelbare Auswirkungen auf die im Grundgesetz, Art. 35 Abs. 1, verankerte und in §§ 4 bis 8 VwVfG näher geregelte Einrichtung der *Amtshilfe*[59].

Wenn es nämlich die ratio des RiS ist, daß der Bürger weiß – oder mindestens bei gehöriger Nachfrage wissen könnte –, »wer was wann und bei welcher Gelegenheit« über ihn weiß, und wenn der Grundsatz der bestimmten Zweckbindung der Datenerhebung und -verarbeitung der Sicherung dieses rechtlichen Schutzzweckes dient, dann liegt auf der Hand, daß das Prinzip der Amtshilfe ihm tendenziell gerade zuwiderlaufen kann. Denn Amtshilfe qua Informationshilfe bedeutet die Übermittlung von Daten an eine andere Behörde auf deren Ersuchen und zu deren Zweckverfolgung, ohne daß der Betroffene von diesem Vorgang Kenntnis erhalten muß. Während Amtshilfe der Tendenz nach den Ausgleich bestehender Informationsgefälle zwischen den Behörden bedeutet, fordert Datenschutz die »künstliche« Aufrechterhaltung bestimmter Kommunikationsbarrieren zwischen den einzelnen Zweigen der öffentlichen Verwaltung.

Wegen der verfassungsrechtlich geforderten gesetzlichen Zweckbindung der Datenverwendung fordert das Gericht auch einen »amtshilfefesten« Schutz gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote[60]. Eine nähere Erläuterung oder Eingrenzung dieser sehr pauschalen Feststellung gibt das Gericht nicht. Da nun aber nicht anzunehmen ist, das Gericht habe entgegen dem Grundsatz des Art. 35 Abs. 1 GG jegliche Amtshilfe als Informa-

59 S. vor allem *Schlink*, Die Amtshilfe 1982, ferner *Denninger*, Einführung in Probleme des Amtshilferechts, insbesondere im Sicherheitsbereich, JA 1980, 280 ff. und *derselbe*, Amtshilfe im Bereich der Verfassungsschutzbehörden, in: BMJ (Hrg.), Verfassungsschutz und Rechtsstaat, 1981, S. 19 ff.; *Bull*, Datenschutz und Ämter für Verfassungsschutz, ebenda, S. 133 ff., *Evers*, Verfassungsschutz und Polizei, ebenda, S. 65 ff.

60 EuGRZ, 1983, 589 re. Sp. = BVerfGE 65, 46.

tionshilfe unterbinden wollen, sind auch hier entsprechend den allgemeinen Kriterien bereichsspezifische Abwagungsregeln zu entwickeln.

Dabei ist zu erwarten, daß bei den Auseinandersetzungen um gesetzliche Einzellösungen auf diesem Felde die »Interessen« der Datenschützer und die »Interessen« der beteiligten Verwaltungsressorts besonders heftig aufeinander prallen werden. Wie auch in der bisherigen Diskussion werden dabei voraussichtlich zu zwei Grundfragen unterschiedliche Positionen und Argumente aufgebaut werden, zwei Fragen, denen für die gesamte Problematik »Datenschutz contra Amtshilfe«[61] Schlüsselcharakter zukommt. Es geht, in aller Kürze skizziert, um Folgendes:

Die erste Frage setzt grundrechtlich an und kann etwa so zugespitzt werden: Ist tatsächlich jede (personenbezogene) Informationsweitergabe, die zwischen verschiedenen Zweigen der öffentlichen Verwaltung ohne Einwilligung des Betroffenen erfolgt – z. B. zwischen den Sozialämtern und der Ausländerpolizei – schon als solche ein »Eingriff« in die grundrechtlich geschützte Individualsphäre, obwohl das betroffene Datensubjekt, der Bürger, von diesem Vorgang in aller Regel gar nichts erfährt und in seiner Handlungsfreiheit (und schon gar in seiner Meinungsfreiheit oder in anderen Grundrechten) unmittelbar nicht beeinträchtigt werde[62]? Wer diese Ausgangsfrage verneint, kann durchaus zur Bejahung vernünftiger und weitreichender Eingrenzungen einer uferlosen zwischenbehördlichen Informationshilfepraxis gelangen. Doch wird er sich zur Begründung dann nicht auf ein generelles grundrechtliches Informationsweitergabeverbot – etwa aufgrund des RiS – berufen, sondern auf den abgestuften Schutz konkreter Geheimnisbereiche[63]. Die Gegenposition kehrt gewissermaßen die Regel-Ausnahme-Situation um: Nicht muß im Einzelfall ein zugunsten des Betroffenen streitendes subjektives Recht auf Geheimnisschutz nachgewiesen werden, um die Informationshilfe zu unterbinden, sondern der auskunftsverpflichtete und -erteilende Bürger muß darauf vertrauen können, daß seine Daten nur für den bekannten Zweck verwendet werden[64]. Die Weitergabe der Information (an private Dritte wie an Stellen öffentlicher Verwaltung) ist dann die Ausnahme, die einer gesetzlichen Rechtfertigung durch überwiegende Allgemeininteressen bedarf.

Die zweite Frage in diesem Zusammenhang setzt staatstheoretisch und organisationsrechtlich an und ist auf die Funktionsbedingungen moderner Staatlichkeit gerichtet: Da wird auf der einen Seite das Prinzip der Einheit (oder Einheitlichkeit) der Staatsgewalt ins Feld geführt, als dessen Ausdruck das Amtshilfegebot die einheitsgefährdende Wirkungen der Gewaltentrennung und Behördenaufgliederung kompensiere[65]. Die Gegenargumentation deutet den Amtshilfegrundsatz umgekehrt als eine Bestätigung der rechtsstaatlich unverzichtbaren Gewaltenteilung und der »Uneinheit« der Staatsgewalt, deren Friktionen durch die Amtshilfeverpflichtung abgemildert würden[66]. Auf der abstrakten Höhe dieses Argumentationsniveaus kann ein Regel-Ausnahme-Verhältnis zwischen Amtshilfeleistung und Informa-

61 So der Titel eines grundlegenden, auch die staatstheoretischen Implikationen mitberücksichtigenden Aufsatzes von *H. P. Bull*, DÖV 1979, 689 ff.

62 Vgl. z. B. *Loschelder*, Rasterfahndung – polizeiliche Ermittlung zwischen Effektivität und Freiheitsschutz, Der Staat 1981, 349 ff., 366 m. w. N.

63 Z. B. *Krause*, (Anm. 53), 245 ff.

64 *Wiese*, Der Schutz des Sozialgeheimnisses, DRV 1979, 172; vgl. auch *Benda*, in: FS für W. Geiger, 1974, S. 23 ff., 38.

65 *Krause*, (Anm. 53), 259 mit Hinweis auf BVerfGE 31, 43, 46. *Scholz/Pitschas*, S. 118 sprechen von der »Einheit des Staatsorganismus«. Sie stellen dann auf die Informationseinheit durch »funktionalen Zweckverband« ab, S. 120. Dieses Kriterium ist, für sich genommen, zu unbestimmt. Besser ist es, auf aufgabenbezogenen Zweckeinheiten abzustellen, vgl. u. (III 4.b).

66 *Bull* (Anm. 61), 691.

tionsschutz in der einen wie auch in genau der entgegengesetzten Richtung konstruiert und »begründet« werden; beides bleibt gleichermaßen unbefriedigend. Noch einen Schritt weiter geht die Datenschutzverteidigung und wird damit gleichsam offensiv, wenn auf dem Wege über einen »Grundsatz der Systemdifferenzierung der öffentlichen Verwaltung« das normative Prinzip der Einheit der Rechtsordnung durch ein »empirisches Prinzip der Konkurrenz der staatlichen Teilsysteme« ersetzt werden soll[67]. Die Sicherung der für den Bürger notwendigen Freiheitsspielräume, so die dem zugrundeliegende Vorstellung, könne angesichts des in der Datenverarbeitung erreichten Technisierungsgrades nur noch dadurch gewährleistet werden, daß (in bezug auf Bürgerdaten) gegeneinander informationell abgeschottete Einzelverwaltungen jeweils ihre »Interessen« konkurrierend verfolgen und dadurch auch die je bereichsspezifisch verwalteten Bürgerinteressen zur Geltung bringen. Der Einwand, daß eine solche Konkurrenzstrategie leicht in eine die staatliche Leistungsfähigkeit mindernde Blockadestrategie zum Schaden des Bürgers ausarten könnte, erscheint hier nicht unberechtigt[68].

Eine verfassungsgemäße Antwort auf das Problem »Datenschutz contra Amtshilfe« muß die beiden Teilaspekte, den grundrechtlichen und den organisationsrechtlichen, zusammenführen und versuchen, beiden gerecht zu werden. Das Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz gibt eine solche synthetische Antwort, die übrigens die gleichen Elemente aufnimmt wie die Antwort des Landesverfassungsgesetzgebers von Nordrhein-Westfalen in Art. 4 Abs. 2 LaVerfNW[69]: Dem grundsätzlich anerkannten Anspruch des Bürgers auf Schutz seiner personenbezogenen Daten steht die grundsätzliche Eingriffsbefugnis des Staates – sei es im Wege der Amtshilfe, sei es in anderer Weise – im überwiegenden Interesse der Allgemeinheit und aufgrund eines Gesetzes gegenüber. Alle Regel-Ausnahme-Konstruktionen in der einen oder der anderen Richtung werden an dieser aufrechterhaltenen Grundspannung zunächst einmal zuschanden: das erste – und im Normalfall auch letzte – Wort hat hier der Gesetzgeber.

Das bedeutet zweierlei: 1. Auch die Datenverarbeitung als »Informationshilfe« steht unter Gesetzesvorbehalt, auch sie stellt einen Eingriff in das RiS dar[70]. Auf die Kenntnis des Datensubjekts kommt es nicht entscheidend an: Hat der Bürger keine aktuelle Kenntnis vom zwischenbehördlichen Informationsaustausch, muß er ihn aber für möglich halten, so beeinträchtigt schon dies seine Entscheidungsfreiheit und beeinflußt seine Verhaltensweisen. Wird aber der Vorgang der Datenverarbeitung dem Bürger mitgeteilt und ohne Rücksicht auf sein Einverständnis vollzogen, so liegt in dieser bewußten Negierung des RiS eine Herabwürdigung des Betroffenen zum bloßen Informationsobjekt, sofern nicht überwiegende Gemeinwohlinteressen den Eingriff rechtfertigen. 2. Es ist durchaus anzuerkennen, daß Art. 35 Abs. 1 GG eine aktuell geltende und ausreichende Rechtsgrundlage für Amtshilfeleistung in all den Fällen abgibt, in denen keine personenbezogenen Daten im Spiele sind. Ist das letztere der Fall, bedarf es keiner speziellen gesetzlichen Eingriffsgrundlage, in der die vom Gesetzgeber geforderte Abwägung zwischen Einzel- und Allgemeininteresse zum Ausdruck kommt.

67 *Podlech*, Datenschutz im Bereich der öffentlichen Verwaltung, DVR Beiheft 1, 1973, S. 39 f.

68 *Benda*, (Anm. 64), S. 39.

