Deutscher Bundestag
6. Wahlperiode

Drucksache VI/3826

Der Bundesminister des Innern
V III 4 — 131 136/162

Bonn, den 7. September 1972

An den Herrn
Präsidenten des Deutschen Bundestages

Betr.: **Schutz der Privatsphäre**

Bezug: **Kleine Anfrage der Fraktionen der SPD, FDP**
— Drucksache VI/3711 —

Namens der Bundesregierung beantworte ich die Kleine Anfrage wie folgt:

1. Wie ist der derzeitige Stand der Vorbereitung des Entwurfs eines Bundesgesetzes über den Schutz der Privatsphäre bei der Datenverarbeitung?

2. Wurden bisher die Bundesländer beteiligt?

In meinem Hause wurde noch vor Ende des Jahres 1971 ein erster Referentenentwurf eines Bundesgesetzes über den Schutz der Privatsphäre bei der Datenverarbeitung (Bundes-Datenschutzgesetz) fertiggestellt. Der Entwurf ist so angelegt, daß er die Bereiche abdeckt, für die die Gesetzgebungskompetenz des Bundes gegeben ist, also Schutz vor mißbräuchlichen Eingriffen in öffentlichen und in privaten Bereichen gewährt. Dies wurde bereits in der Antwort der Bundesregierung vom 5. Oktober 1970 (Drucksache VI/1223) auf die Kleine Anfrage der Abgeordneten Hirsch, Dichgans, Mertes und Genossen (Drucksache VI/1150) zum Ausdruck gebracht.

Die Vorbereitungsarbeiten an dem Entwurf erwiesen sich wegen der Neuartigkeit der Materie und ihrer Ausstrahlungen in weite Rechts- und Lebensgebiete als schwierig und langwierig. Es zeigten sich von der Natur der Sache her gegebene Interessengegensätze und Sachkonflikte wie die Polarität zwischen dem Informationsanspruch der Gesellschaft sowie des einzelnen und dem Anspruch auf Unversehrtheit der Privatsphäre, ohne deren Ausgleich eine zweckgerechte gesetzliche Regelung des Datenschutzes nicht denkbar ist. Ein zentrales Problem der

Druck: Bonner Universitäts-Buchdruckerei, 53 Bonn 1
Alleinvertrieb: Verlag Dr. Hans Heger, 53 Bonn-Bad Godesberg 1,
Postfach 821, Goethestraße 56, Tel. (0 22 29) 6 35 51

Datenschutzgesetzgebung besteht darin, daß Vorschriften und Maßnahmen zum Schutz des Bürgers vor Mißbrauch bei der Datenverarbeitung die Erfüllung seiner hohen Anforderungen an die Leistungsfähigkeit von Staat und Wirtschaft, die weithin nur noch mit Hilfe moderner Verfahren der Rationalisierung und Automatisierung möglich ist, beeinträchtigen können. Die vielfach geforderte Kontrolle des Datenschutzes durch eine zentrale Überwachungsinstitution der öffentlichen Hand kann durch damit verbundene Maßnahmen wie Anlegung von umfangreichen Registern und sonstigen Ansammlungen von Personendaten Gefährdungen der Privatsphäre herbeiführen, die dem Datenschutzgedanken zuwiderlaufen.

Die Beratung und Abstimmung des Entwurfs innerhalb der Bundesverwaltung und mit den Verwaltungen der Bundesländer sowie dem Kommunalbereich war demzufolge ungewöhnlich zeitraubend. Der Referentenentwurf wurde aufgrund der Ergebnisse einer Reihe von mehrtägigen Besprechungen mit Vertretern dieser Bereiche neu gefaßt. Bei den Erörterungen des Entwurfs mit den Bundesländern und dem Kommunalbereich wurde deutlich, daß die Initiative der Bundesregierung, nicht zuletzt wegen der drohenden Rechtszersplitterung auf diesem Gebiet, durchweg begrüßt und gefördert wird.

3. Hat die Bundesregierung mit Rücksicht auf die Schwierigkeit und Vielschichtigkeit der Materie Verbindung mit der Wissenschaft aufgenommen, etwa durch Erteilung von Forschungsaufträgen?
   Können gegebenenfalls Ergebnisse aus solchen Aufträgen (Gutachten oder ähnliches) dem Bundestag zugänglich gemacht werden?

Unsere Rechtsordnung kennt eine Fülle von Vorschriften auf dem Gebiet etwa des Verfassungs-, Verwaltungs-, Privat- oder Strafrechts, die dem Schutz des Persönlichkeitsrechts bzw. der Privat- oder Geheimsphäre zu dienen bestimmt sind. Gleichwohl ist eine umfassende gesetzliche Regelung des Schutzes der Privatsphäre unter dem Gesichtspunkt ihrer Gefährdung durch die Datenverarbeitung Neuland. Es erschien deshalb angezeigt und für die Vorbereitungsarbeiten an dem Regierungsentwurf eines Bundes-Datenschutzgesetzes nützlich, frühzeitig Verbindung mit Wissenschaftlern, die sich bereits mit Fragen des Datenschutzes befaßt hatten, aufzunehmen und Forschungsaufträge zu erteilen.

1. Professor Dr. Steinmüller vom Fachbereich Rechtswissenschaft der Universität Regensburg erhielt im Dezember 1970 den Auftrag, mit der von ihm gebildeten „Arbeitsgemeinschaft Datenschutz" ein Gutachten über Grundfragen des Datenschutzes zu erstellen, das auch auf eine künftige Datenschutzgesetzgebung des Bundes eingehen sollte. Das sehr umfangreiche Gutachten liegt seit Juli 1971 vor.

2. Dr. Kamlah, Assistent an der Juristischen Fakultät der Universität Erlangen, wertete in der Zeit von November 1970 bis September 1971 im Rahmen eines Forschungsauftrages amerikanische und englische Quellen über Vorschläge zur Datenschutzgesetzgebung aus. Seine Arbeit „Datenschutz im

Spiegel der anglo-amerikanischen Literatur" ist eine systematische Zusammenfassung dieser Auswertung.

3. Professor Dr.-Ing. Steinbuch und Dipl.-Ing. Wacker, Institut für Nachrichtenverarbeitung und -übertragung, Universität Karlsruhe, erarbeiteten ein Gutachten „Überlegungen zu technischen Möglichkeiten des Datenschutzes im Hinblick auf ein Bundes-Datenschutzgesetz", das im Januar 1972 vorgelegt wurde.

Diese Gutachten enthalten wertvolle Hinweise und Anregungen für die Vorbereitung des Regierungsentwurfs. Darüber hinaus wurde in vielfältiger Weise Verbindung mit dem Wissenschaftsbereich aufgenommen.

Die Gutachten sind diesem Schreiben als Anlagen beigefügt.

4. Bestehen Kontakte mit Wirtschaft, Verbänden und internationalen Institutionen, um auch von dort Vorstellungen über Notwendigkeit und Durchführbarkeit von Datenschutzregelungen in die Vorbereitungsarbeiten einfließen zu lassen?

Es wurde großer Wert darauf gelegt, die in der Wirtschaft und bei Verbänden bestehenden Auffassungen zur Datenschutzproblematik, insbesondere über Notwendigkeit und Durchführbarkeit von Datenschutzregelungen des Bundes kennenzulernen. Die Öffentlichkeitsarbeit meines Hauses zur Vorbereitung eines Bundes-Datenschutzgesetzes führte zu einer Fülle von Kontakten, aus denen sich Gespräche mit Vertretern der Wirtschaft und von Verbänden sowie schriftliche Meinungsäußerungen aus diesem Bereich ergaben. Zu erwähnen wäre auch die Teilnahme meines Hauses an einem vom Ausschuß für Wirtschaftliche Verwaltung e. V. (AWV) gebildeten Arbeitskreis, der sich mit Fragen der Datenschutzgesetzgebung befaßt. Gelegentlich der genannten Kontakte war bei Vertretern dieser Bereiche zum Teil eine gewisse Reserve gegenüber dem Gesetzgebungsvorhaben nicht zu verkennen, die wohl hauptsächlich mit den bei Beantwortung der Frage 1 erwähnten, der Datenschutzproblematik innewohnenden Interessengegensätzen und Sachkonflikten in Zusammenhang steht.

In den von der OECD 1969 und vom Europarat 1971 errichteten Arbeitsgremien zum Studium der Probleme des Schutzes der Privatsphäre bei der Datenverarbeitung wirkten Vertreter der Bundesregierung ständig mit. Es zeigt sich dabei vor allem die Bedeutung einer internationalen Zusammenarbeit auf dem Gebiet des Datenschutzes im Hinblick auf die gegenseitigen Verflechtungen in Politik, Wirtschaft und Wissenschaft und die damit verbundenen Notwendigkeiten des Datenaustausches.

5. Wie ist der weitere Gang der Vorbereitung geplant, wann kann mit der Vorlage eines Regierungsentwurfs gerechnet werden?

Es ist beabsichtigt, den nach verwaltungsinterner Beratung und Abstimmung neu gefaßten Referentenentwurf in diesen Tagen Vertretern von Verbänden und sonstigen Sachverständigen zur

Stellungnahme zuzusenden und diese zu einer Anhörung Anfang November einzuladen. Gleichzeitig wird der Entwurf nach der Gemeinsamen Geschäftsordnung der Bundesministerien den Geschäftsstellen der Fraktionen des Deutschen Bundestages und auch dem Sekretariat des Bundesrates zur Kenntnis gebracht. Nach sorgfältiger Prüfung und Auswertung der Ergebnisse dieser Anhörung wird der Entwurf, ggf. nach Überarbeitung und nochmaliger Beteiligung der Bundesressorts, Länder und Gemeinden, dem Bundeskabinett zur Entscheidung vorgelegt und sodann bei Bundesrat und Bundestag eingebracht werden. Dieses Verfahren wird kaum vor Jahresende abgeschlossen werden können.

Genscher

Grundfragen des Datenschutzes

Gutachten im Auftrag des Bundesministeriums des Innern

Prof. Dr. W. Steinmüller
B. Lutterbeck
C. Mallmann
U. Harbort
G. Kolb
J. Schneider

Juli 1971

Vorwort

Im Winter 1970/71 erhielt der Unterzeichnete vom Bundesministerium des Innern den Auftrag, ein Gutachten über Grundfragen des Datenschutzes zu erstellen. Das Gutachten sollte Vorschläge und Anregungen für eine künftige Datenschutzgesetzgebung des Bundes erarbeiten. Die Verfasser schlossen sich nach der Auftragserteilung in einer „Arbeitsgemeinschaft Datenschutz" zusammen. Das der Arbeitsgemeinschaft gesteckte Ziel, innerhalb des Zeitraumes Januar 1971—Juni 1971 die Grundlagen für ein Datenschutzgesetz des Bundes zu erarbeiten, erwies sich bei Fortschreiten ihrer Arbeit zunächst als immer problematischer. Die enge Verknüpfung von rechtlichen und technischen Details und die Tatsache, daß der Faktor Information im wesentlichen bisher nicht Gegenstand rechtlicher Erörterungen war, erforderte Anstrengungen, die mit dem geringen personellen Besatz der Arbeitsgemeinschaft auf Dauer nicht zu leisten waren.

Dieser personelle Engpaß konnte in der Spätphase unserer Untersuchungen durch die Mitarbeit der Assistenten des Lehrstuhles überbrückt werden: C. E. Eberle; H. J. Garstka; H. Tubies. Die Verfasser möchten sich auch an dieser Stelle ausdrücklich für ihre tatkräftige Unterstützung bedanken; ohne sie hätte das Gutachten in der jetzigen Form nicht entstehen können. Die Verfasser sind sich bewußt, daß wesentliche Probleme künftiger Klärung aufgegeben sind. Insoweit wartet noch ein weites Feld auf Wissenschaft und Rechtsprechung. Sie hoffen aber, daß sie dem Gesetzgeber die Hinweise haben geben können, die nach dem derzeitigen Stand der Forschung möglich waren.