69 Art. 4 Abs. 2 LaVerfNW lautet: »Jeder hat Anspruch auf Schutz seiner personenbezogenen Daten. Eingriffe sind nur in überwiegendem Interesse der Allgemeinheit auf Grund eines Gesetzes zulässig.«

70 Dazu schon *Schlink*, (Anm. 49), S. 202. Der »Abschied« vom informationellen Selbstbestimmungsrecht, den *Evers* (Anm. 59), S. 75, glaubt feststellen zu können, hat, wenn es denn überhaupt einer war, nicht lange gedauert. Wie hier im Ergebnis auch der Bundesbeauftragte für den Datenschutz in seiner Stellungnahme für den Innenausschuß des Deutschen Bundestages vom 25. 4. 1984 – BfD – I – 192 100/15 – S. 16.

e) An mehreren Stellen des Urteils geht das Gericht auf die Frage der Verfassungsmäßigkeit einer *Zusammenfügung personenbezogener Daten zu einem »totalen« oder partiellen »Persönlichkeitsbild«* oder »Persönlichkeitsprofil« ein[71].

Zunächst wird die besondere Schutzbedürftigkeit der informationellen Selbstbestimmung u. a. mit der aus integrierten Informationssystemen entstehenden Gefahr begründet, daß die Daten zu einem »teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt« würden, »ohne daß der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren« könne. An anderer Stelle wird die Erschließung eines Datenverbundes durch ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal als verfassungswidrig erwähnt, »denn eine umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger ist auch in der Anonymität statistischer Erhebungen unzulässig (BVerfGE 27, 1/6f)«. Auch hier kann das Gericht also an frühere Rechtsprechung unmittelbar anknüpfen. Das einheitliche Personenkennzeichen »oder dessen Substitut« wird auch noch in anderem Zusammenhang als ein »entscheidender Schritt« in Richtung auf einen verfassungswidrigen Zustand bezeichnet.

Dieser Befund macht zunächst deutlich, daß das Gericht die Erstellung eines »Persönlichkeitsprofils« jedenfalls als mit der Menschenwürde und mit dem RiS unvereinbar ansieht, wenn hierunter »das systematische Erheben von Informationen über eine Vielzahl von Lebensbereichen des Betroffenen durch rechnerunterstützte Ausschöpfung von Informationsquellen[72] verstanden wird. Hiermit wird die tendenziell vollständige Registrierung und Katalogisierung der Persönlichkeit als verfassungswidrig verworfen. Bemerkenswert ist, daß das Gericht darüber hinaus in erweiternder Rezeption der Formulierung aus dem Mikrozensus-Beschluß (E 27, 6) mehrfach auch die Herstellung bloßer »Teilabbilder der Persönlichkeit« in das Verdikt einbezieht. Die Verwendung dieses Begriffs wirft allerdings eine Reihe nicht leicht zu beantwortender Fragen auf.

Was ist hier aus überwiegenden Gemeinwohlgründen noch gerechtfertigt, wo beginnt die Zone der menschenwürdeverletzenden Persönlichkeitsabbildung? Darf beispielsweise die Kriminalpolizei die Reisebewegungen Verdächtiger oder nur potentiell Verdächtiger systematisch beobachten und aufzeichnen, wenn sie hofft, auf diese Weise einem Rauschgift- oder Waffenhändlerring oder einer terroristischen Gruppe auf die Spur zu kommen? Dürfen die Ämter für Verfassungsschutz unter entsprechenden, ihrer Aufgabenbeschreibung gemäßen Voraussetzungen das »politische Verhalten« möglicher »Verfassungsfeinde« (also ihren Versammlungsbesuch, ihre Konferenzen, Reisen, Kontakte, Verhaltensweisen im Wahlkampf usw.) registrieren oder ergäbe dies bereits ein unzulässiges Teilabbild der Persönlichkeit?

Auf diese Fragen nach den praktischen Konsequenzen gibt das Zensus-Urteil keine Antworten. Sie waren freilich auch nicht Streitgegenstand des Verfahrens. Unter Berücksichtigung der früheren Rechtsprechung wird man jedoch folgendes als gefestigte Rechtsauffassung des Bundesverfassungsgerichts festhalten müssen:
1. Die Herstellung tendenziell vollständiger oder nahezu umfassender Persönlichkeitsbilder (-profile) verstößt in jedem Falle gegen das RiS.
2. Die Herstellung partieller Persönlichkeitsbilder (Reisebewegungsbilder, Profile politischen Verhaltens etc.) kann u. U. gegen das allgemeine Persönlichkeitsrecht in Verbindung mit dem Menschenwürdesatz verstoßen. Mit Hilfe des Güterabwägungsgrundsatzes und des Übermaßverbotes sind hierzu genauere Kriterien zu entwickeln.

f) Das Gericht widmet den *grundrechtssichernden Regelungen der Organisation und des Verfahrens* besondere Aufmerksamkeit, allerdings, dem Verfahrensgegenstand entsprechend, bezogen auf eine verfassungsgemäße Durchführung einer statisti-

71 Vgl. Abschnitt C II 1a des Urteils = EuGRZ 1983, 588 li. Sp. = BVerfGE 65, 42; C III 1a = 591 li. Sp. = BVerfGE 65, 53; C III 1 c)bb = 592 li. Sp. = BVerfGE 65, 56f.

72 So § 12 AEPolG, *Arbeitskreis Polizeirecht*, 1979, S. 55. Die Formulierung stammt von *A. Podlech*.

schen Erhebung[73]. Darüber hinaus betont es jedoch schon bei den allgemeinen Darlegungen zum RiS, der Gesetzgeber habe angesichts der gestiegenen Gefährdungen mehr als früher auch organisatorische und verfahrensrechtliche *Schutzvorkehrungen* zu treffen. Die einschlägige Rechtsprechung wird zitiert[74]. Dazu gehört etwa, daß das Verfahrensrecht der Grundrechtsausübung nicht so hohe Hindernisse entgegensetzen darf, daß die Gefahr einer Entwertung der materiellen Grundrechtsposition entsteht[75].

g) Zu den wichtigsten, weil wirksamsten Maßnahmen der Grundrechtssicherung gehört eine fortlaufende *Kontrolle der Einhaltung der Datenschutzvorschriften* im »Verwaltungsalltag«. Für diese Aufgabe sehen die geltenden Datenschutzgesetze die Einrichtung *unabhängiger Datenschutzbeauftragter* innerhalb wie außerhalb der öffentlichen Verwaltung vor[76].

Das Gericht erkennt die Bedeutung einer solchen Einrichtung sowohl generell als auch im Zusammenhang mit der Löschung der Hilfsmerkmale bei statistischen Erhebungen (vgl. § 11 Abs. 7 BStatG) ausdrücklich an. Eine nähere Beschreibung der einem Datenschutzbeauftragten mindestens zuzuweisenden Kontrollbefugnisse, damit er seine Aufgaben wirksam wahrnehmen kann, gibt das Urteil allerdings nicht. Immerhin wird die Funktion des Datenschutzbeauftragten »auch im Interesse eines vorgezogenen Rechtsschutzes« gesehen[77].

2. Kriterien der Erhebung und Verarbeitung personenbezogener Daten für statistische Zwecke

Dem konkreten Prüfungsanlaß entsprechend liegt der Schwerpunkt der Entscheidung hinsichtlich des Umfangs und der Behandlung von Detailfragen bei der Erörterung der *verfassungsrechtlichen Bedingungen für statistische Erhebungen*, insbesondere aufgrund gesetzlich angeordneter Bürgerbefragungen (Zensus, Mikrozensus). Die Grundsätze, die das Gericht für diesen Bereich entwickelt, sollen hier gleichwohl nur knapp resümiert werden, da das Schwergewicht der hier vorzunehmenden Analyse und Folgeuntersuchung weniger bei Fragen einer verfassungsgemäßen Statistik als vielmehr bei der datenschutzrechtlichen Durchdringung des Handelns der Sicherheitsbehörden liegen soll.

a) Die normativen Besonderheiten einer Datenerhebung für statistische Zwecke ergeben sich zunächst aus dem *Zweck einer Statistik*. Er geht dahin, für zahlreiche politische Entscheidungen, für im engeren Sinne »planerische« wie für nichtplanerische, grundlegende, vor allem auch quantitative Daten über Zusammensetzung und soziale Struktur der Bevölkerung in bestimmten Räumen sowie sonstige, ökonomisch, sozialpolitisch oder ökologisch wichtige Informationen verfügbar zu halten. Die gleiche Information kann in sehr verschiedenen Handlungszusammenhängen benötigt werden. Im Hinblick auf diese Situation ergeben sich Besonderheiten gegenüber der »nichtstatistischen« Erhebung und Verarbeitung personenbezogener Daten:

(1) Der Grundsatz der präzisen und konkreten Zweckbestimmung kann für statistische Erhebungen nicht gelten. Diese sind mehrzweckbezogen oder *›multifunktional‹*, soweit es sich nicht um spezielle Erhebungen handelt, die nur »zur Erfüllung bestimmter, im Zeitpunkt der Erhebung schon festliegender Bundeszwecke erforderlich« sind (vgl. § 6 Abs. 2 Nr. 1 BStatG).

73 Abschnitt C II 2 a) bb) des Urteils, C III 2., BVerfGE 65, 47 ff., 58 ff.
74 Zuletzt: BVerfGE 63, 131, 143, m. w. N.
75 S. vorige Anm.
76 Vgl. z. B. §§ 17, 28, 38 BDSG.
77 Vgl. Abschnitt C II 2a = EuGRZ 1983 589 re. Sp. = BVerfGE 65, 46.

(2) Der *relativen Zweckunbestimmtheit* statistischer Daten entspricht ihr Charakter als Information »auf Vorrat«. Das Verbot der Datensammlung auf Vorrat wäre, eng interpretiert, in diesem Bereich sinnwidrig. Der Gesetzgeber, der eine statistische Erhebung anordnet, kann zu diesem Zeitpunkt nicht absehen, in welchen Fällen und Zusammenhängen ein Datum belangvoll werden kann.
(3) Es ist nur folgerichtig, daß die Mehrzweckbestimmtheit der statistischen Erhebung auch die grundsätzliche Möglichkeit der Weitergabe und sonstigen Verarbeitung der Daten bedingt. Allerdings ist diese Möglichkeit der Verwendung zu statistischen Zwecken begrenzt. Das heißt, daß diese Daten bereits anonymisiert sein müssen. Eine Weitergabe in individualisierter, nichtanonymer Form unterläge hingegen dem Verbot der Zweckentfremdung in aller Strenge.
b) *Trennung von Statistik und Vollzug:* Der Erfolg einer statistischen Erhebung aufgrund von Bürgerauskünften hängt entscheidend von der Bereitwilligkeit der Befragten ab, richtige und vollständige Auskünfte zu geben. Dies kann jedoch nur erwartet werden, wenn der Bürger sicher sein darf, infolge der Auskunftserteilung nicht irgendwelche Nachteile durch Verwaltungsmaßnahmen zu erleiden. Diese Überlegung führt zu dem Grundsatz einer strikten Trennung von Informationserhebungen und -verarbeitungen zu statistischen Zwecken von entsprechenden Informationsvorgängen zu anderen Verwaltungszwecken, nämlich solchen des »Verwaltungsvollzuges«.

Die verschiedenen Tatbestände des § 9 VZG 1983 – Absatz 1: Der »Melderegisterabgleich«; Absatz 2: Übermittlung von Einzelangaben an oberste Bundes- und Landesbehörden; Absatz 3: Übermittlung zu Planungs-, Vermessungs- und Umweltschutzzwecken – hielten der verfassungsrechtlichen Prüfung am Maßstab des Grundsatzes der Trennung von Statistik und Vollzug nicht stand. Dieser Grundsatz veranlaßte das Gericht auch, deutliche Bedenken gegen die Zulässigkeit einer »kombinierten Erhebung« (vgl. o. III., vor 1.) zu statistischen und zu Vollzugszwecken kundzutun, obgleich es nicht abschließend zu dieser Frage Stellung nehmen wollte[78].

c) Das *Statistikgeheimnis*, wie es z. B. in den Vorschriften des § 11 BStatG ausformuliert und in § 203 Abs. 2 StGB strafrechtlich sanktioniert worden ist, gehört zu den wichtigsten rechtlichen Instrumenten, um die Beachtung des *Grundsatzes der Trennung von Statistik und Vollzug* zu gewährleisten. Die Geheimhaltungspflicht wirkt persönlich und organisatorisch; sie trifft die mit statistischen Erhebungen befaßten Amtswalter ebenso wie die zuständigen Behörden. In beiderlei Hinsicht stellt sich die Frage nach den Grenzen der Pflicht zur »Geheimhaltung«, d. h. zur Nichtweitergabe von »Einzelangaben«. Es leuchtet beispielsweise ohne weiteres ein, daß eine Übermittlung zwischen den mit der Durchführung einer Statistik betrauten Personen zulässig sein muß, soweit sie zur Aufgabenerfüllung erforderlich ist, vgl. § 11 Abs. 2 BStatG, s. auch § 203 Abs. 2 Satz 2, 2. Halbs. StGB. Das Gericht fordert, neben einer möglichst frühzeitigen (faktischen) Anonymisierung der Daten und wirksamen Vorkehrungen gegen eine Deanonymisierung vor allem »wirksame Abschottungsregelungen nach außen«[79]. Damit sind, wie insbesondere die Ausführungen zu § 9 Abs. 3 VZG ergeben[80], keineswegs nur der private und der öffentliche Bereich außerhalb der Verwaltung gemeint, sondern auch alle Stellen »vollziehender« und »planender« Verwaltung außerhalb der Statistik-Behörden.

78 EuGRZ 1983, 593, IV. 1. = BVerfGE 65, 61.
79 EuGRZ 1983, 590 li. Sp. = BVerfGE 65, 49.
80 EuGRZ 1983, 595 = BVerfGE 65, 55.

I. Grundrechtssichernde Implementation des Gesetzesvorbehalts

1. Der *Schutzbereich* des RiS ist, folgt man dem Gericht, weit gefaßt. Er erstreckt sich auf die *Erhebung, Speicherung, Übermittlung* und (»natürlich auch«) auf die *sonstige Verarbeitung* personenbezogener Daten. Entsprechend weit gefaßt – und dies folgt der allgemeinen Linie der Auslegung zu Art. 2 Abs. 1 GG im übrigen – ist der Gesetzesvorbehalt, der gesetzliche Beschränkungen des Grundrechts ermöglicht. Insbesondere im Sicherheitsbereich wird sich das Bedürfnis zeigen, Informationseingriffsbefugnisse entsprechen den oben zu B., II., III., dargestellten Kriterien genauer zu regeln. Dabei gerät der Gesetzgeber in eine doppelte Versuchung: *Erstens* besteht die Gefahr einer mehr oder weniger totalen »Verrechtlichung«, besser: »Vergesetzlichung«, indem der Gesetzgeber in formaler Weise zwar dem Verfassungsgebot Genüge tut, in der Sache jedoch lediglich die von der Exekutive behaupteten »Sachzwänge« normativ nachzeichnet. Da jedes »überwiegende Allgemeininteresse« grundsätzlich geeignet ist, eine Beschränkung des RiS zu rechtfertigen, und da der hohe Rang der »Sicherheit des Staates und seiner Bevölkerung« zum gesicherten Bestand der Verfassungswerte-Rechtsprechung des Bundesverfassungsgerichts gehört[81], sind die Konsequenzen sowohl für die vom Gesetzgeber in abstracto vorzunehmende Abwägung zwischen Allgemeininteresse und Einzelgrundrecht, zumal bei einem so »ätherischen« Recht wie dem RiS, als auch für die konkrete Einzelfall-Abwägung der ausführenden Behörde unschwer vorauszuschätzen. Das exekutivisch interpretierte »Gemeinwohlinteresse« wird sich allemal durchsetzen.

Die *zweite*, sachlich mit der ersten zusammenhängende Gefahr besteht darin, daß die Eingriffsbefugnisse der Behörde, sei es zur Datenerhebung und -speicherung, sei es zur Datenübermittlung, lediglich an die Erfüllung einer vagen Generalklausel »gebunden« werden, etwa an die – in den Datenschutzgesetzen beliebte – Erforderlichkeit zur rechtmäßigen Aufgabenerfüllung (vgl. o. bei Anm. 57). Wird der Aufgabenbereich dann ebenfalls nur mit einer weiten Generalklausel – z. B. »Gefahrenabwehr« oder »Schutz der freiheitlichen demokratischen Grundordnung« (vgl. Art. 73 Nr. 10b GG) – umschrieben, dann gewinnt die gesetzesanwendende Behörde für die Beurteilung dessen, was »erforderlich« ist, einen kaum eingegrenzten Spielraum.

Gibt der Gesetzgeber dieser doppelten Versuchung nach, so wird das Zensus-Urteil, zumal im Sicherheitsbereich, praktisch folgenlos bleiben. Das Recht wird einmal mehr seinen Funktionsverlust als freiheitssichernder Instanz dokumentieren, der Polizeipraktiker kann zur elektronisch perfektionierten Tagesordnung übergehen. Nimmt hingegen der Gesetzgeber das RiS in seinem substantiellen Gehalt (wie er oben zu B. I. beschrieben wurde) ernst, so muß er sich einzelfallbezogene, wenngleich typisierende Abwägungen und konkrete Zweckvorstellungen für Befugnisregelungen abfordern. Das im Polizeirecht jetzt durchweg anerkannte *Prinzip der Trennung von Aufgabennorm und Befugnisnorm*, das jedenfalls den einfachen Schluß von der Aufgabenzuweisung auf die Zulässigkeit des Einsatzes aller zwecktauglichen Mittel verbietet, muß dann auch für die Normierung des staatlichen Informationsverhaltens im Sicherheitsbereich leitend sein.

2. Eine weitere grundsätzliche Frage, die der Gesetzgeber angesichts des Zensus-Urteils erneut stellen und beantworten muß, betrifft das Verhältnis von *Fachgesetz-*

81 Mindestens seit BVerfGE 49, 24, 56 f.

gebung zu Querschnittgesetzgebung. Oder konkret gefragt: Empfiehlt es sich, den durch das Urteil ausgelösten Regelungsbedarf durch eine Ergänzung der vorhandenen Querschnittgesetze, also insbesondere des Hessischen Datenschutzgesetzes (und, entsprechend, des BDSG) und des Hessischen Verwaltungsverfahrensgesetzes (und, entsprechend, des BVwVfG) zu befriedigen? Im BDSG böte sich vor allem eine Ergänzung des Zweiten Abschnitts (und in den Landesgesetzen die der entsprechenden Gesetzesteile) an; in den Verwaltungsverfahrensgesetzen wäre in erster Linie an eine Erweiterung der *Amtshilfevorschriften* (z. B. §§ 4–8 HVwVfG) um ein Kapitel »Informationshilfe« zu denken. Als Alternative hierzu käme ein Ausbau des »bereichsspezifischen Datenschutzes« in den einzelnen Fachgesetzen, also beispielsweise für den Bereich der polizeilichen Gefahrenabwehr eine Ergänzung des HSOG in Betracht.

Die Nützlichkeit einer Verbesserung und Vervollständigung der Querschnitt-Regelungen soll hier im Grundsatz nicht angezweifelt werden; doch sind einige rechtssystematische Erwägungen anzustellen, welche für eine *primäre* Regelung der bereichsspezifischen Informationsverarbeitung in den *Fachgesetzen* sprechen: Die Ausfüllung des Gesetzesvorbehaltes soll einerseits einer wirksamen Grundrechtssicherung, der informationellen Selbstbestimmung dienen. Andererseits darf der Datenschutz »nicht zur generellen Staatsverhinderung führen«[82]. Der Gesetzgeber darf sich, will er beiden Aufgaben gerecht werden, nicht mit einer nichtssagenden, weil allgemein bleibenden Wiederholung des Verhältnismäßigkeitsgrundsatzes begnügen, sondern er muß eine »materielle«, »inhaltliche« Gewichtung beider Belange, des individualschützenden Regelungszwecks und des »Gemeinwohlinteresses« vornehmen. Er wird nicht umhin können, an typisierten Beispielen zu verdeutlichen, wie ›hoch‹ oder ›niedrig‹ er die Eingriffsschwelle, wie ›weit‹ oder ›eng‹ er die Grenze zulässiger Eingriffe im Hinblick auf bestimmte Gefahrenlagen gezogen wissen will. Eine solche Vorgehensweise entspricht rechtsstaatlichen Grundsätzen; das Polizeirecht und die Strafprozeßordnung – vgl. etwa die Katalogtaten des § 100a StPO als Voraussetzungen eines schweren Eingriffes: der Überwachung des Telefonverkehrs – bieten zahlreiche mehr oder weniger geglückte Beispiele. Es leuchtet aber ein, daß solche ins Einzelne gehenden materiellen Abwägungen den begrifflichen Rahmen wie auch die praktischen Möglichkeiten eines »Querschnittsgesetzes« sprengen würden.

II. Kriterien polizeilicher Informationsverarbeitung und Typologie polizeilicher Maßnahmen – Prävention und Repression

Ein Gesetzgeber, der nicht nur zufallsbezogene Flickwerksarbeit leisten, sondern prinzipiengesteuerte maßstabsgerechte Problemlösungen vorlegen will, wird versuchen, den Katalog informationsspezifischer Verfassungskriterien mit einer Typologie der informationserheblichen polizeilichen Maßnahmen zu konfrontieren, um sodann diese an jenen messen zu können. Dabei ist von vornherein zu berücksichtigen, daß zahlreiche polizeiliche Maßnahmen *doppelfunktional* sind: Sie dienen zugleich der Gefahrenabwehr und -verhütung wie auch der Straftatverfolgung. Die doppelte Zweckbestimmung ist gerade bei der Informationsverarbeitung häufig nur latent vorhanden: Eine Spurendokumentation im Zusammenhang mit einer konkreten Fahndung (Repression) kann außerdem bei der späteren vorbeugenden Verbrechensbekämpfung benutzt werden; präventiv aufgenommene und gespeicherte erkennungsdienstliche Unterlagen (vgl. z. B § 45a HSOG) erweisen sich bei einer

82 Insoweit zutreffend *M. Kloepfer*, Datenschutz als Grundrecht, 1980, S. 23.

späteren konkreten Täterfahndung als »Treffer« usw. Besondere gesetzgeberische Probleme ergeben sich hierbei aus der unterschiedlichen Gesetzgebungskompetenz des Bundes und der Länder. Im Folgenden wird der *Gefahrenabwehraspekt* und damit die Landeszuständigkeit zur Gesetzgebung in den Mittelpunkt gerückt. Das schließt nicht aus, daß dieselbe oder eine gleichartige Informationsverarbeitungsmaßnahme nicht auch unter repressiven, also strafprozessualen Gesichtspunkten zu betrachten wäre, denen etwa mit einer Novellierung der StPO durch den Bundesgesetzgeber Rechnung zu tragen wäre[83].