Von einem eigentlichen Gesetzesvorschlag wurde abgesehen, da gewisse Alternativen noch der politischen Entscheidung bedürfen.

Das Literaturverzeichnis umfaßt zur leichteren Zugänglichkeit vor allem die deutschsprachige Literatur (im übrigen vgl. Schubert/Steinmüller: JUDAC. Jurisprudenz, Datenverarbeitung, Kybernetik [Internationale Bibliographie], München 1971).

Die Gliederung bietet zugleich eine erste Systematik des Datenschutzes.

W. Steinmüller

Gliederung

A. Grundlegung

I. Einleitung

II. Die gesellschaftliche Bedeutung der Information

III. Bedeutung der EDV in der Verwaltung

IV. Terminologie

B. Allgemeiner Teil des Datenschutzes (Individualschutz)

I. Die unbrauchbare „Privatsphäre"

II. Der neue Ansatz

Exkurs II Datensicherung

C. Besonderer Teil des Individualdatenschutzes — Öffentliche Informationsverarbeitung —

I. Topos Informationsermittlung

II. Topos Informationserfassung

III. Topos Informationsspeicherung

IV. Topos Informationsveränderung

Vorbemerkung zu den Topoi V bis VIII — Informationsweitergabe

V. Topos Informationsaustausch

VI. Topos Informationsweitergabe an Dritte

VII. Topos Informationsverbund

VIII. Topos Informationslöschung

IX. Topos Einsichts- und Auskunftsrechte; Berichtigungs- und Löschungsansprüche

X. Topos Organisatorische Kontrollmöglichkeiten

D. Informationsverarbeitung durch nicht-öffentliche Stellen

I. Grundsätzliches

Literaturverzeichnis

Achterberg, Norbert	Probleme der Funktionslehre, München 1970
Amtliches Handbuch des Deutschen Bundestages — 6. Wahlperiode —	Darmstadt und Bad Homburg v. d. H., (o. J.)
Anschütz, Gerhard Thoma, Richard (Hg.)	Handbuch des Deutschen Staatsrechts, Bd. I, Tübingen 1930 — Bd. II, Tübingen 1932 (zitiert HdbDStR I [II])
Arbeitsgruppe „EDV und Recht" im Fachbereich Rechtswissenschaft an der F. U. Berlin (1)	Juradat kämpft gegen die Informationslawine, in: Kritische Justiz 1970, S. 463 ff.
Arbeitsgruppe „EDV und Recht" im Fachbereich Rechtswissenschaft an der F. U. Berlin (2)	Die Informationsmacher. Zur Fragwürdigkeit einer privaten Datenbank für Rechtsdokumentation. Die Firma Juradat, Berlin 1970
Arbeitsgruppe für Datenverarbeitung im Bundesministerium der Justiz	Juristisches Informationssystem mit Hilfe der elektronischen Datenverarbeitung, in: Beilage 8/70 zum Bundesanzeiger Nr. 41 vom 28. Februar 1970
Arbeitsgruppe Grundbuchdatenbank, eingesetzt vom Bayerischen Staatsministerium der Justiz	Rahmen-Soll-Konzept für die Automatisierung des Grundbuchwesens und den Aufbau einer Grundstücksdatenbank, Band I bis IV, München 1971
Arndt, Adolf (1)	Umwelt und Recht, in: NJW 1960; 2040 f.
Arndt, Adolf (2)	Reform der parlamentarischen Untersuchungsausschüsse? in: DRiZ 1964, S. 290 ff.
Arndt, Klaus F.	Parlamentarische Geschäftsautonomie und autonomes Parlamentsrecht, Berlin 1966
Arnold, Hans	Behördenakten als Beweismittel im Zivilprozeß, in: NJW 1953, S. 1283 ff.
Auernhammer, Herbert (1)	Gedanken zur Datenschutzgesetzgebung, in: ÖVD O (1971), S. 23 ff.
Auernhammer, Herbert (2)	Informationssysteme im öffentlichen Bereich, in: Staats- und Kommunalverwaltung 1971, 118 ff.
Auernhammer, Herbert (3)	Überlegungen zu einem Bundesgesetz über Datenschutz, in: Bulletin des Presse- und Informationsamtes der Bundesregierung vom 9. Juni 1971, Nr. 87/1971
Bardet, Philipp	Die Organisation der Planung, Stuttgart 1965
Bartsch, Wolfgang	Informationswelle überschwemmt Wissenschaft, in: F. R. vom 13. Oktober 1970, S. 16
Bäumlin, Richard (1)	Der schweizerische Rechtsstaatsgedanke, in: Zeitschrift des Bernischen Juristenvereins, 101 (1965), S. 81 ff.
Bäumlin, Richard (2)	Die Kontrolle des Parlaments über die Regierung und Verwaltung, in: Referate und Mitteilungen des schweizerischen Juristenvereins, 100. Jahrgang, Basel 1966, S. 168 ff.
Bäumlin, Richard (3)	Staat, Recht und Geschichte, Zürich 1961
Bayerisches Staatsministerium der Finanzen (Hg.)	Die Datenverarbeitung in der bayerischen Staatsverwaltung, 1970 (o. Ort)
Becker, Erich	Verwaltungsaufgaben, in: Morstein Marx, Fritz, Verwaltung. Eine einführende Darstellung, Berlin 1965, S. 187 ff.
Behlert, Karl	Vom Organisieren, 3. Aufl., Stuttgart 1960
Benjamin, Michael	Kybernetik und staatliche Führung, in: Staat und Recht 1967, S. 1230 ff.
Berg, Klaus	Massenmedien und Menschenrechte, in: JZ 1971, S. 167 f.
Berger, Peter	Verwaltungsautomation erfordert Erweiterung der Staatshaftung, in: ADL-Nachrichten 1971, S. 56
Marschall v. Bieberstein, Fritz Freiherr	Die Verantwortlichkeit der Reichsminister, in: Anschütz, Gerhard, und Thoma, Richard (Hg.), Handbuch des Deutschen Staatsrechts, Bd. I, S. 520 ff.

Bigelow, Robert P.	Bigelow Testifies at Data Bank Hearings, in: Communications of the ACM, Vol. 14, No. 4, S. 299 f.
Blau, Helmut	Sind ausreichende Sicherungen gegen Manipulationen bei der EDV möglich?, in: Bürotechnik und Automation, Heft 1 (1971), S. 8 f.
Blum, Richard	Einführung elektronischer Datenverarbeitung in die Finanzverwaltung des Landes Rheinland-Pfalz, in: Die Verwaltung 1969, S. 235 ff.
Böckenförde, Ernst-W.	Die Organisationsgewalt im Bereich der Regierung, Berlin 1964
Böhret, Carl	Entscheidungshilfen für die Regierung, Köln 1970
Boss, Peter	Systeme der Staatsaufsicht über Versicherungsunternehmen, Berlin 1955
Brandt, Allen	Danger Ahead! Safeguard Your Computer, in: Harvard Business Review XLVI, S. 97 ff.
Brecht, Arnold	Politische Theorie, Tübingen 1961
Brennan, Jean F.	Computer „reparieren" sich selbst, in: IBM-Nachrichten 199 (1970), S. 7 ff.
Brinkmann, Gerhard (Hg.)	Grundrechtskommentar zum Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949, Bonn 1967
Brüggemann, Gerd	Werden die Bürger durch Knopfdruck durchsichtig?, in: Die Welt vom 25. Juni 1969
Buchner, Otto	Boolesche Algebra, in: Data report 4 (1969), S. 31 ff.
Buckingham, Walter	Automation und Gesellschaft, Frankfurt/M. 1964
Bühnemann, Bernt	Datenverarbeitung im Recht. Veranstaltung der Datenverarbeitungskommission des DJT anläßlich des 48. Deutschen Juristentages in Mainz, in: JA 1970, letzte Seiten 46 ff.
Bull, Hans	Verwaltung durch Maschinen, 2. Aufl., Köln, Berlin 1964
Der Bundesminister des Innern	Unterrichtung über den Stand der Vorbereitungen zur Einführung eines Personenkennzeichens: AZ VII 1 — 131 136 — 1/1 vom 1. Juli 1969
Burhenne, Wolfgang — Perband, Klaus (Hg.)	EDV-Recht, Systematische Sammlung der Rechtsvorschriften, organisatorischen Grundlagen und Entscheidungen zur elektronischen Datenverarbeitung, Berlin 1970
Burhenne, Wolfgang	Grundgesetz für die Bundesrepublik Deutschland mit den Verfassungen der Länder. Textsammlung, Bielefeld 1962
Carstanjen	Zur politischen Bedeutung der großen und kleinen Anfrage, Diss. jur., Heidelberg 1969 (noch nicht veröffentlicht)
Commerzbank AG	Richtlinien für Eröffnung und Führung von Konten und Depots, Ausgabe Mai 1965
Control Data Corporation (Hg.)	Computer Systems. Mars-III/Master. Reference Manual, Minnesota, USA, 1970
Creifelds, Carl	Rechtswörterbuch, 2. Aufl., München 1970
Dagtoglou, Prodromos	Kommentierung zu Artikel 34 GG, in: Bonner Kommentar, Hamburg 1970
Deutsch, Karl W.	Politische Kybernetik. Modelle und Perspektiven, Freiburg im Breisgau 1969
Dichgans, Hans	Das Unbehagen in der Bundesrepublik, Düsseldorf, Wien 1968
DIN-Normen der Informationsverarbeitung	DIN 44300
Dippner, Helmuth (1)	Kanzler wird moderner informiert, in: F. R. vom 5. Oktober 1970, S. 12
Dippner, Helmuth (2)	Zukunftswünsche werden durch „ORAKEL" ermittelt, in: F. R. vom 7. Oktober 1970, S. 3
Drath, Martin	Die Gewaltenteilung im heutigen deutschen Staatsrecht, in: Rausch, H. (Hg.), Zur heutigen Problematik der Gewaltentrennung, Darmstadt 1969, S. 21 ff.
Dreher, Klaus	Hammelsprung im Sitzen, in: SZ vom 2. Oktober 1970, S. 3
Dreher, Martin	Die Amtshilfe, Göttingen 1959
Drexelius, Wilhelm — Weber, Renatus	Die Verfassung der Freien und Hansestadt Hamburg vom 6. Juni 1952, Kommentar, Hamburg 1953
Düwel, Peter	Das Amtsgeheimnis, Berlin 1965
Ehmke, Horst (1)	Parlamentarische Untersuchungsausschüsse und Verfassungsschutzämter, in: DÖV 1956, S. 417 ff.

Ehmke, Horst (2)	Empfiehlt es sich, Funktion, Struktur und Verfahren der parlamentarischen Untersuchungsausschüsse grundlegend zu ändern?, in: Verhandlungen des 45. Deutschen Juristentages, Bd. II (Sitzungsberichte), München und Berlin 1965, E 7 ff.
Ehmke, Horst (3)	„Staat" und „Gesellschaft" als verfassungstheoretisches Problem, in: Festgabe für R. Smend zum 80. Geburtstag, Tübingen 1962, S. 23 ff.
Ellwein, Thomas (1)	Das Regierungssystem der Bundesrepublik Deutschland, 2. Aufl., Köln und Opladen 1965
Ellwein, Thomas (2)	Einführung in die Regierungs- und Verwaltungslehre, Stuttgart, Berlin, Köln, Mainz 1966
Ellwein, Thomas (3)	Regierung und Verwaltung. 1. Teil: Regierung und politische Führung, Stuttgart, Berlin, Köln, Mainz 1970
Ellwein, Thomas (4)	s. Ellwein, Thomas — Görlitz, Axel — in Zusammenarbeit mit Schröder, Andreas
Ellwein, Thomas — Görlitz, Axel — in Zusammenarbeit mit Schröder, Andreas	Parlament und Verwaltung. 1. Teil: Gesetzgebung und politische Kontrolle, Stuttgart, Berlin, Köln, Mainz 1967
Ermacora, Felix	Allgemeine Staatslehre, Bd. I und II, Berlin 1970
Erbach, Karl	Stichwort Verwaltungsautomation, in: Grochla, Erwin, Handwörterbuch der Organisation, Stuttgart 1969, Sp. 1734 ff.
Erman, Walter	Handkommentar zum Bürgerlichen Gesetzbuch, Bd. 1, 4. Aufl., Münster 1967
Eschenburg, Theodor	Staat und Gesellschaft in Deutschland, 5. Aufl., Stuttgart 1962
Esser, Josef	Schuldrecht, Bd. I, Allgemeiner Teil, 4. Aufl., Karlsruhe 1970
Evers, Hans	Privatsphäre und Ämter für Verfassungsschutz, Berlin 1960
Eyermann, Erich — Fröhler, Ludwig	Verwaltungsgerichtsordnung, München 1965
Fiedler, Herbert (1)	Theorie und Praxis der Automation in der öffentlichen Verwaltung, in: DÖV 1970, S. 469 ff.
Fiedler, Herbert (2)	Automatisierung im Recht und juristische Informationen. 1. Teil: Grundbegriffe der elektronischen Informationsverarbeitung und der juristischen Anwendung, in: JUS 1970, S. 432 ff.
Fiedler, Herbert (3)	Automatisierung im Recht und juristische Informatik, 2. Teil: Datenverarbeitung und Automatisierung in der öffentlichen Verwaltung, in: JUS 1970, S. 552 ff.
Fiedler, Herbert (4)	Automatisierung im Recht und juristische Informatik. 3. Teil: Elektronische Rechtsdokumentation und juristische Informationssysteme, in: JUS 1970, S. 603 ff.
Fiedler, Herbert — Klug, Ulrich — Simitis, Spiros	Vorbericht über eine Juristische Datenbank. Unveröffentlichtes Gutachten, Gießen und Köln 1969
Finkentscher, Wolfgang	Schuldrecht, 2. Aufl., Berlin 1969
Fischerhof, Hans	Technologie und Jurisprudenz. Ihre gegenseitige Durchdringung als Aufgabe unserer Zeit, in: NJW 1969, S. 1193 ff.
Flechtner, Hans-Joachim	Grundbegriffe der Kybernetik. Eine Einführung, 4. Aufl., Stuttgart 1969
Fischer, Guido	Die Betriebsführung I. Allgemeine Betriebswirtschaftslehre, 10. Auflage, Heidelberg 1964
Forsthoff, Ernst (1)	Lehrbuch des Verwaltungsrechts, I. Bd., Allgemeiner Teil, 9. Aufl., München, Berlin 1966
Forsthoff, Ernst (2)	Begriff und Wesen des sozialen Rechtsstaates, in: VVDStRL 12 (1954), S. 8 ff.
Forsthoff, Ernst (3)	Verwaltungsorganisation, in: Die Verwaltung (Schriftenfolge zur beruflichen Fortbildung der Beamten und Behördenangestellten), Bd. 7, 4. Aufl., Braunschweig 1957
Forsthoff, Ernst (4)	Der Persönlichkeitsschutz im Verwaltungsrecht, in: Festschrift für den 45. Deutschen Juristentag, Karlsruhe 1964, S. 41 ff.
Fraenkel, Ernst (1)	Diktatur des Parlaments? Parlamentarische Untersuchungsausschüsse, öffentliche Meinung und Schutz der Freiheitsrechte, in: Zeitschrift und Politik 1954, S. 99 ff.

Fraenkel, Ernst (2)	Deutschland und die westlichen Demokratien, 2. Aufl., Stuttgart, Berlin, Köln, Mainz 1964
Franke, Detlef	Daten-Mixtur aus 24 000 Akten für den Computer, in: F. R. vom 29. Juli 1970, S. 15
Freed, Roy N.	Computer Fraud-A Mangagement Trap, in: Lawand Computer Technology, Vol. 3, No. 4, S. 86 ff.
Frenkel, Max	Institutionen der Verwaltungskontrolle, Zürich 1969
Friedrich, Hannes	Staatliche Verwaltung und Wissenschaft, Frankfurt/Main 1970
Friesenhahn, Ernst	Parlament und Regierung im modernen Staat, in: VVDStRL 16 (1958), S. 9 ff.
Gäfgen, Gerhard	Theorie der wirtschaftlichen Entscheidung, 2. Aufl., Tübingen 1968
Gallwas, Hans	Faktische Beeinträchtigungen im Bereich der Grundrechte. Ein Beitrag zum Begriff der Nebenwirkungen, Berlin 1970
Gehrig, Norbert	Parlament — Regierung — Opposition. Dualismus als Voraussetzung für eine parlamentarische Kontrolle der Regierung, München 1969
Geib, Ekkehard	Verwaltungseinheit: Prinzip und Gegentendenzen, in: Morstein-Marx, Fritz (Hg.), Verwaltung, S. 148 ff., Berlin 1965
Genscher, Hans-D.	Probleme der Verwaltung von morgen, in: Moderne Mittel des Verwaltungshandels, S. 17 ff., Bonn-Bad Godesberg 1970
Gerwin, Robert	Die Computer und unsere Zivilisation, in: Universitas 1968, S. 579 ff.
Giesing, Hans-Horst	Besprechung zu N. Gehrig, Parlament — Regierung — Opposition, in: NJW 1971, S. 185
Giger, Hans	Massenmedien, Informationsbetrug und Persönlichkeitsschutz als privatrechtliches Problem. Neue Aspekte im Bereich des privatrechtlichen Persönlichkeitsschutzes, in: JZ 1971, S. 249 ff.
Giloi, Wolfgang	Der Computer und die Rechte des einzelnen, in: Datascope 2 (1970), S. 1 ff.
Glum, Friedrich	Das parlamentarische Regierungssystem in Deutschland, Großbritannien und Frankreich, 2. Aufl., München, Berlin 1965
Görlitz, Axel	Informationsmonopole durch Datenbanken, in: ZRP 1970, S. 95
Grießbauer, Hans	Auskunftswesen, Mannheim 1954
Grochla, Erwin (1)	Automation und Organisation. Die technische Entwicklung und ihre betriebswirtschaftlich organisatorischen Konsequenzen, Wiesbaden 1966
Grochla, Erwin (2)	Zur Diskussion über die Zentralisationswirkung automatischer Datenverarbeitungsanlagen, in: Zeitschrift für Organisation 1969, S. 47 ff.
Grochla, Erwin (3)	Handwörterbuch der Organisation, Stuttgart 1969
Grochla, Erwin (4)	Stichwort Automation, in: ders., Handwörterbuch der Organisation, Sp. 249 ff., Stuttgart 1969
v. d. Groeben, Klaus — Knack, Hans-J.	Allgemeines Verwaltungsgesetz für das Land Schleswig-Holstein (Landesverwaltungsgesetz), Köln, Berlin, Bonn, München 1968
Gros, Paul	Auskunftspflicht des Arbeitgebers, in: Sitzler, Friedrich (Hg.), Arbeitsrecht Blattei D. Handbuch für die Praxis (o. J.)
Gudohr, Herbert	Der gegenwärtige Stand und die künftigen Möglichkeiten der automatischen Datenverarbeitung bei der BfA, in: DAngVers (1968), S. 6 ff.
Guha, Anton-Andreas	Der Bürger im Computer, in: F. R. vom 27. Juni 1970
Habermas, Jürgen — Luhmann, Niklas	Theorie der Gesellschaft oder Sozialtechnologie — Was leistet die Systemforschung? Frankfurt 1971 (zit.: Habermas-Luhmann)
Habermas, Jürgen — v. Friedeburg, Ludwig — Oehler, Christoph — Weltz, Friedrich	Student und Politik. Eine soziologische Untersuchung zum politischen Bewußtsein Frankfurter Studenten, 2. Aufl., Neuwied, Berlin 1967
Haft, Fritjof	Elektronische Datenverarbeitung im Recht, Berlin 1970
Haft, Fritjof — Müller-Krumbhaar, Heiner	SEDOC — ein Verfahrensvorschlag zur Erschließung juristischer Literatur mit Computern, in: JA 1970, letzte Seiten S. 32 ff.
Hahn, Hugo J.	Über die Gewaltenteilung in der Wertwelt des Grundgesetzes, in: Rausch, Heinz (Hg.), Zur heutigen Problematik der Gewaltentrennung, S. 438 ff., Darmstadt 1969
Hammerbacher, Gerhard	Computer in der Rechtsanwendung, Ein Beitrag zur Frage: Können Computer im Rechtswesen eingesetzt werden? in: IBM-Nachrichten 1969, S. 663 ff.