In erster Linie kommt also, unter Berücksichtigung des zu C I.1. Ausgeführten, eine *Ergänzung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG)* in Betracht. Die informationsspezifischen Verfassungskriterien, die dabei besonders zu beachten sein werden, wurden in Teil B. III. näher beschrieben und werden hier der Übersichtlichkeit halber noch einmal zusammengestellt:

1. Grundsatz des überwiegenden Allgemeininteresses,
2. Grundsatz der konkreten und präzisen Zweckbestimmung.
3. Verbot der Datensammlung auf Vorrat,
4. Verbot der Zweckentfremdung,
5. Verbot der Herstellung von Persönlichkeitsbildern,
6. Einwirkungsmöglichkeiten und Schutzansprüche des Betroffenen (Rechtsschutzgewährleistung, Auskunfts-, Berichtigungs-, Löschungsansprüche)
7. Kontrollmöglichkeiten des Datenschutzbeauftragten

Ein Versuch, typische Maßnahmen polizeilicher Informationsverarbeitung nach den Hauptphasen der Datenverarbeitung zu ordnen, ergibt, ohne jeden Anspruch auf Vollständigkeit, folgendes Bild:

1. Maßnahmen polizeilicher Informationserhebung im Einzelfall
- Befragung des Betroffenen
- Befragung Dritter
- Observation
- Ausforschung von Versammlungen

2. Maßnahmen polizeilicher Informationsspeicherung
- Kriminalpolizeiliche personenbezogene Sammlungen (KpS)
- Polizeiliche Beobachtung und Erstellung von Persönlichkeitsprofilen (auch Bewegungsbilder u. ä.)

3. Maßnahmen polizeilicher Informationsveränderung
- Datenabgleich
- Rasterfahndung

4. Polizeiliche Informationsübermittlung (Informationshilfe)
- insbesondere: Zusammenarbeit mit den Verfassungsschutzbehörden

Im Folgenden soll versucht werden, am Maßstab der oben genannten Kriterien Anhaltspunkte für die verfassungsrechtliche Zulässigkeit bzw. Unzulässigkeit der einzelnen typischen Maßnahmen und für die tatbestandliche Ausgestaltung der erforderlichen Eingriffsermächtigungen zu entwickeln.

III. Zu den einzelnen Maßnahmen

1. Die Intensität, mit der eine polizeiliche Informationserhebung das informationelle Selbstbestimmungsrecht berührt, kann sehr verschieden sein. Es macht einen erheblichen Unterschied, ob sich jemand selbst in der Öffentlichkeit durch Worte und Handlungen darstellt und damit rechnet oder rechnen muß, daß er dabei beobachtet oder auch nur wahrgenommen wird, oder ob die Polizei durch heimliches oder offenes Befragen des Betroffenen oder Dritter, durch gezieltes und

83 Zum Verhältnis der StPO zu den Landespolizeigesetzen vgl. *Denninger*, Strafverfahren und Polizeibefugnisse, in: Denninger/Lüderssen, (S. Anm. 45), S. 300 ff. m. w. N.

systematisches »Observieren«, Fotografieren und ähnliche Maßnahmen personenbezogene Daten zusammenträgt und zu einem mehr oder weniger geschlossenen Verhaltensbild zusammenfügt. Die seit langem und auch wieder in den Reaktionen auf das Zensus-Urteil umstrittene Frage ist die nach der *Grenze*, jenseits welcher von einem nur kraft besonderer gesetzlicher Ermächtigung zulässigen »*Informationseingriff*« gesprochen werden muß[84]. Das Gericht hat, wie oben in B II.1. ausgeführt, diese Grenze zwar nicht mit begrifflicher Schärfe gezogen. Es hat aber die entscheidenden Kriterien aufgezeigt, an denen sich die Grenzziehung bei der Beurteilung einzelner Maßnahmen zu orientieren hat. Wesentlich ist danach a) die Freiwilligkeit der »Preisgabe« der personenbezogenen Daten und b) das im Hinblick auf die eigene Entscheidungsfreiheit grundsätzlich zu fordernde Vermögen, »das Wissen möglicher Kommunikationspartner ... einigermaßen abzuschätzen«[85]. Schon an diesen Kriterien scheitert mithin der Versuch einer restriktiven Bestimmung des Informationseingriffs, der davon ausgeht, »jeder, der eine Information preisgibt, (müsse) daher damit rechnen, daß sie unbeschränkt weitergegeben und verwendet wird«[86]. Gerade eine solche Vermutung der Nichtexistenz irgendwelcher kontextgebundener Kommunikationsbarrieren oder Diskretionsschwellen müßte das RiS in seinem Kern treffen. Schon das alltägliche Kommunikationsverhalten zeigt, daß man jederzeit mit einem relativen Funktionieren von Kommunikationsschranken rechnet (vgl. nur auch die Graduierungen der Geheimschutzordnung des Deutschen Bundestages!).

Vor dem Hintergrund dieser Maßstäbe lassen sich typische *polizeiliche Informationserhebungen* beurteilen. Die zufällige oder in Verbindung mit einer anderen Diensthandlung (Durchsuchung z. B.) sich ergebende *personenbezogene Wahrnehmung eines Verhaltens in der Öffentlichkeit* scheidet als grundrechtsrelevanter Eingriff aus. Etwas anderes muß aber schon für das *gezielte, systematische Beobachten, »Observieren«* gelten, und zwar sowohl für das »offene« wie für das heimliche Beobachten. Außerdem ist hier (theoretisch) danach zu differenzieren, ob sich die polizeiliche Tätigkeit im bloßen Observieren erschöpft oder ob dieses die Vorstufe für entsprechende Datenspeicherung und damit für die Erstellung von »Persönlichkeitsprofilen«, »Bewegungsbildern« o. ä. bilden soll. Alle vier in diesem Kreuz-Schema denkbaren Möglichkeiten (offenes oder heimliches Observieren mit oder ohne Speicherungsabsicht) überschreiten die Eingriffsschwelle, was hier nur für den (eher theoretischen, »mildesten«) Fall der heimlichen Observation ohne Speicherungsabsicht noch einmal unterstrichen werden soll: Müßte der Bürger damit rechnen, bei allen (oder bei beliebigen) seiner Verhaltensweisen in der (mehr oder weniger beschränkten) Öffentlichkeit beobachtet zu werden, so würde ihn schon dies wegen der Befürchtung nachteiliger staatlicher Reaktionen in seiner Entscheidungsfreiheit beeinträchtigen. Es bedarf keiner Ausführungen, daß auch alle Arten von *Befragungen* (Verdächtiger, Nichtverdächtiger, unbeteiligter Dritter), denen eine Auskunftspflicht des Befragten entsprechen soll, Eingriffscharakter besitzen und einer besonderen gesetzlichen Grundlage bedürfen.

84 Wie weit die ersten Reaktionen auf und Interpretationen des Urteils auseinanderklaffen, zeigen die Stellungnahmen von *A. Podlech*, Die Begrenzung staatlicher Informationsverarbeitung durch die Verfassung angesichts der Möglichkeit unbegrenzter Informationsverarbeitung mittels der Technik, in: Leviathan, 1984, 85 ff. einerseits und von *P. Krause*, Das Recht auf informationelle Selbstbestimmung – BVerfGE 65, 1, JuS 1984, 268 ff. andererseits.

85 EuGRZ 1983, 588 re. Sp. = BVerfGE 65, 43, s. auch o. B II. 1. Ähnlich auch der Wissenschaftliche Dienst des Landtages von Rheinland-Pfalz, Abt. II, vom 6. 2. 1984, Az.: II/52–428, S. 7. Dort wird darauf abgehoben, ob die Datenpreisgabe geeignet sei, »in der Bevölkerung verbreitet freiheitshemmende Befürchtungen auszulösen.« Das ist als Kriterium viel zu vage. Außerdem kommt es auf jeden einzelnen Bürger an.

86 So *Krause* (Anm 84) 271.

Ähnliche Überlegungen wie hinsichtlich des (heimlichen) Observierens sind auch bei einer gesetzlichen Regelung der »*Ausforschung (öffentlicher) Versammlungen*« anzustellen[87]. Zunächst ist darauf hinzuweisen, daß eine Ausforschung nichtöffentlicher Versammlungen nicht nur wegen des RiS (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG), sondern auch wegen der Unverletzlichkeit der Wohnung auf engste verfassungsrechtliche Grenzen stößt, vgl. Art. 13 Abs. 3 GG[88]. Für die Beurteilung der Ausforschung öffentlicher Versammlungen (zu denen also auch Polizeibeamte in Zivil Zutritt haben) – hierunter fällt auch das (verdeckte) Anfertigen von Teilnehmerlisten – kommt es darauf an, ob die Teilnehmer, Redner oder Diskutanten den Umständen nach damit rechnen müssen, daß z. B. ihre Worte durch heimlich anwesende Polizeibeamte auf Tonträger aufgenommen werden. Um einer uferlosen Überwachungstätigkeit vorzubeugen, müßte der Gesetzgeber die Zulässigkeit bloßer »Gefahrerforschungseingriffe« insoweit ausschließen, erst wenn sich eine konkrete Gefahr von erheblichem Gewicht realisiert, darf der Ausforschungseingriff beginnen[89]. Die Ausführungen des Gerichts über die Bedeutung der informationellen Selbstbestimmung für die freie demokratische Meinungs- und Willensbildung – vgl. oben B. I. 5. – müssen hier zum Tragen kommen.

Bei der Normierung der Tatbestandsvoraussetzungen für einen Informationseingriff in der Phase der Erhebung, sei es durch Befragung oder Beobachtung oder in anderer Weise, hat der Gesetzgeber einen Gestaltungsspielraum. Doch muß er den Grundsätzen der Normenklarheit und der Verhältnismäßigkeit Rechnung tragen. Dies gilt um so mehr, als die Informationserhebung häufig bereits im Vorfeld der eigentlichen Aufgabe der Polizei, nämlich der Gefahrenabwehr und Störungsbeseitigung, also bereits bei der Gefahrenvorbeugung, z. B. bei der »vorbeugenden Verbrechensbekämpfung« stattfindet und deshalb häufig auch »Nichtstörer«, unverdächtige Dritte als Informanten in Anspruch genommen werden sollen. Die darin liegende Ausweitung des materiellen Polizeibegriffs ist nur bei sorgfältiger Abwägung der Grundrechts-Risiken gegenüber dem Eingriffsinteresse zu rechtfertigen.