Hamann, Andreas — Lenz, Helmut	Das Grundgesetz für die Bundesrepublik Deutschland vom 23. Mai 1949, 3. Aufl., Neuwied, Berlin 1970
Handbuch des Bundesrates	2. Aufl., Darmstadt 1963 (17. Ergänzungslieferung 1969)
Hatschek, Julius (1)	Das Interpellationsrecht im Rahmen der modernen Ministerverantwortlichkeit, Leipzig 1909
Hatschek, Julius (2)	Deutsches und Preußisches Staatsrecht, Erster Band, Berlin 1922; Zweiter Band, Berlin 1923
Heinemann, Gustav W. (1)	Empfiehlt es sich, Funktion, Struktur und Verfahren der parlamentarischen Untersuchungsausschüsse grundlegend zu ändern?, in: Verhandlungen des 45. Deutschen Juristentages, Bd. II (Sitzungsberichte), E 53 ff., München, Berlin 1965
Heinemann, Gustav W. (2)	Gesetzgebung und technischer Fortschritt, in: IBM-Nachrichten 1968, S. 82
Held, Kurt	Der autonome Verwaltungsstil der Länder und das Bundesratsveto nach Artikel 84 Abs. 1 GG, in: AöR 80 (1955), S. 64 ff.
Heller, Hermann	Staatslehre, Leiden 1934
Henkel, Heinrich	Strafverfahrensrecht, Stuttgart 1968
Hermann, Lutz	Marschiert der „große Bruder" auf Bonn?, in: Süddeutsche Zeitung vom 13. November 1968
Hertel, Joachim	Das Personenkennzeichen und die Neuordnung des Meldewesens, in: Staats- und Kommunalverwaltung 1971, S. 122 ff.
Herzog, Günter	Probleme der Anwendung der kybernetischen Modellmethode in der Kriminologie, in: Staat und Recht 1968, S. 781 ff.
Herzog, Roman	Gesetzgeber und Verwaltung, in: VVDStRL 24 (1966), S. 183 ff.
Hesse, Konrad (1)	Der Rechtsstaat im Verfassungssystem des Grundgesetzes, in: Festgabe für R. Smend zum 80. Geburtstag, S. 71 ff., Tübingen 1962
Hesse, Konrad (2)	Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, 4. Aufl., Karlsruhe 1970
Hessische Zentrale für Datenverarbeitung (Hg.)	Hessen '80. Großer Hessenplan. Entwicklungsprogramm für den Ausbau der Datenverarbeitung in Hessen, Wiesbaden 1970
v. Heydebreck, Claus-Joachim	Empfiehlt es sich, Funktion, Struktur und Verfahren der parlamentarischen Untersuchungsausschüsse grundlegend zu ändern?, in: Verhandlungen des 45. Deutschen Juristentages, Bd. II (Sitzungsberichte), E 64 ff., München, Berlin 1965
v. d. Heydte, Friedrich-August Freiherr	Stiller Verfassungswandel und Verfassungsinterpretation, in: ARSPh 39 (1950/51), S. 461 ff.
Hinkamp, Klaus	Analyse und Strukturwandel von Bundeslegislative und Bundesregierung unter besonderer Berücksichtigung der Gewaltenteilung, Diss. iur., Köln 1966
Hoffmann, Cance J.	Computers and Privacy: A Survey, in: Computing Reviews, Vol. 1, 1969, 86 ff.
Hölder, Egon	Die elektronische Datenverarbeitung und die öffentliche Verwaltung, in: Staats- und Kommunalverwaltung 1971, 114 ff.
Horn, Günter	Die Einrichtung verknüpfter supraregionaler Datenbänke. Zur Überwindung der aus den gesetzlichen Bestimmungen über die Zuständigkeit der Versicherungsträger hinsichtlich Kontenführung und Leistungsgewährung erwachsener Schwierigkeiten, in: Die Sozialversicherung 1968, S. 69
Huber, Ernst R. (1)	Deutsche Verfassungsgeschichte seit 1789, Bd. III, Stuttgart 1963
Huber, Ernst R. (2)	Der Streit um das Wirtschaftsverfassungsrecht (II), in: DÖV 1956, S. 135 ff.
Huber, Hans	Das Recht im technischen Zeitalter, Bern 1960
Hubmann, Heinrich (1)	Das Persönlichkeitsrecht, 2. Aufl., Köln, Graz 1967
Hubmann, Heinrich (2)	Der zivilrechtliche Schutz gegen Indiskretion, in: JZ 1957, S. 521 ff.
Hueck, Alfred — Nipperdey, Hans C.	Lehrbuch des Arbeitsrechts, 1. Bd., 7. Aufl., Berlin, Frankfurt 1963
Hueck, Alfred Nipperdey, Hans C. Dietz, Rolf	Nachschlagewerk des Bundesarbeitsgerichts. Arbeitsrechtliche Praxis. Kurzausgabe 1954 bis 1961, München und Berlin 1962
Imboden, Max (1)	Montesquieu und die Lehre der Gewaltentrennung, Berlin 1959
Imboden, Max (2)	Gewaltentrennung als Grundproblem unserer Zeit, in: Rausch, H. (Hg.), Zur heutigen Problematik der Gewaltentrennung, S. 487 ff., Darmstadt 1969

Imboden, Max (3)	Politische Systeme — Staatsformen, Basel, Stuttgart 1964
Interparlamentarische Arbeitsgemeinschaft (IPA)	Gesetz (Entwurf) zum Schutz der Privatsphäre gegen Mißbrauch von Datenbank-Informationen mit individualisierendem Charakter (Datenüberwachungsgesetz), KEDV-Drucksache Nr. 12
Ipsen, Hans P.	Hamburgs Verfassung und Verwaltung, Hamburg 1956
Jähnig, Werner (1)	Gemeinsame kommunale Datenverarbeitungsanlagen für integrierte Datenverarbeitung, in: Der Städtetag 1969, S. 325
Jähnig, Werner (2)	Zusammenarbeit der Gemeinden auf dem Gebiet der elektronischen Datenverarbeitung, Mitteilungen der KGSt, Sonderdruck 1968
Jähnig, Werner (3)	Mechanisierung und Automation in der Verwaltung, in: Mitteilungen der KGSt, Sonderdruck 1961
Jahn, Gerhard	Elektronische Datenverarbeitungsanlagen im Dienste der Justiz, in: Recht und Politik 3 (1970), S. 90 f.
Jahn, Ingeborg	Wenn wir alle Nummern werden, in: F. R. vom 31. Oktober 1970, S. 2
Jakob, Josef	Privacy and the Law, in: Law and Computer, Technology, Vol. 2, No. 10, S. 20 ff.
Jaumann, Anton (1)	Amtomationsgerechte Vorschriftengebung, in: Bayerische Staatszeitung Nr. 28 (1969), S. 4 ff.
Jaumann, Anton (2)	Staatspolitische Aspekte der Datenverarbeitung, unveröffentlichter Vortrag, gehalten am 21. Oktober 1970 auf dem Bayerischen Datenverarbeitungskongreß in München
Jaumann, Anton (3)	Automation und Staat, in: data report 6 (1970), S. 2 ff.
Jellinek, Georg	System der subjektiven öffentlichen Rechte, 2. Aufl., Tübingen 1905
Jesch, Dietrich	Gesetz und Verwaltung, Tübingen 1961
Joseph, Earl C.	Die Rolle des Computers in der menschlichen Gesellschaft, in: Datascope 3 (1971), S. 1 ff.
Kaiser, Joseph H. (Hg.) (1)	Planung, Bd. I, Baden-Baden 1965, Bd. II, Baden-Baden 1966, Bd. III, Baden-Baden 1968
Kaiser, Joseph H. (2)	Vorwort, in: derselbe (Hg.) Planung I, S. 7 ff., Baden-Baden 1965
Kamlah, Ruprecht (1)	Right of Privacy, Köln 1969
Kamlah, Ruprecht (2)	Datenüberwachung und Bundesverfassungsgericht, in: DÖV 1970, S. 361 ff.
Kamlah, Ruprecht (3)	Diskussionsbeiträge, in: Drucksache 14 der Kommission für Fragen der elektronischen Datenverarbeitung der Interparlamentarischen Arbeitsgemeinschaft, (1970)
Kannegießer, Karlheinz	Das gesellschaftliche System. Seine Struktur, Funktion und Organisation, in: Staat und Recht 1968, S. 29 ff.
Kassimatis, Georg	Der Bereich der Regierung, Berlin 1967
Kaufmann, Erich	Untersuchungsausschuß und Staatsgerichtshof, in: Gesammelte Schriften, Bd. I: Autorität und Freiheit, S. 309 ff., Göttingen 1960
Keller, Thomas — Raupach, Hubert	Informationslücke des Parlaments, Hannover 1970
Kerkau, Hans J.	Automatsiche Datenverarbeitung (ADV) — Kybernetik in Rechtswissenschaft und Praxis, Berlin 1970
Kessler, Uwe	Die Aktenvorlage und Beamtenaussage im parlamentarischen Untersuchungsverfahren, in: AöR 49 NF (1963), S. 313 ff.
Kienapfel, Diethelm	Urkunden und technische Aufzeichnungen, in: JZ 1971, S. 163 ff.
Kiesinger's Informationskrieg	in: Capital 9/68, S. 12 ff.
Kirsch, Werner	Entscheidungsprozesse. Bd. I: Verhaltenswissenschaftliche Ansätze der Entscheidungstheorie, Wiesbaden 1970 Bd. II: Informationsverarbeitungstheorie des Entscheidungsverhaltens, Wiesbaden 1971
Kisker, Gunter	Bericht über den 45. Deutschen Juristentag, in: JZ 1964, S. 727 f.
Klaus, Georg	Wörterbuch der Kybernetik, Frankfurt, Hamburg 1969
Kleinrahm, Kurt	Gesetzgebungshilfsdienst für deutsche Parlamente? Zur Ontologie der gesetzgeberischen Willensbildung, in: AöR 79 (1953/54), S. 137 ff.
Klett, Arnulf	Chancen der Verwaltung mit elektronischer Datenverarbeitung, in: IBM-Nachrichten 20. Jg., Heft 200 (1971), S. 97 ff.

Klug, Ulrich	Juristische Logik, 3. Aufl., Berlin 1966
Kluxen, Kurt (Hg.) (1)	Parlamentarismus, Köln, Berlin 1967
Kluxen, Kurt (2)	Die Herkunft der Lehre von der Gewaltentrennung, in: Rausch, H. (Hg.), Zur heutigen Problematik der Gewaltentrennung, S. 131 ff., Darmstadt 1969
Koellreuter, Otto	Parlament und Verwaltung, in: DJZ 1926, Sp. 857 ff.
König, René	Person, in: ders., Soziologie, S. 241 ff., Frankfurt/Main 1967
Köttgen, Arnold	Struktur und politische Funktion öffentlicher Verwaltung, in: Festschrift für G. Leibholz, Bd. II, S. 771 ff., Tübingen 1966
Kosiol, Erich (1)	Organisation der Unternehmung, Wiesbaden 1962
Kosiol, Erich (2)	Grundlagen und Methoden der Organisationsforschung, Berlin 1968
Kraushaar, Roland — Vollmeyer, Werner	Datensicherung beim Erfassen, Übertragen und Ausgeben von Daten, in: Siemens-Zeitschrift 43 (1969). Beiheft: Datenfernverarbeitung, S. 27 ff.
Krauthausen, Udo	Tatsachenerhebung und Beratung in der deutschen öffentlichen Verwaltung, in: DVBl 1958, S. 729 ff.
Krönniger, Alois	Automation — Schlüssel zur Leistungsverwaltung, in: Amtsblatt des Bayerischen Staatsministeriums für Arbeit und soziale Fürsorge 1970, S. 77 ff.
Küchenhoff, Günther — Küchenhoff, Erich	Allgemeine Staatslehre, 7. Aufl., Stuttgart, Berlin, Köln, Mainz 1971
Küster, Otto	Das Gewaltenproblem im modernen Staat, in: Rausch, H. (Hg.), Zur heutigen Problematik der Gewaltentrennung, S. 1 ff., Darmstadt 1969
Laband, Paul (1)	Das Staatsrecht des Deutschen Reiches, I. Bd., 2. Aufl., Freiburg 1888
Laband, Paul (2)	Das Interpellationsrecht, in: DJZ 1909, S. 677 ff.
Lammers, Hans H.	Parlamentarische Untersuchungsausschüsse, in: Anschütz, Gerhard, und Thoma Richard, Handbuch des Deutschen Staatsrechts, Bd. II, S. 454 ff.
Lammers, Hans — Simons, Walter	Die Rechtsprechung des Staatsgerichtshofs für das Deutsche Reich und des Reichsgerichts aufgrund Artikel 13 Abs. 2 der Reichsverfassung, Bd. I, Berlin 1929
Lampe, Ernst-Joachim	Fälschung technischer Aufzeichnungen, in: NJW 1970, S. 1097 ff.
Landmann, Robert — Rohmer, Gustav — Eyermann, Erich — Fröhler, Ludwig	Gewerbeordnung. Kommentar, 12. Aufl., München 1964
Lang, Eberhard	Zu einer kybernetischen Staatslehre. Eine Analyse des Staates auf der Grundlage des Regelkreismodells, Salzburg 1970
Langreuter, Friedrich W.	Wer regiert die Datenbanken? in: Planet 2 (Juli/August 1969), S. 79 ff.
Lechner, Hans — Hülshoff, Klaus	Parlament und Regierung, 2. Aufl., München, Berlin 1958
Lehmann-Grube, Hinrich	Der Anwender und seine Anforderung an das Informationssystem, hektographierter Projektbericht, Köln 1969
Lehmbruch, Gerhard	Einführung in die Politikwissenschaft, Stuttgart, Berlin, Köln, Mainz 1967
Leibholz, Gerhard (1)	Die Kontrollfunktion des Parlaments, in: Macht und Ohnmacht der Parlamente, S. 57 ff., Stuttgart 1965
Leibholz, Gerhard (2)	Das Wesen der Repräsentation und der Gestaltwandel der Demokratie im 20. Jahrhundert, 3. erweiterte Aufl., Berlin 1966
Leibholz, Gerhard (3)	Strukturprobleme der modernen Demokratie, 3. erweiterte Aufl., Karlsruhe 1967
Leibholz, Gerhard (4)	Gesellschaftsordnung, Verbände, Staatsordnung, in: Leibholz, Gerhard, Strukturprobleme der modernen Demokratie, 3. Aufl., S. 326 ff. Karlsruhe 1967
Leibholz, Gerhard — Rinck, Hans J.	Grundgesetz für die Bundesrepublik Deutschland. Kommentar an Hand der Rechtsprechung des Bundesverfassungsgerichts, 3. Aufl., Köln, Marienburg 1968
Leisner, Walter	Grundrechte und Privatrecht, München 1960
Lewald, Walter	Enquêterecht und Aufsichtsrecht, in: AöR 5 (1923), S. 269 ff.
Loewenstein, Karl (1)	Verfassungslehre, 2. Aufl., Tübingen 1969
Loewenstein, Karl (2)	Das Gleichgewicht zwischen Legislative und Exekutive: Eine vergleichende verfassungsrechtliche Untersuchung, in: Rausch, H. (Hg.), Zur heutigen Problematik der Gewaltentrennung, S. 210 ff., Darmstadt 1969