2. Das Bundesverfassungsgericht hat »die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken« als unvereinbar mit dem Grundsatz der bereichsspezifischen und präzisen Zweckbestimmung bezeichnet. Außerdem weist es in diesem Zusammenhang noch einmal ausdrücklich auf das Mindesteingriffsgebot hin. Beide Äußerungen des Gerichts sind für die Fragen der verfassungsrechtlichen Zulässigkeit »*Kriminalpolizeilicher personenbezogener Sammlungen (KpS)*« von besonderer Bedeutung. Zunächst ergibt sich aus ihnen, daß das Gericht die prinzipielle Notwendigkeit und Zulässigkeit solcher Sammlungen offensichtlich nicht in Zweifel zieht. Allerdings fallen sie insgesamt unter den Gesetzesvorbehalt, so daß es künftig nicht mehr ausreicht, KpS gemäß den »Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen«[90] anzulegen, aufzubauen und zu nutzen. Im Hinblick auf die vom Bundesverfassungsgericht in ständiger Rechtsprechung vertretene »Wesentlichkeitstheorie« zum Gesetzesvorbehalt[91] kann auch eine gesetzliche Regelung nicht als verfassungs-

87 Vgl. dazu *Arbeuskreis Polizeirecht* (Hrg.), AEPolG Alternativentwurf, 1979, S. 57 ff.

88 *De Lazzer/Rohlf*, Der »Lauschangriff«, JZ 1977, 207 ff., *Denninger*, in: Denninger/Lüderssen, (Anm. 45) S. 316 ff.

89 Vgl. § 30 BremPolG vom 21. 3. 1983: Heimliche Informationserhebung in Versammlungen nur zur Abwehr einer »erheblichen Gefahr«. Die Regelung ist allerdings ziemlich unpraktikabel.

90 Erlaß des BMI vom 26. 2. 1981 – P I 5 – 625 14/3, GMBl S. 120. Der Text wurde von der Innenminister-Konferenz beschlossen, sollte also im wesentlich wortgleich von den Ländern übernommen werden. Vgl. den Abdruck bei *R. Riegel*, Polizei- und Ordnungsrecht in der Bundesrepublik Deutschland, 1981, S. 263 ff. Dort auch der Wortlaut der »Dateien-Richtlinien« für das BKA vom gleichen Tage, S. 271 ff.

91 Vgl. nur BVerfGE 49, 46, 78 ff.

rechtlich unbedenklich angesehen werden, die, wie § 36 BremPolG[92], alle wichtigen Bestimmungen den vom zuständigen Senator (Minister) zu erlassenden Richtlinien (Verwaltungsvorschriften) überläßt. Wenn im grundrechtsrelevanten Bereich – und in diesem bewegt sich die Einrichtung von KpS – »wesentlich« in der Regel »wesentlich für die Verwirklichung der Grundrechte« bedeutet[93], dann muß der *Gesetzgeber*

- den Zweck der Sammlung festlegen,
- den betroffenen Personenkreis,
- die Art der zu speichernden Daten,
- die Voraussetzungen einer Informationsübermittlung,
- die Dauer der Aufbewahrung, also die Löschungsfristen und
- die Auskunftspflichten zugunsten des Bürgers bestimmen.

Auch die Kontrollbefugnisse des Datenschutzbeauftragten, insbesondere auch für den Fall der Auskunftsversagung gegenüber dem betroffenen Bürger, sind in den Grundzügen im Gesetz zu normieren.

Von besonderer Relevanz für die kriminalpolizeiliche Arbeit ist die Frage der Zulässigkeit der *Herstellung von Persönlichkeitsbildern (Persönlichkeitsprofilen).* Technisch gesehen berührt sie nicht allein Maßnahmen der Informationsspeicherung, sondern ebenso der sonstigen Informationsverarbeitung, insbesondere der -übermittlung. Da letztlich auch bei der Zusammenführung von Daten aus verschiedenen Dateien das daraus entstehende »Profil« an einer Stelle gespeichert wird, ist es gerechtfertigt, die normative Problematik an dieser Stelle zu behandeln, vgl. oben B III 1.e).

Mit der Möglichkeit der Herstellung von Persönlichkeitsbildern erreicht die elektronische Datenverarbeitung eine Grenze, an der der Ausnutzung des Technisch-Machbaren von Verfassungs wegen u. U. ein *absolutes* »Halt!« geboten werden muß.

Wir unterscheiden »totale« und »partielle« Persönlichkeitsbilder, wohl wissend, daß auch das »totale« Bild eine Person niemals in schlechthin allen ihren Äußerungsweisen und Beziehungen erfassen kann[94]. Dennoch ist es gerechtfertigt, von einem »totalen« Bild zu sprechen, wenn die *Intention* seiner Urheber auf eine Zusammenfassung möglichst zahlreicher Daten eines Bürgers aus seinen unterschiedlichen Lebensbereichen gerichtet ist.

Ein in diesem Sinne totales Bild würde beispielsweise entstehen, wenn die wesentlichen Daten einer beruflichen Karriere mit den »Gesundheitsdaten«, den Daten über politisches und Freizeitverhalten, über persönliche Beziehungen einschließlich des geschlechtlichen Verhaltens und den Daten über kulturell-religiöses Verhalten eines Menschen zusammengeführt würden. Ein »partielles« Persönlichkeitsbild bleibt hingegen auf einen zeitlich, räumlich und/oder sachlich abgegrenzten Lebensausschnitt beschränkt. Hierunter fallen auch systematische Aufzeichnungen von Reisebewegungen des Betroffenen, sogenannte »Bewegungsbilder«, die für die Straftatverfolgung, aber auch für die präventive Überwachung der Mitglieder einer kriminellen Vereinigung nach §§ 129/129a StGB oder auch des organisierten Rauschgifthandels wichtig werden können.

Die Ergebnisse der *»Polizeilichen Beobachtung«* eines Tatverdächtigen oder eines potentiellen künftigen Straftäters können zu partiellen Persönlichkeitsbildern verarbeitet werden. Die Herstellung von Persönlichkeitsprofilen ist über den polizeilichen Bereich hinaus für die Arbeit der Ämter für Verfassungsschutz von Bedeutung, insbesondere wenn sie bei der Spionageabwehr oder beim Geheimnis- und Sabota-

92 § 36 BremPolG vom 21. 3. 1983, immerhin bisher die einzige gesetzliche Regelung dieser Art überhaupt.

93 S. Anm. 91, S. 79 m. w. N.

94 Vgl. die Nachweise oben bei Anm. 71.

geschutz individuelle Beteiligte auf ihr »Sicherheitsrisiko« hin zu überprüfen haben, § 3 Abs. 1 Nr. 2 und Abs. 2 Nr. 1 bis 3 BVerfSchG i. V. m. § 1 HVerfSchG vom 19. 7. 1951.

Die Herstellung eines *»totalen Persönlichkeitsbildes«* stößt verfassungsrechtlich an eine *absolute* Grenze, vgl. o. B. III 1.e). Sie wäre die Realisierung der Orwell'schen Vision vom totalitären Überwachungsstaat, das Ende der Autonomie der Persönlichkeit, eine unter keinem Gesichtspunkt zu rechtfertigende Verletzung der Menschenwürde. In diesem Punkt ist vermutlich auch Konsens mit jenen Autoren zu erzielen, die sonst schnell, allzu schnell mit dem (ja nur polemischen, sachlich nichtssagenden) Vorwurf einer »überbordenden Datenschutzhysterie«[95] zur Hand sind. Daß hier eine absolute und nicht nur relative, je nach »Güterabwägung« so oder anders zu ziehende Grenze besteht, ließe sich anthropologisch und kommunikationstheoretisch im einzelnen nachweisen.

Hier sollen nur drei Stichwörter zur Verdeutlichung gegeben werden: 1) Ein »totales« Persönlichkeitsbild muß notwendigerweise falsch, verzerrend sein, nicht so sehr wegen seiner unvermeidlichen Unvollständigkeit, sondern weil die einzelnen Daten-Mosaiksteine bewußt aus dem situativen Kontext ihrer Entstehung herausgerissen und »abstrakt« gespeichert werden. Damit sind notwendig Sinnveränderungen verbunden. 2) Da der Computer »die Gnade des Vergessens« nicht kennt, ist dem Betroffenen die Chance einer Umkehr, einer Selbstkorrektur und eines Neubeginns verwehrt. Diese gehört aber unverzichtbar zur conditio humana. 3) Ein menschlicher Dialog ist mit dem Computer nicht möglich. Der Staat behandelt den Bürger als ein Objekt, eine Sache, wenn er ihn auf einen Datenbestand reduziert; er verzichtet auf die »Auseinandersetzung« mit einem lebendigen Gegenüber, wie sie Grundbedingung jedes rechtsstaatlichen Verfahrens ist, wenn er (der Staat) Maßnahmen gegen eine Person lediglich oder maßgeblich aufgrund ihres Datenabbildes trifft.

Hinsichtlich der tatbestandlichen Voraussetzung, die die Anordnung einer polizeilichen Beobachtung oder der Erstellung eines *partiellen Persönlichkeitsbildes* rechtfertigen können, sind schon mit Rücksicht auf die Schwere des Eingriffs in das Recht der informationellen Selbstbestimmung strenge Maßstäbe an das Kriterium der Erforderlichkeit anzulegen. Polizeiliche Beobachtung und Herstellung eines Persönlichkeitsbildes weisen im Charakter der Maßnahme eine gewisse Ähnlichkeit mit der heimlichen Überwachung des Fernmeldeverkehrs nach § 100a StPO oder §§ 1 ff. G 10 auf. Dies legt es nahe, wie bei diesen Vorschriften, die Zulässigkeit des Eingriffs nur bei Vorliegen bestimmter katalogartig aufgezählter Verdachtsgründe vorzusehen. Eine schematische Übernahme der »Katalogtaten« des § 100a StPO oder des § 2 G 10 wird dabei nicht in Betracht kommen; doch können diese Tatbestände dem Gesetzgeber gewisse Hinweise bieten[96].

Darüber hinaus sollte der Gesetzgeber den Versuch einer Konkretisierung des Verhältnismäßigkeitsgrundsatzes hinsichtlich des höchstzulässigen Umfanges einer der in Rede stehenden Maßnahmen machen. Das ist in zeitlich-räumlicher wie in gegenständlicher Hinsicht möglich. Erweist es sich dabei als unvermeidlich, auf den Gebrauch einer verhältnismäßig abstrakt bleibenden Generalklausel zurückzugreifen, so wird es um so wichtiger, den Grundrechtsschutz durch »flankierende« *verfahrensrechtliche/organisatorische Regelungen* sicherzustellen. In erster Linie ist hier daran zu denken, die Anordnung der Maßnahme dem *Richter*, allenfalls bei repressiver Tätigkeit und bei Gefahr im Verzuge auch dem *Staatsanwalt* zu übertragen[97]. Soweit die nichtpolizeiliche, rein *nachrichtendienstliche* Beobachtung und Erstellung von Persönlichkeitsbildern in Betracht kommt, empfiehlt sich eine ausdrückliche *Ergänzung des Bundes- bzw. des Landes-Verfassungsschutzgesetzes.*

95 *Krause*, JuS 1984, 270.
96 Vgl. auch § 12 Abs. 2 AEPolG (Anm. 87), der einfach auf § 100a StPO Bezug nimmt.
97 Vgl. § 12 Abs. 3 AEPolG.

Denn die Generalklausel über die Anwendung nachrichtendienstlicher Mittel ist zu allgemein gehalten, als daß damit die Erstellung von Persönlichkeitsbildern in rechtsstaatlich einwandfreier Weise abgedeckt wäre[98]. Eine *richterliche* Anordnung wird hier im Bereich des Verfassungsschutzes i. e. S. wohl nicht in allen, sondern nur in besonders gravierenden Fällen der Herstellung eines Persönlichkeitsbildes vorzusehen sein. Auch das gesteigerte Geheimhaltungsbedürfnis spielt bei der Beurteilung dieser Frage eine Rolle.