Luhmann, Niklas (1)	Der Funktionsbegriff in der Verwaltungswissenschaft, in: Verw.-Arch. 49 (1958), S. 97 ff.
Luhmann, Niklas (2)	Funktionen und Folgen formaler Organisation, Berlin 1964
Luhmann, Niklas (3)	Recht und Automation in der öffentlichen Verwaltung, Berlin 1966
Luhmann, Niklas (4)	Theorie der Verwaltungswissenschaft. Bestandsaufnahme und Entwurf, Köln 1966
Luhmann, Niklas (5)	Grundrechte als Institution, Berlin 1965
Lutz, Theo	Was ist eine Datenbank?, in: BTA 1967, S. 250 ff.
Macht und Ohnmacht der Parlamente	Schriftenreihe der Friedrich-Naumann-Stiftung zur Politik und Zeitgeschichte Nr. 9, Stuttgart 1965
Mallmann, Walter	Schranken nichthoheitlicher Verwaltung, in: VVDStRL 19 (1961), S. 165 ff.
v. Mangoldt, Hermann — Klein, Friedrich	Das Bonner Grundgesetz, 2. Aufl., Bd. I, Berlin und Frankfurt 1966, Bd. II, Berlin und Frankfurt 1964, Bd. III, 6. Lieferung, Berlin und Frankfurt 1969
Marcic, René	Abriß einer Genealogie des Gewaltenteilungsprinzips, in: Perennitas. Festschrift für Thomas Michels, S. 642 ff., Münster 1963
Markull, Fritz	Rationalisierung in der öffentlichen Verwaltung, in: Verw.-Arch., Bd. 48 (1957), S. 5 ff.
Maunz, Theodor	Deutsches Staatsrecht, 17. Aufl., München 1969
Maunz, Theodor — Dürig, Günter — Herzog, Roman	Grundgesetz. Kommentar Bd. I, II, 3. Aufl., München 1969
Maurach, Reinhard	Deutsches Strafrecht, Besonderer Teil, 5. Aufl., Karlsruhe 1969
Mayntz, Renate	Soziologie der Organisation, Reinbeck, Hamburg 1969
Medicus, Dieter	Bürgerliches Recht, 3. Aufl., Köln 1970
Meincke, Eberhard	Integrierte Datenverarbeitung in der öffentlichen Verwaltung unter besonderer Berücksichtigung der Kommunalverwaltung, Köln 1970
Menke-Glückert, Peter	Datenbanken als Bürgerschreck?, in: Beilage der Süddeutschen Zeitung am 18. September 1968
Meyer, Poul	Die Verwaltungsorganisation, Göttingen 1962
Meyer, Georg	Lehrbuch des Deutschen Staatsrechts, in: 6. Aufl., bearbeitet von Gerhard Anschütz, Leipzig 1905
Meyer-Uhlenried, Karl-H.	Systemanalyse und Entwurf eines integrierten, automatisierbaren Informations- und Dokumentationssystems, dargestellt am Projekt „Entwicklung eines Dokumentationssystems für die Parlamentsmaterialien" im Auftrag des Deutschen Bundestages, München-Pullach, Berlin 1970
Miller, R. A.	Computer and Privacy, in: Michigan Law Review, Vol. 67, S. 1091 ff.
Möller, Franz	Die parlamentarischen Kontroll- und Untersuchungsrechte des Bundestages, in: RiA 1965, S. 81 ff.
Morstein-Marx, Fritz (Hg.)	Verwaltung. Eine einführende Darstellung, Berlin 1965
Mrachacz, Hans P. — Bauer, Richard	Daten optimal erfassen, München 1970
Müller, Hermann — Sax, Walter	Kommentar zur Strafprozeßordnung, 6. Aufl., Darmstadt 1966
Müller, Jörg P.	Die Grundrechte der Verfassung und der Persönlichkeitsschutz des Privatrechts, Bern 1964
Müller, Wolfgang	Schadensverhütung und Versicherung für Datenverarbeitungsanlagen, Datenträger und Programmierungsunterlagen, in: IBM-Nachrichten 195 (1969), S. 710 ff.
Mundhenke, Ehrhard	Automatisierung der Datenverarbeitung in der Kommunalverwaltung, in: Betriebswirtschaftliche Forschung und Praxis 20 (1968), S. 706 ff.
Narr, Wolf D.	Rationalität und Regierung — Bemerkungen zum Programming-, Planning-Butgeting-System (PPBS), in: Britische Justiz 1971, S. 1 ff.
Nawiasky, Hans	Allgemeine Staatslehre, 2. Teil: Staatsgesellschaftslehre, Bd. II, Einsiedeln, Zürich, Köln 1955
Nawiasky, Hans — Leusser, Claus	Die Verfassung des Freistaates Bayern vom 2. Dezember 1946, München 1948

Neumann-Hofer, Adolf	Die Wirksamkeit der Kommissionen in den Parlamenten, in: Zeitschrift für Politik 1911, S. 51 ff.
Nipperdey, Hans C. (1) (Hg.)	Die Grundrechte und Grundpflichten der Reichsverfassung. Kommentar zum zweiten Teil der Reichsverfassung, Bd. I, Berlin 1929
Nipperdey, Hans C. (2)	Grundrechte und Privatrecht. Eine Universitätsrede, in: Festschrift für Erich Molitor zum 75. Geburtstag, S. 17 ff., München, Berlin 1962
Nipperdey, Hans C. (3)	Die Würde des Menschen, in: Neumann, Franz L. — Nipperdey, Hans C. — Scheuner, Ulrich, Die Grundrechte. Handbuch der Theorie und Praxis der Grundrechte, Bd. II, 2. Aufl., S. 1 ff., Berlin 1968
Nordsieck-Schröer, Hildegard	Organisationslehren. Eine vergleichende Darstellung, Stuttgart 1961
Obermayer, Klaus	Allgemeines Verwaltungsrecht, in: Mang, Johann — Maunz, Theodor — Mayer, Franz — Obermayer, Klaus, Staats- und Verwaltungsrecht in Bayern, 3. Aufl., S. 118 ff., München 1968
Odewald, Jens	Der parlamentarische Hilfsdienst in den Vereinigten Staaten von Amerika und in der Bundesrepublik Deutschland, Berlin 1967
Osswald, Albert	Verwaltungsreform und elektronische Datenverarbeitung, Stuttgart 1969
Partsch, Karl J. (1)	Parlament und Regierung im modernen Staat, in: VVDStRL 16 (1958), S. 74 ff.
Partsch, Karl J. (2)	Anmerkung zum Urteil des Niedersächsischen Staatsgerichtshofs vom 19. Dezember 1957, in: AöR 83 (1958), S. 459 ff.
Partsch, Karl J. (3)	Empfiehlt es sich, Funktion, Struktur und Verfahren der parlamentarischen Untersuchungsausschüsse grundlegend zu ändern?, in: Verhandlungen des 45. Deutschen Juristentages, Bd. I (Gutachten), Teil 3, München, Berlin 1964
Perels, Kurt	Geschäftsgang und Geschäftsformen, in: Anschütz, Gerhard, und Thoma, Richard (Hg.), Handbuch des Deutschen Staatsrechts, Bd. I, S. 449 ff.
Perschel, Wolfgang	Der geheime Behördeninformant — BVerwG, DÖV 1965, 488, in: JuS 1966, S. 231 ff.
Peters, Hans (1)	Zentralisation und Dezentralisation. Zugleich ein Beitrag zur Kommunalpolitik im Rahmen der Staats- und Verwaltungslehre, Berlin 1928
Peters, Hans (2)	Die Gewaltentrennung in moderner Sicht, in: Rausch, Heinz (Hg.), Zur heutigen Problematik der Gewaltentrennung, S. 78 ff., Darmstadt 1969
Peters, Hans (3)	Lehrbuch der Verwaltung, Berlin, Göttingen, Heidelberg 1949
Philipps, Lothar	Recht und Information, unveröffentlichtes Referat, (Freiburg 1970)
Podlech, Adalbert (1)	Verfassungsrechtliche Probleme öffentlicher Datenbanken, in: DÖV 1970, S. 473 ff.
Podlesch, Adalbert (2)	Wertungen und Werte im Recht, in: AöR 95 (1970), S. 185 ff.
Poetzsch, Fritz	Zwei Urteile des Staatsgerichtshofes über Untersuchungsausschüsse, in: AöR 43 (1922), S. 210 ff.
Pollock, Friedrich	Automation. Materialien zur Beurteilung der ökonomischen und sozialen Folgen, Frankfurt/Main 1964
Presse und Informationsamt der Bundesregierung	Bulletin Nr. 115 vom 13. September 1968, S. 990 f.
Projektgruppe Juristisches Informationssystem	1. Zwischenbericht über die Arbeiten der Projektgruppe Juristisches Informationssystem an den Bundesminister der Justiz, in: Beilage zum Bundesanzeiger Nr. 62 vom 31. März 1971
Rasch, Ernst	Die staatliche Verwaltungsorganisation, Köln, Berlin, Bonn, München 1967
Rausch, Heinz (Hg.)	Zur heutigen Problematik der Gewaltentrennung, Darmstadt 1969
Rave, Dieter	„Datenverarbeitung im Recht" — Industrialisierung der Justiz?, in: Kritische Justiz 1970, S. 470 ff.
Redeker, Konrad — v. Oertzen, Hans-J.	Verwaltungsgerichtsordnung, 4. Aufl., Münster 1971
Reichel, Hans	Die mißbräuchliche Benutzung von Tonaufnahme- und Abhörgeräten, in: Der Betrieb 1968, S. 339 ff.
Ridder, Helmut (1)	Artikel: Untersuchungsausschuß, in: Görres-Gesellschaft (Hg.), Staatslexikon. Recht — Wirtschaft — Gesellschaft, Bd. 7, 6. Aufl., Sp. 1170 ff., Freiburg 1962
Ridder, Helmut (2)	Meinungsfreiheit, in: Neumann, Franz L. — Nipperdey, Hans C. — Scheuner, Ulrich. Die Grundrechte. Handbuch der Theorie und Praxis der Grundrechte, Bd. II, 2. Aufl., S. 1 ff., Berlin 1968

Ritzel, Heinrich G. — Koch, Helmut	Geschäftsordnung des Bundestages. Text und Kommentar, Frankfurt/Main 1952
Roese, Peter	Ein Knopfdruck genügt, in: Die Zeit vom 9. August 1968
Ruggles, Richard	Die zentrale Datenbank — Möglichkeiten ihrer Arbeitsweise, in: IBM-Nachrichten 20. Jg., Heft 200 (1970), S. 101 ff.
Rupp, Hans H.	Grundfragen der heutigen Verwaltungslehre, Tübingen 1965
Sauer, Karl	Das Interpellationsrecht in der Bundesrepublik Deutschland und im Freistaat Bayern, Diss. jur., München 1968
Schäfer, Friedrich	Der Bundestag, Köln, Opladen 1967
Schäfer, Hans	Persönlichkeitsrecht und Informationsanspruch, in: Bulletin des Presse- und Informationsamtes der Bundesregierung vom 16. April 1971, Nr. 58, S. 607 ff.
Scheubel, Josef	Stand und Organisation der Datenverarbeitung in der Staatsverwaltung Bayerns, in: ÖVD/O (1971), S. 19 ff.
Scheuner, Ulrich (1)	Über die verschiedenen Gestaltungen des parlamentarischen Regierungssystems, in: AöR 13 (1927), S. 209 ff.: 337 ff.
Scheuner, Ulrich (2)	Der Bereich der Regierung, in: Festschrift für Rudolf Smend zum 70. Geburtstag, s. 253 ff., Göttingen 1952
Scheuner, Ulrich (3)	Artikel: Staat, in: Beckerat, Erwin — Bente, Hermann u. a. (Hg.), Handwörterbuch der Sozialwissenschaften (HdSW), zugleich Neuauflage des Handwörterbuches der Staatswissenschaften, Bd. 12, S. 653 ff., Stuttgart, Tübingen, Göttingen 1965
Schmidt, Carl	Inhalt und Bedeutung des zweiten Hauptteils der Reichsverfassung, in: Anschütz, Gerhard, und Thoma, Richard (Hg.), Handbuch des Deutschen Staatsrechts, Bd. II, S. 572 ff.
Schmidt, Reimer	Rationalisierung und Privatrecht, in: AcP 1966, S. 1 ff.
Schmidt-Bleibtreu, Bruno — Klein, Franz	Die Grundrechte. Auszug aus dem Kommentar zum Grundgesetz von Schmidt — Bleibtreu — Klein, Neuwied, Berlin 1970
Schmidt-Schmiedebach, Heinrich	Datenbanken im Dienste der Gesetzgebung, der Rechtsprechung und der Verwaltung, in: Almanach 1970, S. 66 ff., Köln, Berlin, Bonn, München 1970
Schnaufer, Erich — Agthe, Klaus (Hg.)	Organisation, Berlin, Baden-Baden 1961
Schneider, Carl (1)	Datenverarbeitungslexikon, Wiesbaden 1970
Schneider, Carl (2)	Stichwort: Datensicherung, in: Schneider (1), S. 60
Schneider, Peter	Zur Problematik der Gewaltenteilung im Rechtsstaat der Gegenwart, in: Rausch, H. (Hg.), Zur heutigen Problematik der Gewaltentrennung, S. 153 ff., Darmstadt 1969
Scholler, Heinrich	Die Interpellation in Theorie und Wirklichkeit, in: Politische Studien, Jg. 21 (1970), S. 406 ff.
Schramm, Friedrich	Die parlamentarische Gesetzgebungshilfe unter besonderer Berücksichtigung der entsprechenden Einrichtungen des Deutschen Bundestages, Diss. iur., Köln 1965
Schubert, Wolfram — Steinmüller, Wilhelm (Hg.)	JUDAC — Jurisprudenz, Datenverarbeitung, Kybernetik. Internationale Bibliographie, München 1971
Schulze, Jürgen H.	Datenschutz in der Datenverarbeitung, in: IBM-Nachrichten, 21. Jg., Heft 205 (1971), S. 640 ff.
Schwarz, Otto — Kleinknecht, Theodor	Strafprozeßordnung, 28. Aufl., München 1969
Schwörbel, Dieter H.	Automation als Rechtstatsache des Bürgerlichen Rechts, Diss. iur., Hamburg 1970
Seidel, Ulrich	Persönlichkeitsrechtliche Probleme der elektronischen Speicherung privater Daten, in: NJW 1970, S. 1581 ff.
Seydel, Max	Kommentar zur Verfassungsurkunde für das Deutsche Reich, Würzburg 1873
Shaari, Jehuda	Diskussionsbeitrag, in: Macht und Ohnmacht der Parlamente, S. 84 ff.
Siemens Aktiengesellschaft (1) (Hg.)	Bayerisches Informationssystem. Beiträge zur integrierten Datenverarbeitung in der öffentlichen Verwaltung Bayerns, Heft 1 (1970)
Siemens Aktiengesellschaft (2) (Hg.)	Stichwort: Datensicherung, in: Lexikon der Datenverarbeitung, 2. Aufl., S. 122 ff., München 1969
Simitis, Spiros (1)	Informationskrise des Rechts und Datenverarbeitung, Karlsruhe 1970

Simitis, Spiros (2)	Chancen und Gefahren der elektronischen Datenverarbeitung. Zur Problematik des Datenschutzes, in: NJW 1971, S. 673 ff.
Soergel, Hans T. — Siebert, Wolfgang	Kommentar zum Bürgerlichen Gesetzbuch, Bd. 3, 10. Aufl., Stuttgart 1969
Steffani, Winfried (1)	Funktion und Kompetenz parlamentarischer Untersuchungsausschüsse, in: politische Vierteljahresschrift 1960, S. 153 ff.
Steffani, Winfried (2)	Die Untersuchungsausschüsse des Preußischen Landtages zur Zeit der Weimarer Republik, Düsseldorf 1960
Steffani, Winfried (3)	Gewaltenteilung im demokratisch-pluralistischen Rechtsstaat, in: Rausch, H. (Hg.), Zur heutigen Problematik der Gewaltentrennung, Darmstadt 1969, S. 313 ff.
Steffani, Winfried (Hg.) (4)	Parlamentarismus ohne Transparenz, Opladen 1971
Stein, Ekkehardt	Lehrbuch des Staatsrechts, Tübingen 1968
Steinbuch, Karl (1)	Die informierte Gesellschaft. Geschichte und Zukunft der Nachrichtentechnik, Reinbek bei Hamburg, April 1968
Steinbuch, Karl (2)	Falsch programmiert, 5. Aufl., München 1970
Steinbuch, Karl (Hg.) (3)	Taschenbuch der Nachrichtenverarbeitung, 2. Aufl., Berlin-Göttingen-Heidelberg 1967
Steinmüller, Wilhelm, u. a. (1)	EDV und Recht. Einführung in die Rechtsinformatik, Berlin 1970
Steinmüller, Wilhelm (2)	Rechtsinformatik. Elektronische Datenverarbeitung und Recht, in: JR 1971, S. 1 ff.
Süss, Theodor	Geheimsphäre und moderne Technik, in: Festschrift für Heinrich Lehmann zum 80. Geburtstag, Bd. I, S. 189 ff., Berlin, Tübingen, Frankfurt 1956
Stromausfall — die Achillessehne des Computers	in: F. A. Z. vom 16. Juni 1971, S. I
Van Tassel, Dennie	The Computer vs. Privacy. A Computer Bill of Rigths, in: Law and Computer, Technology, Vol. 3, No. 1, S. 2 ff.
Thiele, W.	Parlamentarische Untersuchungsausschüsse und Personalakten der Beamten, in: ZBR 1955, S. 76 ff.
Thieme, Werner	Verwaltungslehre, Köln, Berlin, Bonn, München 1967
Thoma, Richard	Die juristische Bedeutung der Grundrechte und die Artikel 102—117, in: Nipperdey (1), S. 1 ff.
Tiemann, Burkhard	Zur staatsrechtlichen Stellung und Funktion des Bundesrechnungshofes nach der Haushaltsreform, in: DVBl 1970, S. 954 ff.
Triepel, Heinrich	Die Reichsaufsicht, Berlin 1917
Trossmann, Hans	Parlamentsrecht und Praxis des Deutschen Bundestages, Bonn, o. J. (1967)
Tsatsos, Themistokles	Zur Geschichte und Kritik der Lehre von der Gewaltenteilung, Heidelberg 1968
Ule, Karl H.	Verwaltungsprozeßrecht, 4. Aufl., München 1966
in t'Veld, Joris	Hebung der Verwaltungsleistung, in: Morstein-Marx, Fritz (Hg.), Verwaltung, S. 354 ff.
Vogel, Klaus	Gesetzgeber und Verwaltung, in: VVDStRL 24 (1966), S. 125 ff.
Wahl, Manfred P.	Grundlagen eines Management-Informationssystems, Neuwied 1969
Weber, Hermann	Das hessische Datenschutzgesetz, in: JuS 1971, S. 55 f.
Weber, Max	Parlament und Regierung im neugeordneten Deutschland, in: Gesammelte politische Schriften, 2. Aufl., S. 294 ff., Tübingen 1958
Weber, Werner (1)	Staats- und Selbstverwaltung in der Gegenwart, 2. Aufl., Göttingen 1967
Weber, Werner (2)	Spannungen und Kräfte im westdeutschen Verfassungssystem, 2. Aufl., Stuttgart 1958
Weber, Werner (3)	Die Teilung der Gewalten als Gegenwartsproblem, in: Rausch, H. (Hg.), Zur heutigen Problematik der Gewaltentrennung, S. 185 ff., Darmstadt 1969
Wernicke, Kurt G.	Kommentierung zu Artikel 2 GG, in: Bonner Kommentar, Bd. 1, Hamburg 1950 ff.
Wersig, Gernot — Meyer-Uhlenried, Karl-Heinrich	Versuche zur Terminologie in der Dokumentation II: Kommunikation und Information, in: Nachrichten für Dokumentation 1969, S. 199 ff.
Westin, Alan F. (1)	Der Mensch und seine Privatsphäre, in: IBM-Nachrichten — Nr. 201 (1970), S. 189 ff., Nr. 202 (1970), S. 289 ff.

Westin, Alan F. (2)	The Computer and Privacy, in: Union Calendar No. 746; House Report No. 1842; Privacy and the National Data Bank Concept, Washington 1968, S. 25 ff.
Wieacker, Franz	Recht und Automation, in: Festschrift für Eduard Böttticher, S. 383 ff., Berlin 1969
Wiebel, Bernhard	Das Berufsgeheimnis in den freien Berufen, Köln 1970
Wiener, Norbert	Mensch und Menschmaschine. Kypernetik und Gesellschaft, 3. Aufl., Frankfurt/Main, Bonn 1966
Windsheimer, Hans	Die Information als Interpretationsgrundlage für die subjektiven öffentlichen Rechte des Artikels 5 Abs. 1 GG, Berlin 1968
Wittkämper, Gerhard W.	Grundgesetz und Interessenverbände, Köln, Opladen 1963
Wolff, Christoph	Servolenkung für das Staatsschiff, in: Die Welt (Ausgabe Berlin) vom 31. Mai 1969
Wolff, Hans J. (1)	Verwaltungsrecht I, 7. Aufl., München 1968
Wolff, Hans J. (2)	Verwaltungsrecht II. Organisations- und Dienstrecht, 3. Aufl., München 1970
Wolff, Hans-H. (3)	Verwaltungsrecht III, 2. Aufl., München 1967
Zehner, Günter	Die Rechtsprechung des Bundesverfassungsgerichts zum Aufbau des Staates, in: Das Bundesverfassungsgericht, S. 195 ff., Karlsruhe 1963
Zeidler, Karl	Zur Technisierung der Verwaltung. Eine Entgegnung, in: DVBl 61, 493 ff.
Zippelius, Reinhold	Allgemeine Staatslehre, 2. Aufl., München 1970
Zweig, Egon	Die parlamentarische Enquête nach deutschem und österreichischem Recht, in: Zeitschrift für Politik 1913, S. 264 ff.