3. Die technische Entwicklung in der elektronischen Datenverarbeitung hat zu einschneidenden *Veränderungen in den Methoden der polizeilichen Fahndungsarbeit* geführt[99]. Ein weiterer, auch struktureller Wandel des Arbeitsplatzes des Kripobeamten ist zu erwarten. Auf den kürzesten Nenner gebracht läßt sich ein wesentlicher Aspekt des Wandels so charakterisieren: Die herkömmliche Personen- und Sachfahndung aufgrund konkreter tat-/täterbezogener Verdachtsmerkmale wird nicht überflüssig. Aber sie wird ergänzt und überlagert durch eine (meist vorangehende) »systematisierte und automatisierte Suche nach Personen und Sachen«, bei der ein praktisch (d. h. von den technischen Möglichkeiten her gesehen) unbegrenzt großer Kreis zunächst *nichtverdächtiger* Personen auf das Vorliegen oder Nichtvorliegen bestimmter Einzelmerkmale hin überprüft wird, um so schrittweise einen immer enger werdenden Personenkreis herauszufiltern, auf den immer zahlreichere der für den Täter als charakteristisch *angenommenen* Einzelmerkmale zutreffen. Auf diesem Wege der *gestuften Verdachtsverdichtung* hofft man erst einmal, »ermittlungsfähige Einzelspuren« zu gewinnen. Technisch wird dies durch automatisierten *Dateienabgleich*[100] bewerkstelligt; teilweise wird der anschauliche Ausdruck *»Rasterfahndung«* sinngleich verwendet[101].

Zwei Formen der »Rasterung« werden unterschieden, die, wenig hilfreich und bei nicht ganz einheitlichem Begriffsverständnis[102], als *positiver* oder *negativer* Dateienabgleich bzw. positive oder negative Rasterfahndung bezeichnet werden.

Beim »positiven Dateienabgleich« werden zwei Magnetbänder (mit personenbezogenen Daten) mit dem Ziel gegeneinander gespielt, eine Datei derjenigen Personen zu erhalten, die die Merkmale der beiden Ausgangsdateien auf sich vereinen. So wurden die Fahndungsdateien mit den Dateien der Einwohnermeldeämter, des Kraftfahrtbundesamtes und anderer Behörden »abgeglichen«. Ein anderes Beispiel bietet der Vergleich der Hotelmeldezettel-Daten mit der Fahndungsliste. Im Unterschied hierzu dient der »negative Dateienabgleich« (»Negative Rasterfahndung«) dazu, aus einem Ausgangsdatenbestand (von einem Ausgangsband) alle Personendaten auszuscheiden (zu löschen), die auch (unter ganz anderen Gesichtspunkten) auf einem Gegenband gespeichert sind. Nach wiederholtem Gegenspiel mit verschiedenen Dateien (Bändern) bleibt auf dem Ausgangsband nur noch ein »Bodensatz« von Daten der Personen übrig, die zahlreiche Merkmale *nicht* aufweisen, die auch der vermutete Täter mutmaßlich nicht besitzt. Gegen diese Restgruppe wird dann in traditioneller Weise weiterermittelt. Vermutet man beispielsweise[103], daß ein Terrorist die Stromrechnungen für eine »konspirative Wohnung« nicht überweist, sondern bar bezahlt, daß er außerdem weder sich selbst noch ein Kraftfahrzeug angemeldet hat, so läßt man eine Datei aller barzahlenden Stromkunden gegen eine Datei des betreffenden Einwohnermeldeamtes und eine Datei der Kfz.-Halter der Region laufen. Unter dem Restbestand an Daten darf man dann die des Gesuchten vermuten.

98 § 3 Abs. 3 Satz 2 BVerfSchG gilt nach G. vom 19. 7. 1951 der Sache nach auch für das Hessische Landesamt für Verfassungsschutz.

99 Hierzu und zum Folgenden: *Ermisch*, Fahndung und Datenschutz – aus der Sicht der Polizei, BKA Vortragsreihe Band 25, 1980, S. 63 ff., 70; ferner *Riegel*, Rechtsprobleme der Rasterfahndung, ZRP 1980, 300 ff.

100 Das BremPolG § 29 verwendet den möglicherweise noch weiteren Begriff des »Datenabgleichs«.

101 Umfassende Untersuchung der umstrittenen Rechtsgrundlagen der Rasterfahndung bei *Simon/Taeger*, Rasterfahndung, 1981.

102 Vgl. *Ermisch* (Anm. 99) einerseits, *H. Herold*, Polizeiliche Datenverarbeitung und Menschenrechte, Recht und Politik 1980, 79 ff. andererseits.

103 Zur Rasterfahndung »Energieprogramm« 1979/80 vgl. den 3. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz, 1981, S. 50 f., *Herold* (Anm. 102).

Logisch gesehen unterscheiden sich die beiden Abgleichmethoden darin, daß beim positiven Abgleich eine Schnittmenge bzw. eine Schnittmenge von Schnittmengen gesucht wird, während beim negativen Abgleich das Ziel eine möglichst kleine Restmenge nach Abscheidung möglichst zahlreicher Schnittmengen ist. Datenschutzrechtlich gesehen kann diese Verschiedenheit keine ausschlaggebende Rolle spielen: Die erstrebte Schnittmenge bei der positiven bzw. die Restmenge bei der negativen Rasterfahnung enthält bezüglich jedes der in ihr gespeicherten Datensätze ein Mehr an Informationen gegenüber den entsprechenden Datensätzen der Ausgangsdateien. Insofern liegt eine Informationsveränderung i. S. der §§ 2 Abs. 2 Nr. 3, 9, 25 BDSG vor[104], und grundrechtlich gesehen ein Eingriff in das RiS.

Das automatische elektronische Aussondern der meisten Merkmalsträger durch sukzessives Löschen vom Ausgangsband hat Herold[105] veranlaßt, die Rasterfahndung als eine »nahezu klinisch sterile Fahndungsform« zu loben, die »erhebliche Verbesserungen im Menschenrechts- und Grundrechtsschutz zu bewirken« vermöge. Solche Euphorie bedarf einer gewissen Dämpfung.

Dabei braucht hier die Frage nicht abschließend beantwortet zu werden, ob die Rasterfahndung – läßt man einmal die Grundrechtsproblematik des RiS außer Betracht – in den bisher geltenden Vorschriften eine ausreichende Rechtsgrundlage findet. Dies ist mit beachtlichen Argumenten sowohl für die Stützung auf die strafprozessualen Generalklauseln der §§ 161, 163 StPO als auch für § 94 StPO als auch für die präventivpolizeiliche Generalklausel als auch für die datenschutzrechtliche Generalklausel der »Wahrung berechtigter Interessen der Allgemeinheit« in § 24 BDSG bezweifelt worden[106]. Zumal die letztgenannte Vorschrift vermöchte schon nach ihrer systematischen Stellung zwar u. U. die Datenherausgabe durch die privaten Unternehmen usw. zu rechtfertigen, sie liefert aber keine Ermächtigungsgrundlage für einen hoheitlichen Informationseingriff. Im repressiven Tätigkeitsbereich würde die Heranziehung der Aufgabenzuweisungsnormen (§§ 161, 163 StPO) als Eingriffsermächtigung das sonst durchgehaltene Prinzip der speziellen Befugnisregelung unterlaufen. Wie die §§ 111 und 163b Abs. 2 StPO belegen, gilt dieses Prinzip in besonderem Maße, wenn, wie im Falle der Rasterfahndung, Maßnahmen massenweise gegen *Nichtverdächtige* gerichtet werden sollen. Kommt gefahrenabwehrendes präventives Handeln der Polizei in Betracht, so gilt Entsprechendes. In großer Zahl werden die Daten Unbeteiligter, also von »Nichtstörern«, verarbeitet. Polizeilich dürfen diese nur unter den strengen Voraussetzungen des »polizeilichen Notstandes« – vgl. §§ 15 i. V. m. 1 Abs. 2 Satz 1 HSOG; § 6 MEPolG – in Anspruch genommen werden. Offenbar im Hinblick auf diese Rechtslage hat der Gesetzgeber der bisher einzigen[107] Spezialvorschrift über polizeilichen »Datenabgleich«, der Gesetzgeber des Bremischen Polizeigesetzes 1983 in § 29 wenigstens einen Teil der tatbestandlichen Voraussetzungen des polizeilichen Notstandes, nämlich das Vorliegen »einer gegenwärtigen erheblichen Gefahr« aufgenommen.

Beim Dateienabgleich, insbesondere bei der negativen Rasterfahndung, werden in weitem Umfang Informationen aus Dateien in Anspruch genommen, die zu ganz anderen Zwecken (z. B. zur Kontrolle der pünktlichen Bezahlung der Stromrechnungen) angelegt wurden. Schon nach dem Grundsatz der konkreten und präzisen Zweckbestimmung sowie aufgrund des Verbots der Zweckentfremdung muß also der Gesetzgeber versuchen, in einer spezifischen Regelung des Dateienabgleichs die

104 Vgl. *Dammann* in *Simitis/Dammann/Mallmann/Reh*, BDSG Kommentar, 3. Aufl. 1981, § 2 Rdnr. 112.
105 *Herold* (Anm. 102), 83.
106 Z. B. von *Simon/Taeger* (Anm. 101) S. 48 ff. m. w. N. S. ferner *Simitis*, BDSG Kommentar, § 24, Rdnr. 40 f., *Bull*, 3. Tätigkeitsbericht des BfD, S. 50 ff.
107 Vgl. aber AEPolG, (Anm. 87), bes. §§ 37, 38, 40, 45 welche die Rasterfahndung miterfassen.

näheren Voraussetzungen der Zulässigkeit, z. B. den Grad der polizeilichen Gefahr oder das Gewicht der aufzuklärenden Verbrechen näher zu umreißen. Entsprechend dem bundesstaatlich ausgeprägten Dualismus von Strafprozeß- und Polizeigesetzgebung wird man aufeinander abgestimmte Ergänzungen in beiden Gesetzeswerken anstreben müssen. Bei der Regelung der materiellen Voraussetzungen einer Rasterfahndung wird auch zu prüfen sein, ob – enger als etwa in § 72 SGB-X – bestimmte Daten, z. B. Gesundheitsdaten, nicht ganz von der Verarbeitung im Dateienabgleich auszuschließen oder aber ihm nur unter erschwerten Voraussetzungen zur Verfügung zu stellen sind. Da diese Art der polizeilichen Fahndung naturgemäß nicht in aller Öffentlichkeit vor sich gehen kann, gewinnen verfahrensmäßige und organisatorische Schutzvorschriften hier eine besondere Bedeutung. Hierzu gehört als eine Möglichkeit die Entscheidungsverlagerung auf die höchste (und politisch verantwortliche) Verwaltungsebene[108]. Nicht minder wichtig ist die Pflicht zur sofortigen Löschung bzw. Vernichtung (von Amts wegen) der »ausgerasterten« Datenbestände und Unterlagen. Weiter ist an eine Pflicht zur Führung entsprechender Protokolle zu denken. Da es bei der Rasterfahndung, stärker noch als bei anderen Maßnahmen, vorwiegend um eine Kontrolle der internen Polizeiarbeit geht, dürfte hier eine Sachlage gegeben sein, die *zwingend* eine wirksame, d. h. nicht nur nachträgliche, sondern *begleitende Kontrolle durch den Datenschutzbeauftragten* erfordert. Sie kann in der Weise eingeleitet werden, daß das an einen Dritten gerichtete Ersuchen um Überlassung einer Datei für Zwecke des Abgleichs jeweils dem Datenschutzbeauftragten angezeigt wird[109].

4. Polizeiliche Informationsübermittlung (Informationshilfe, Amtshilfe)

a) In den Jahren 1979–81 entzündete sich die *Amtshilfe*diskussion im Bereich der Sicherheitsbehörden vor allem an der Frage nach den verfahrensrechtlichen und organisationsrechtlichen Grundlagen der sogenannten »So-GK« (= Sonderanweisung über die Erfassung bestimmter Erkenntnisse bei der grenzpolizeilichen Kontrolle), derzufolge die Kräfte des Bundesgrenzschutzes (einer Polizei des Bundes!) u. a. personenbezogene Erkenntnisse permanent und in großem Umfang an das Bundesamt für Verfassungsschutz und an den Bundesnachrichtendienst übermittelten[110]. Diese spezielle Fragestellung wurde maßgeblich von der Auslegung des positivrechtlichen Gebotes der Trennung zwischen Verfassungsschutz und Polizei beeinflußt; das Recht oder gar Grundrecht auf informationelle Selbstbestimmung wurde keineswegs allgemein anerkannt und nur da und dort als Argument in die Diskussion miteingebracht[111]. Inzwischen und erst recht seit dem Zensus-Urteil hat die Problematik der informationellen Zusammenarbeit von Behörden überhaupt und speziell der Sicherheitsbehörden vom Technischen wie vom Normativen her eine neue Dimension gewonnen.

Die Fortschritte in der Informationstechnologie ermöglichen den Aufbau beliebig zentralisierter oder dezentralisierter Informationssysteme, die untereinander in einen technisch ebenso beliebig steuerbaren, erweiterbaren oder reduzierbaren Datenverbund treten können. Die normative Bewältigung dieser von der Technik und ihren Möglichkeiten geprägten Situation steht damit vor einer völlig anderen Aufgabe als die, auf welche die Regeln der »klassischen« Amtshilfe (vor allem §§ 4 bis 8 VwVfG) zugeschnitten sind. Modellhaft zugespitzt kann man sagen: Das Problem ist nicht mehr, wie bei der »klassischen« Amtshilfe, die optimale

108 § 29 Abs. 1 letzter Satz BremPolG: vorherige Zustimmung des Senators für Inneres.

109 § 29 Abs. 4 BremPolG: nur nachträgliche Unterrichtung des Datenschutzbeauftragten. Vgl. auch den Gesetzesvorschlag (Abs. 5) von *Riegel* (Anm. 99), 306.

110 Vgl. den Sammelband Verfassungsschutz und Rechtsstaat, 1981, besonders die Beiträge von *Bull*, *Denninger*, *Evers* (s. o. Anm. 59). Die damals vom BMI in Auftrag gegebenen Gutachten von Denninger, Evers, Kirchhof, Martens, v. Münch, Obermayer sind leider nicht veröffentlicht worden.

111 Vgl. *Denninger* (Anm. 35).

Verfügbarmachung entscheidungsnotwendiger, knapper und an entfernter Stelle vorhandener Informationen (Stichwort: »Aktenübersendung«), sondern das Problem besteht in der Begrenzung und Kanalisierung eines virtuell ubiquitären Datenüberflusses, in der Herstellung einer machtbegrenzenden Gewaltenteilung durch *Informationsteilung und -verteilung*[111].

Das Recht auf informationelle Selbstbestimmung ist der grundrechtliche Aspekt dieses übergreifenden Problems rechtsstaatlicher Staatsorganisation.

Angesichts dieses grundlegenden Wandels in der »Informationssituation« erscheint es wenig sinnvoll, die Diskussion unter dem Blickwinkel einer bloßen Ergänzung und technischen Aktualisierung der Amtshilfevorschriften der Verwaltungsverfahrensgesetze einschließlich einer sogenannten »erweiterten Amtshilfe«[112] zu führen. Denn wesentliche Begriffsmerkmale der herkömmlichen Amtshilfe stehen mit den technischen Möglichkeiten und damit einer uneingeschränkten Ausnutzung des elektronischen Informationsaustausches im Dateienverbund tendenziell in Widerspruch: (1) Amtshilfe ist immer nur *ergänzende* Hilfe; die ersuchte Behörde darf nicht die Herrschaft über das Verfahren, in dem sie für eine untergeordnete Teilleistung beansprucht wird, gewinnen. (2) Amtshilfe wird nur auf ein jeweils gestelltes Ersuchen einer nicht weisungsbefugten Behörde hin geleistet. (3) Amtshilfe ist auf den Einzelfall, eventuell auch auf eine Vielzahl von Einzelfällen bezogen. Es ist umstritten, inwieweit ein Amtshilfeersuchen auf Dauer und generalisiert gestellt werden kann. Zu (1): Ein ungebremster elektronischer Informationsaustausch würde dazu führen, daß von der Herrschaft einer bestimmten (nämlich zuständigen) Behörde über ein bestimmtes Verwaltungsverfahren sinnvoll nicht mehr gesprochen werden könnte. Zu (2): Ein besonderes Amtshilfe-Ersuchen wird überflüssig, wenn insbesondere beim On-line-Anschluß die informationssuchende Stelle alle nur gewünschten Daten ohne weiteres »abrufen« kann. Zu (3): Der organisationsrechtlich bedeutsame Unterschied zwischen aushilfeartiger Mitwirkung (der ersuchten Behörde) im Einzelfall und dauernder, generell formulierter Aufgabenzuweisung wird hinfällig, wenn die Übermittlung bestimmter Arten anfallender Daten an die »ersuchende« Behörde generell, auf Dauer und automatisch erfolgt.

Es wird deshalb hier *vorgeschlagen*, die *»elektronische Informationshilfe«* begrifflich-rechtlich und gesetzgebungspolitisch von der Regelung der »Amtshilfe« abzukoppeln und jeweils aufgaben- und verwendungsspezifisch zu normieren.

b) Der Terminus *»Informationsaustausch«* bezeichnet die Möglichkeit der (elektronischen) Datenübermittlung in beiden Richtungen, läßt aber auch zu, daß die Möglichkeit in nur einer Richtung genutzt wird. Voraussetzungen und Grenzen des polizeilichen wie des »überpolizeilichen« Informationsaustausches sind gesetzlich zu regeln (vgl. oben B III 1d)). Der Gesetzgeber hat dabei außer den allgemeinen Grundsätzen wie dem Übermaßverbot vor allem das Prinzip der möglichst konkreten und präzisen Zweckbestimmung und das Verbot der Zweckentfremdung zu berücksichtigen. Dies rechtfertigt zunächst eine Unterscheidung danach, ob polizeilich gespeicherte Informationen innerhalb der Polizeibehörde zu deren Aufgabenwahrnehmung übermittelt werden oder ob sie an Behörden außerhalb des Polizeibereichs oder an (private) Dritte weitergegeben werden sollen.

(1) Daß *zwischen Polizeibehörden*, insbesondere zwischen Kriminalpolizeibehörden ein Informationsaustausch zu polizeilichen Zwecken, also etwa zur Straftatver-

111 Zur »Informationsverteilung« s. den Bericht der *Sachverständigenkommission* (Anm. 45), 1983, Rz. 219 ff.

112 Dazu *Kopp*, VwVfG § 4 Anm. 2; *Meyer/Borgs*, VwVfG § 4 Rz. 19. Vgl. zum Folgenden auch *Riegel*, Datenschutz bei den Sicherheitsbehörden, 1980 S. 18 ff.

folgung, möglich sein muß, dürfte und sollte außer Streit sein. Fraglich kann hier nur sein, ob im Rahmen der polizeilichen Aufgabenerledigung (als der generellen Zweckbestimmung) ein grundsätzlich unbeschränkter Austausch zulässig sein soll oder ob *von Verfassungs wegen* engere Grenzen gezogen werden können und müssen. Bei der Beantwortung dieser Frage ist zu berücksichtigen, daß die verschiedenen Polizeibehörden (von der Bund-Länder-Problematik einmal ganz abgesehen) zwar datenschutzrechtlich keine Informationseinheit, wohl aber funktional eine *Zweckeinheit* bilden, jedenfalls, wenn man spezifische Aufgaben, z. B. die Verbrechensbekämpfung, ins Auge faßt. Ferner ist zu bedenken, daß zwar auch ›innerpolizeiliche‹ Informationsübermittlung hinsichtlich des RiS prinzipiell grundrechtsrelevant ist, daß also auch insoweit das Übermaßverbot und das Zweckentfremdungsverbot zu beachten sind, daß andererseits aber die »Eingriffsintensität« und das Schutzinteresse u. U. gering sind. Dies wird deutlich, wenn man sich die ratio essendi, den zu schützenden Kerngehalt des RiS – vgl. oben B I 3. und C III 1. – vor Augen hält. Der polizeilich gesuchte Straftäter muß und wird »damit rechnen«, daß die Kripostellen bei der Fahndung kooperieren; er muß aber z. B. nicht ohne weiteres damit rechnen, daß die Polizei ihren Verdacht seinem Arbeitgeber mitteilt, wenn die Straftat keinerlei Bezug zu seinem Arbeitsplatz aufweist.

Zum ersten ergibt sich hieraus, daß die Frage der *Zulässigkeit des On-line-Verkehrs* etwa zwischen kriminalpolizeilichen Dateien und Terminals weder generell bejaht noch generell verneint werden kann. Die Frage, ob eine »Übermittlung« erforderlich war, darf allerdings nicht im Hinblick auf die »Übermittlungs-Fiktion« des § 2 Abs. 1 Nr. 2 BDSG (Übermitteln = zum Abruf Bereithalten), sondern nur in bezug auf die tatsächlich abgerufenen Informationen beurteilt werden. Gegen einen On-line-Verbund werden um so weniger Bedenken erhoben werden können, je aufgabenspezifischer die bereitgehaltenen Datenbestände aufgegliedert werden. Hält sich der konkrete Datenabruf im Rahmen des zweckspezifisch zu konkretisierenden Übermaßverbotes, so ist die Tatsache, daß er im On-line-Verkehr erfolgt, grundrechtlich irrelevant.

Zum zweiten sind auch die Grenzen der zulässigen *Zentralisierung* (kriminal)polizeilicher Informationssysteme an diesen Kriterien auszurichten. Im Bund-Länder-Verhältnis sind außerdem die kompetenzrechtlichen Vorgaben der Verfassung – Art. 73 Nr. 10a GG für die Zusammenarbeitsgesetzgebung, Art. 87 Abs. 1 Satz 2 GG für die Einrichtung von Zentralstellen – zu beachten. Die Ausfüllung durch das Gesetz über die Einrichtung eines Bundeskriminalpolizeiamtes (Bundeskriminalamtes) vom 29. 6. 1873 hält sich in diesem Rahmen, sofern die Generalklausel des § 2 Abs. 1 Nr. 1 BKAG (das BKA »ist insoweit auch Zentralstelle für den elektronischen Datenverbund zwischen Bund und Ländern«) im Hinblick auf das RiS verfassungskonform ausgelegt und angewendet wird.