Abkürzungsverzeichnis

a. A.	=	anderer Auffassung
a. a. O.	=	am anderen Ort
AcP	=	Archiv für civilistische Praxis
Anm.	=	Anmerkung
AöR	=	Archiv für öffentliches Recht
APKA	=	Kurzausgabe der Arbeitsrechtlichen Praxis
ARSPh	=	Archiv für Rechts- und Sozialphilosophie
Art.	=	Artikel
Aufl.	=	Auflage
Bay. EDVG	=	Bayerisches EDV-Gesetz
BayVGHE	=	Sammlung von Entscheidungen des Bayerischen Verwaltungsgerichtshofes mit Entscheidungen des Bayerischen Verfassungsgerichtshofes
Bd.	=	Band
BGB	=	Bürgerliches Gesetzbuch
BAG	=	Bundesarbeitsgericht
BGH	=	Bundesgerichtshof
BGHZ	=	Bundesgerichtshof in Zivilsachen
BR	=	Bundesrat
BT	=	Bundestag
BetrVerfG	=	Betriebsverfassungsgesetz
BTA	=	Bürotechnik und Automation
BVerfG	=	Bundesverfassungsgericht
BVerfGE	=	Entscheidungen des Bundesverfassungsgerichts
BVerwGE	=	Sammlung der Entscheidungen des Bundesverwaltungsgerichts
bzw.	=	beziehungsweise
DAngVers.	=	Die Angestelltenversicherung
ders.	=	derselbe
d. h.	=	das heißt
DJT	=	Deutscher Juristentag
Diss. jur.	=	juristische Dissertation
DJZ	=	Deutsche Juristenzeitung
DöV	=	Die öffentliche Verwaltung
DRiZ	=	Deutsche Richterzeitung
DSch	=	Datenschutz
DSchG	=	Datenschutzgesetz
DVBl	=	Deutsches Verwaltungsblatt
ebd.	=	ebenda
EDV	=	Elektronische Datenverarbeitung
EDVA	=	Elektronische Datenverarbeitungsanlage
EDVG	=	EDV-Gesetz
entspr.	=	entsprechend

EVwVfG	=	Entwurf eines Verwaltungsverfahrensgesetzes des Bundes
f.	=	folgende Seite
ff.	=	folgende Seiten
FN	=	Fußnote
F.R.	=	Frankfurter Rundschau
gem.	=	gemäß
GewO	=	Gewerbeordnung
GG	=	Grundgesetz
GOBT	=	Geschäftsordnung des Bundestages
GVBl	=	Gesetz- und Verordnungsblatt
Hg.	=	Herausgeber
h. L.	=	herrschende Lehre
h. M.	=	herrschende Meinung
i. e. S.	=	im engeren Sinne
IPA	=	Interparlamentarische Arbeitsgemeinschaft
IS	=	Informationssystem
i. S.	=	im Sinne
IV	=	Informationsverarbeitung
i. V. m.	=	in Verbindung mit
JA	=	Juristische Arbeitsblätter
Jhg.	=	Jahrgang
JR	=	Juristische Rundschau
JuS	=	Juristische Schulung
JZ	=	Juristenzeitung
KEDV-Drucksache	=	Drucksache 14 der Kommission für Fragen der Datenverarbeitung der Interparlamentarischen Arbeitsgemeinschaft
KGSt	=	Kommunale Gemeinschaftsstelle für Verwaltungsvereinfachung
KWG	=	Kreditwesengesetz
LVwG	=	Landesverwaltungsgesetz von Schleswig-Holstein
m. a. W.	=	mit anderen Worten
MdB	=	Mitglied des Bundestages
MRVO	=	Militärrechtsverordnung
m. w. N.	=	mit weiteren Nachweisen
N.	=	Nota
NJW	=	Neue Juristische Wochenschrift
Nr.	=	Nummer
ÖVD	=	Öffentliche Verwaltung und Datenverarbeitung
o. J.	=	ohne Jahr
OLG	=	Oberlandesgericht
OVG	=	Oberverwaltungsgericht
PAIS	=	Parlamentarisches Informationssystem
PKZ	=	Personenkennzeichen
PPBS	=	Programming-Planning-Budgeting System
PR	=	Privatrecht
Preuß. OVG	=	Preußisches Oberverwaltungsgericht

RGZ	=	Reichsgericht in Zivilsachen
RiA	=	Das Recht im Amt
Rspr.	=	Rechtsprechung
RuStAG	=	Reichs- und Staatsangehörigkeitsgesetz
s.	=	siehe
S.	=	Seite
s. o.	=	siehe oben
sog.	=	sogenannt
Sp.	=	Spalte
StGB	=	Strafgesetzbuch
StGH	=	Staatsgerichtshof
StPO	=	Strafprozeßordnung
str.	=	streitig
s. u.	=	siehe unten
SZ	=	Süddeutsche Zeitung
USA	=	Vereinigte Staaten von Amerika
usw.	=	und so weiter
u. U.	=	unter Umständen
v.	=	vom
VAG	=	Versicherungsaufsichtsgesetz
Verw.Arch.	=	Verwaltungsarchiv
Verw.Rspr.	=	Verwaltungsrechtsprechung
vgl.	=	vergleiche
VVDStRL	=	Veröffentlichungen der Vereinigung der deutschen Staatsrechtlehrer
VwGO	=	Verwaltungsgerichtsordnung
VwVG	=	Verwaltungsverfahrensgesetz
WRV	=	Weimarer Reichsverfassung
z. B.	=	zum Beispiel
ZBR	=	Zeitschrift für Beamtenrecht
zit.	=	zitiert
ZRP	=	Zeitschrift für Rechtspolitik
z. T.	=	zum Teil

Teil A

Grundlegung

A. Grundlegung

I. Einleitung

1. Gegenstand

Gegenstand dieser Untersuchung ist die Erstellung eines Gutachtens über ausgewählte *Grundfragen des Datenschutzrechts* im Hinblick auf die aktuellen Probleme der Datenschutzgesetzgebung des Bundes und der Länder.

Es handelt sich also um eine Arbeit, die sich vorwiegend auf *rechtspolitischem* Gebiet bewegt. Als rechtspolitisch ist in unserem Zusammenhang eine Erörterung anzusehen, wenn sie sich auf vorzuschlagende, d. h. „erwünschte" Rechtsnormen bezieht, auch wenn dies zur Kritik von vorhandenen Normen führt (z. B. Datenschutznormen der Länder).

Erwünscht ist eine Regelung dann, wenn sie von den Grundentscheidungen der Verfassung und unter Berücksichtigung der Verfassungswirklichkeit eine zweckmäßige Regelung des Rechtsgebietes erzielt, hier des Datenschutzrechtes. *Zweckmäßig* ist sie, wenn sie sowohl die Bedürfnisse des Staates, insbesondere der Verwaltung, als auch der Gesellschaft, insbesondere der Bürger, erfüllt — wobei gerade in diesem Bereich die enge Verflechtung von Staat und Gesellschaft zu beachten ist.

Wo eine solche wünschbare Regelung des Datenschutzrechts noch nicht vorgeschlagen werden kann, sei es, weil die wissenschaftliche Erörterung noch nicht soweit gediehen ist, sei es, weil die tatsächliche Entwicklung noch zu sehr im Fluß ist, sollen wenigstens die Prinzipien angegeben werden, die eine künftige Regelung bestimmen sollten.

2. Datenschutz als Kehrseite der Datenverarbeitung

Die Ausgangsthese lautet: Datenschutz ist die Kehrseite der Datenverarbeitung. Wo Datenverarbeitung, da Datenschutz. Wie der Schatten notwendig dem Licht folgt, und ohne Licht kein Schatten bestehen kann, so begleitet Datenschutz die Datenverarbeitung.

Denn zu groß sind ihre Chancen, als daß ihre Gefahren gering zu achten wären.

Folgerungen aus dieser These: Zunächst *sachlich:*

1. Datenschutz ist *nicht auf den staatlichen Bereich beschränkt,* sondern umfaßt auch die Datenverarbeitung in Wirtschaft und Wissenschaft (wobei letztere hier zweckmäßigerweise außer Betracht bleibt).
2. Datenschutz ist nicht auf den Bereich der elektronischen Datenverarbeitung beschränkt, umfaßt also auch die „Datenverarbeitung zu Fuß", insgesamt also *die manuelle, die mechanische und die automatisierte Datenverarbeitung.*

Im Hinblick darauf wird im folgenden generell statt von Datenverarbeitung von Informationsverarbeitung gesprochen. Entsprechendes gilt bezüglich der Daten/Informationen, Datenerfassung/Informationserfassung usw. (vgl. dazu die Abschnitte über die Terminologie — Teil A. IV. — und die Phasen der Informationsverarbeitung — Teil B. II. 2. —).

Daraus folgt ferner methodisch:

1. Datenschutz setzt die *Kenntnis* der grundsätzlichen Möglichkeiten der Datenverarbeitung voraus: „Was ist und was kann Datenverarbeitung?" Hierauf ist also vorweg kurz einzugehen.
2. Der Komplexität der Datenverarbeitung entspricht es allein, nicht nur juristische und rechtspolitische, sondern auch *interdisziplinäre* (informatische, system- und informationswissenschaftliche) Gesichtspunkte beizuziehen. Denn zur rechtlichen Normierung eines bestimmten Sachverhaltes (erwünschte Gestaltung der Datenverarbeitung) sind *alle* Gesichtspunkte beizuziehen, die geeignet sind, den Sachverhalt zu erhellen. Sie werden bereitgestellt von der Rechtsinformatik und der Rechtsinformationswissenschaft.

3. Beschränkungen

Im Hinblick auf das Ziel des Gutachtens sei die Untersuchung der unerwünschten Zustände beschränkt auf die Gefährdungen der sog. „Privatsphäre" durch öffentliche (Teil C) und private Datenverarbeitung (Teil D). Auf das Informationsrecht des Parlaments wird im Anhang eingegangen.

Aufgrund dieser Beschränkungen *entfällt* z. B. die Erörterung der Datenschutzproblematik im Hinblick auf das Selbstverwaltungsrecht der Gemeinden, negative Auswirkungen auf die hergebrachten Grundsätze des Berufsbeamtentums (Artikel 33 Abs. 5 GG), aber auch diejenigen Gefährdungen, die durch die Verarbeitung von nicht auf die Privatsphäre bezogenen Daten ausgehen können, namentlich der reinen Sachinformationen und der rein statistischen Informationen. Ausgeklammert ist auch die Datenschutzproblematik der Wissenschaft.

4. Aufbau

Diese Erwägungen führen zu folgendem weiteren Aufbau:

Der Faktor Information ist „Chance und Gefahr zugleich", die (auch) mit den Mitteln des Rechts bewältigt werden muß (II). Dies gilt erst recht für die Verwaltung, namentlich im Hinblick auf den Einsatz informationsverarbeitender Maschinen (III). Abschließend wird die Terminologie für das weitere Gutachten festgelegt.