Konkret stellt sich hier die Frage, ob etwa ein beim BKA zentral geführter *Kriminalaktennachweis (KAN)*, der auch den Kriminalpolizeibehörden der Länder voll zugänglich sein soll, auch zulässig wäre, wenn er bundesweit schlechthin alle kriminalpolizeilichen Vorfälle erfassen und zum Informationsabruf bereit halten sollte oder ob hier Beschränkungen in gegenständlicher und/oder räumlicher Hinsicht geboten sind. Der Erforderlichkeitsgrundsatz und das Verbot der Datensammlung auf Vorrat sind hier zu berücksichtigen. Sicherlich werden danach Fallgruppen von Bagatellkriminalität auszuscheiden haben; im übrigen wird der Gesetzgeber prüfen müssen (vgl. oben C III 2), ob und wie er *regionale* Begrenzungen der Datenspeicherung und -übermittlung ausformulieren kann.

(2) Die Fülle der Möglichkeiten des *Informationsaustausches zwischen Polizeibehörden und anderen öffentlichen Stellen oder gar Privaten (»Dritten«)* kann hier nicht

erörtert werden. Nach der Darstellung der für die verfassungsrechtliche Beurteilung maßgeblichen Kriterien erscheint dies auch nicht erforderlich; vielmehr kommt es darauf an, diese Kriterien auf die jeweils zur Diskussion stehende Sachlage vernünftig anzuwenden.

Im Folgenden sollen exemplarisch drei Bereiche der ›überpolizeilichen‹ informationellen Kooperation im Hinblick auf die Auswirkungen des RiS näher betrachtet werden:
- die Zusammenarbeit zwischen Polizei (Bundesgrenzschutz) und Verfassungsschutz als Beispiel der Informationsübermittlung von der Polizei »nach außen« (I),
- die Zusammenarbeit zwischen dem Kraftfahrt-Bundesamt und den Polizeibehörden als Beispiel der Informationsübermittlung »von außen« an die Polizei (II), sowie
- die Informationsübermittlung zwischen Meldebehörden und Polizeibehörden (III).

(I): Für das Verhältnis zwischen *Polizei und den Ämtern für Verfassungsschutz* – die Rechtslage ist insoweit für das Bundesamt einerseits, für die Landesämter andererseits materiell nicht verschieden[114] – und zwischen den Bundesgrenzschutzbehörden und den Verfassungsschutzbehörden im besonderen ist in erster Linie das institutionalisierte und funktionelle *Trennungsgebot* zu beachten, wie es in § 3 Abs. 3 BVerfSchG zum Ausdruck kommt. Diesem Grundsatz kommt als einer Ausprägung des Rechtsstaatsprinzips zwar nicht formell, aber materiell Verfassungsrang zu, wie sich aus der Entstehungsgeschichte der Vorschriften und der des Grundgesetzes ergibt[115]. Der (einfache) Gesetzgeber könnte danach zwar den § 3 BVerfSchG in Einzelheiten abändern, aber dem Grundgedanken des Trennungsgebotes müßte er Rechnung tragen.

In großem Umfang und als Daueraufgabe nach generellen Richtlinien – die seinerzeit umstrittene »So-GK« ist seit dem 1. Dezember 1981 durch eine *›Dienstanweisung zur Durchführung der Amtshilfeersuchen der Verfassungsschutzbehörden und des Bundesnachrichtendienstes‹* abgelöst worden – führen die Grenzschutzbehörden anläßlich der Kontrollen an der deutsch-deutschen Grenze personenbezogene Informationserhebungen und -übermittlungen »auf Ersuchen« des Bundesamtes für Verfassungsschutz (BfV) und des Bundesnachrichtendienstes (BND) durch. Die Zwecke, zu denen dies geschieht, sind unzweifelhaft *nicht grenzschutzpolizeilicher Art*[116].

Gleichgültig, ob man diese Hilfeleistungen des BGS noch unter den herkömmlichen Amtshilfe-Begriff und damit unter § 3 Abs. 4 BVerfSchG subsumieren oder aber, wie hier vorgeschlagen, als (elektronische) Informationshilfe klassifizieren und einer Sonderregelung unterwerfen will, in jedem Fall ist im Hinblick auf die personenbezogenen Informationsübermittlungen der Gesetzgeber in Bund und Ländern zur Aktivität aufgerufen. Dem steht nicht entgegen, daß es sich jedenfalls bei einem Teil der Betroffenen um Nichtdeutsche handelt. Das RiS mag in bezug auf Ausländer stärkeren Beschränkungsmöglichkeiten unterliegen als in bezug auf Deutsche (im Sinne des Art. 116 Abs. 1 GG), als eine Ableitung aus dem allgemeinen Persönlichkeitsrecht in Verbindung mit dem Menschenwürdesatz bietet es in seinem Kerngehalt für jedermann Schutz. Der Gesetzgeber wird dem Grundsatz der möglichst präzisen und konkreten Zweckbestimmung und dem Verbot der Datensammlung auf Vorrat in ähnlicher Weise Rechnung tragen müssen, wie es die Leitlinien 1981 bei der Ersetzung der So-GK durch die »Dienstanweisung Amtshilfeersuchen« vorsahen:
- Abschaffung der Massen-(Melde-)Verfahren,
- keine Durchkämmung ganzer Gruppen zur Verdachtsgewinnung,
- Aufgabe des Schleppnetzgedankens.

114 Vgl. etwa § 2 HessVerfSchG vom 19. 7. 1951.

115 Vgl. den Polizei-Brief der Alliierten Militärgouverneure vom 14. 4. 1949, auf den das Genehmigungsschreiben der Alliierten zum Grundgesetz vom 12. 5. 1949 inhaltlich Bezug nimmt.

116 Dazu *Denninger* (Anm. 59) S. 39 f.

Mit Rücksicht auf das hier obwaltende Geheimhaltungsbedürfnis ist es allerdings nicht erforderlich, daß der Gesetzgeber selbst die einzelnen Tatbestände, die eine Aktivität der BGS-Stellen auslösen sollen, konkretisiert. Dies kann nach wie vor durch Dienstanweisung geschehen, die dann allerdings nach hier vertretener Auffassung nicht ein generalisiertes Amtshilfeersuchen wäre, sondern eine ergänzende Aufgabenbeschreibung für den BGS darstellen müßte. Aufgabe des Gesetzgebers ist es, in abstrakter Form, aber möglichst bestimmt die begrenzenden Maßstäbe, nach denen die Gruppen der Betroffenen auszuwählen sind, festzulegen. Er wird dabei auf die gesetzliche Aufgabenumschreibung für den Verfassungsschutz zurückgreifen können[117].

(II) und (III): Obwohl der frühere Präsident des Bundeskriminalamtes, Horst Herold, als ersten Grundsatz eines menschenrechtlich fundierten, international anzuerkennenden polizeilichen Datenschutzes formuliert: »Kein Datenverbund der Polizei mit anderen Behörden und Institutionen«, möchte er doch für das Einwohnermeldewesen und für die Kraftfahrzeugzulassung hiervon eine Ausnahme machen[118]. Tatsächlich sind die technisch-organisatorischen Grundlagen für einen – ausbaufähigen – Direktzugriff beliebiger oder aller Polizeidienststellen auf ein vom Kraftfahrt-Bundesamt eingerichtetes »*Zentrales Verkehrsinformationssystem*« (ZEVIS)[119] gelegt. Und die Meldebehörden werden ausdrücklich ermächtigt, einen genau umschriebenen Satz persönlicher Daten an andere Behörden, insbesondere auch an Sicherheitsbehörden, zu übermitteln, vgl. § 18 Abs. 3 MRRG vom 16. 8. 1980, § 31 Abs. 3 HessMeldeG vom 14. 6. 1982.

Es bedarf hier keiner Ausführungen darüber, daß eine Zugriffsmöglichkeit auf die in ZEVIS gespeicherten Kfz.-Halter-Daten und auf die im Einwohnermelderegister gespeicherten Daten für die polizeiliche Arbeit von erheblichem Nutzen ist. Insbesondere im Hinblick auf die Bekämpfung jeglicher irgendwie mit Kraftfahrzeugen in Zusammenhang stehender Kriminalität leuchten auch die Vorteile eines polizeilichen Direktzugriffs (im On-line-Anschluß) auf die Kfz.-Halter-Datei unmittelbar ein. Auf diese Weise kann z. B. u. U. innerhalb von Minuten geklärt werden, ob, wo und unter welchen Umständen ein Kraftfahrzeug gestohlen wurde oder sonst abhanden gekommen ist. Der Gesetzgeber, der hier – z. B. im Gesetz über das Kraftfahrt-Bundesamt – eine entsprechende Regelung über Voraussetzungen und Umfang der zu übermittelnden bzw. der direkt abrufbaren Daten zu treffen hätte, müßte allerdings gewährleisten, daß auch nur die typischerweise erforderlichen Daten (Name und Anschrift des Kfz.-Halters) dem Direktzugriff offenstehen; weitere Angaben können im besonders begründeten Einzelfall übermittelt werden.

Das auf dem Melderechtsrahmengesetz des Bundes aufbauende Hessische Meldegesetz von 1982 versucht dem Gedanken der informationellen Selbstbestimmung durch ein abgestuftes System von Auskunftsberechtigungen Rechnung zu tragen, vgl. die §§ 30 bis 35 HMG. Die Dienststellen der Vollzugspolizei sind dabei neben den anderen Sicherheits- und Strafverfolgungsbehörden sowie der Strafjustiz insofern »privilegiert«, als gegenüber ihren Auskunftsersuchen eine besondere Prüfung und Abwägung der schutzwürdigen Belange des (der) Betroffenen durch die auskunftserteilende Meldebehörde entfällt, § 31 Abs. 3 HMG. Die auskunftsersuchenden Dienststellen trifft eine Protokollierungspflicht bezüglich des Vorgangs. Diese Sonderreglung, die die Wirksamkeit der polizeilichen Arbeit fördern soll, darf nicht zu der falschen Annahme verleiten, die Polizei selbst wäre von der Beachtung

117 In Betracht kommt in erster Linie eine Ergänzung des Bundesgrenzschutzgesetzes (BGSG) vom 18. 8. 1972. Hinsichtlich des BND erweist sich auch hier das Fehlen einer gesetzlichen Grundlage als mißlich.

118 *Herold* (Anm. 102), 81.

119 Vgl. *Hessischer Datenschutzbeauftragter*, 12. Tätigkeitsbericht, 1983, S. 137 ff., 13. Tätigkeitsbericht, 1984, S. 33 ff. und 99 ff.

der materiellen, in § 7 HMG (= § 6 MRRG) normierten Datenverarbeitungskriterien entbunden. Nur haben die Sicherheitsbehörden die Prüfung der schutzwürdigen Belange des (der) Betroffenen in eigener Kompetenz und Verantwortung vorzunehmen. Da es sich dabei auch gar nicht um eine Spezialität der Melderegisterdaten und ihrer Übermittlung handelt, ist zu erwägen, ob nicht eine Vorschrift entsprechenden Inhalts jedenfalls in das Kapitel über Informationsverarbeitung und Informationshilfe aufzunehmen wäre, durch welches das Hessische Gesetz über die öffentliche Sicherheit und Ordnung ohnehin zu ergänzen ist.