Es handelt sich dabei um folgende Teile:

B — Allgemeiner Teil des Individualdatenschutzes
C — Besonderer Teil des Individualdatenschutzes — öffentliche Informationsverarbeitung —
D — Informationsverarbeitung durch nicht-öffentliche Stellen
Anhang — Das Informationsrecht des Parlaments

II. Die gesellschaftliche Bedeutung der Information

1. Gesellschaft, Staat und Information

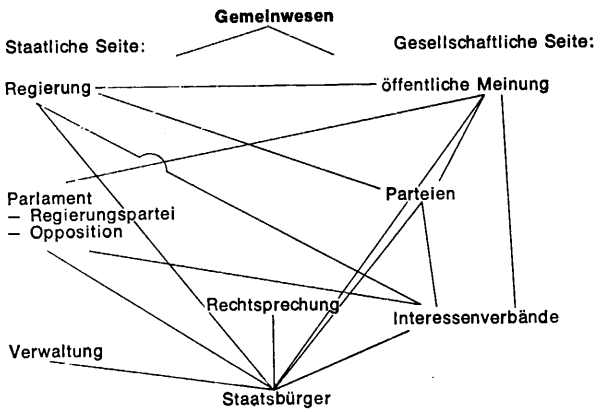
„Information", so heißt es bei Steinbuch [1]), „ist Anfang und Grundlage der Gesellschaft". Das Zusammenwirken und Zusammenleben der Menschen, so fährt er weiter fort, werde erst durch — wie immer geartete — Verarbeitung [2]) von Informationen ermöglicht.

Steinbuch drückt damit eine zentrale Erkenntnis aus, die seit N. Wieners bahnbrechenden Forschungen die Diskussion fast aller Wissenschaftler, der Natur- wie der Gesellschaftswissenschaften, beherrscht: Information beherrscht unser gesamtes Leben und ist nicht wegzudenken, ohne daß Fortschritt, Wirtschaft, Staat, die Individuen ihrer Existenzgrundlage beraubt würden. *Gesellschaft wird durch Information geradezu erst konstituiert.*

Diese hochindustrielle, stark differenzierte Gesellschaft ist ständig in ihrem Bestand bedroht: Sie ruft ständig Veränderungen hervor, schafft alte Sachverhalte und Normen ab, wechselt die Zielrichtung ihres sozialgestaltenden Willens, schafft Mißstände, die sich auf einzelne oder Gruppen negativ auswirken, sie schafft Sachverhalte *in einem* gesellschaftlich relevanten Bereich, die Auswirkungen auf die Gesellschaft *insgesamt* haben. Um es mit einem modern gewordenen Schlagwort auszudrücken: Die Gesellschaft ist in hohem Maße komplex [3]). Eine derart komplexe Gesellschaft ist in ihrem Bestand bedroht, wenn es nicht gelingt, Steuerungsmechanismen zu finden, die die sozialen Veränderungen beeinflussen können. Seit N. Wiener ist bekannt, daß diese Steuerungsmechanismen in engem Zusammenhang mit Informationen gesehen werden müssen: *Eine Lenkung der Gesellschaft ist nur möglich mit Hilfe von Informationen über den zu lenkenden Bereich.*

Das Ergebnis dieser Überlegungen scheint paradox, gleichwohl stellt es *das* gesellschaftspolitische Problem unserer Zeit dar: Einerseits wird Gesellschaft durch Informationen überhaupt erst konstituiert, andererseits ist der Bestand dieser Gesellschaft nur dann gesichert, wenn mit Hilfe von Informationen aus ihrem Bereich auf die Gesellschaft eingewirkt werden kann. Für die Beurteilung der Informationsverarbeitung ist es wichtig, daß man die Information nicht getrennt sehen kann nach ihrer Bedeutung für den Staat und — getrennt davon — für die Gesellschaft. Der Dualismus Staat — Gesellschaft wird den Problemen unserer Zeit nicht mehr gerecht [4]). Vielmehr sind beide Bereiche untrennbar zu einem Gemeinwesen verschmolzen [5]); sie bilden eine Wirkungseinheit [6]). Sie wirken zusammen, indem sie die politische Richtung des Gemeinwesens beeinflussen [7]), Prioritäten setzen und Interessen geltend machen.

Dies geschieht über folgende Einfluß- und Kommunikationskanäle [8]):



(Der Übersichtlichkeit halber sind nur die wichtigsten Beziehungen eingezeichnet.)

Regierung und Parlament einerseits, öffentl. Meinung, Parteien und Interessenverbände andererseits stehen in reger Verbindung miteinander. Sie geben Anregungen, entwickeln Zielvorstellungen und tragen vielfältige Konflikte aus. Staat und Gesellschaft sind eng miteinander gekoppelt und rückgekoppelt [9]). Als Mittel dazu dient, wie Lang sagt,

[1]) (1), 17
[2]) Der Begriff Verarbeitung wird hier zunächst unterschiedlich gebraucht.
[3]) Zu diesem Begriff vgl. neuerdings Habermas, in Habermas-Luhmann, 147: Komplexität ist ein Maß für die Anzahl von Ereignissen oder Zuständen in der Welt.
[4]) Ehmke (3), 24; Leibholz (3), 328; Hesse (2), 8 ff.; Hesse (1), 79; Stein, 23
[5]) Scheuner (3) 660; Ehmke (3), 44 ff.
[6]) Heller, 228 ff.
[7]) Scheuner (3), 660
[8]) Stein, 23
[9]) Lang, 212 ff.; Stein, 28 und 73

die Kommunikation [10]; und da Kommunikation Informationsaustausch ist [11], dient dazu auch die Information [12]. Die Bedeutung der Informationsverarbeitung bleibt also nicht auf begrenzte soziale Räume beschränkt, sondern umfaßt alle denkbaren Bereiche in Staat und Gesellschaft.

2. Chancen der EDV

Das Problem der Lenkung der Gesellschaft schien lange Zeit unlösbar: Wie sollte es möglich sein, aus der Unmenge der in der Gesellschaft anfallenden Informationen diejenigen herauszugreifen, die wirklich zur Lenkung benötigt werden? Wie sollte es möglich sein zu wissen, welche Informationen man überhaupt benötigt? Denn „nur wer weiß, was er will, weiß auch, was er wissen will" (Ellwein). Eine Antwort auf diese Fragen gab dem Staat (hier vordringlich Regierung und Verwaltung), der in erster Linie von der Verfassung zur Steuerung gesellschaftlicher Prozesse beauftragt ist, ein technisches Konzept: die EDV. Erlauben doch EDVA erstmals über den bloßen Rationalisierungseffekt hinaus jene oben beschriebene Komplexität mit Hilfe von sinnvoll zusammengestellten Informationen zu reduzieren. Voraussetzung dafür ist, daß sog. Informationssysteme entwickelt werden, die — jederzeit auskunftsbereit — gesellschaftliche Zustände, Veränderungen und zu treffende Maßnahmen dem zur Entscheidung berufenen Organ liefern. Derartige Informationssysteme sind für den Bereich des Bundes im Planungs-, sonst zum Teil schon in konkreten Entwicklungsstadium. Es sind dies

— das Bundesdatenbankprojekt [13];

— das Allgemeine arbeitsteilige universelle Informationsdatenbanksystem [14]. Zwar wird noch einige Zeit ins Land ziehen, bis diese Projekte verwirklicht sind. Sicher ist indes, daß es in diesen Systemen in Zukunft kaum einen Bereich von Belang geben wird, der nicht mit Informationen vertreten ist. Entsprechende IS im Bereich der Wirtschaft sind in Vorbereitung.

3. Gefahren der EDV

Diese Vorteile und Chancen von EDV und Informationssystemen sind nun freilich an bestimmte Voraussetzungen geknüpft. Soll das IS wirklich Informationen über alle relevanten gesellschaftlichen Bereiche liefern, müssen eben diese Bereiche nahezu lückenlos erfaßt sein. Da die Aufnahmekapazität des Systems begrenzt ist, müssen Methoden gefunden werden, die Vielzahl von Informationen Kosten und Speicherplatz sparend zu organisieren. Das wichtigste Organisationsmittel dieser Art ist das sog. Personenkennzeichen (PK), ein Ordnungsbegriff für IS, über den es möglich ist, alle irgendwo in System gespeicherten Informationen abzurufen und — vor allem — Systeme verschiedener Organisationen zu Großsystemen zu verknüpfen.

Schon bald, nachdem die Bundesregierung mit diesen Plänen an die Öffentlichkeit getreten ist, wurden Bedenken gegen diese Pläne in der Öffentlichkeit laut: Wer verfügt über die gespeicherten Informationen; welche Informationen werden gesammelt; wie erfahren Außenstehende, welche Informationen gespeichert sind? Wie kann sichergestellt werden, daß nur die Informationen über den einzelnen gespeichert werden, die wirklich zu verfassungsmäßig zulässiger Aufgabenerfüllung benötigt werden? Wie also kann den Gefahren begegnet werden, die die EDV mit sich bringt:

1. der Gefährdung der „Privatsphäre" des einzelnen;
2. der Gefährdung des Machtgleichgewichts.

Es läßt sich feststellen, daß diese Gefährdungen, die der Einsatz moderner Datenverarbeitungssysteme mit sich bringt, inzwischen in das Bewußtsein einer breiteren Öffentlichkeit gedrungen sind. Insbesondere die Publizistik hat sich dieses Themas seit Bekanntgabe des Bundesdatenbankprojekts mit großer Intensität, doch leider mit bisher wenig Sachkenntnis bemächtigt [15]. Wenn sie auch teilweise bei ihrem berechtigten Bemühen nach Aufklärung über das Ziel hinausgeschossen ist [16], so hat sie doch berichtet, daß die Öffentlichkeit dem Vorhaben der Regierung mit einem wachen Mißtrauen gegenübersteht; sie hat das Bewußtsein gegenüber diesen Gefährdungen wesentlich gestärkt. Dieser „Sensibilisierungsprozeß", dieses Mißtrauen gegenüber staatlicher Machtentfaltung ist inzwischen auch auf anderen gesellschaftlichen Bereichen zu beobachten: So ist etwa der Deutsche Anwaltsverein mit dem Vorschlag an die Öffentlichkeit getreten, Eingriffe in die Privatsphäre von Angeklagten im Strafprozeß mit Hilfe eines sog. Schuldinterlokuts [17] zurückzudrängen.

4. Die Aufgabe des Rechts

Das Recht enthält bislang explizit *keine umfassenden Normen, die den Faktor Information in seiner Bedeutung für Staat und Gesellschaft erfassen:* Es gibt noch kein *Informationsrecht* in diesem Sinne [18].

Die übergreifende Bedeutung der Information wurde auch von der Literatur noch nicht erkannt und nicht in einem bestimmten Rechtsgebiet angesiedelt. Für das Staatsrecht gilt, daß ältere Lehrbücher „Information" noch nicht einmal im Stichwortverzeichnis aufführen [19]. Neuere Lehrbücher sprechen von Information nur im Rahmen von Artikel 5 GG [20]. Ähnlich liegt die Situation bei Kommentaren [21].

[10]) Lang, 212
[11]) Steinmüller (1), 23
[12]) Lang, 236 ff.
[13]) erstmals öffentlich vorgestellt im Bulletin Nr. 115 vom 13. September 1968, S. 990 f.
[14]) vgl. 2. EDV — Bericht Drucksache VI/1953, 25 f.
[15]) vgl. etwa die Beiträge von Brüggemann, Dippner (1), (2) Görlitz, Hermann, J. Jahn, Langreiter, Menke-Glückert, Kiesinger's Informationskrieg, Roese, C. Wolff
[16]) vgl. etwa Guha, der die Bedeutung des PKZ offensichtlich verkennt
[17]) näheres in „Der Spiegel", vom 21. Juni 1971, 44
[18]) Fiedler (4), 607
[19]) Maunz, Deutsches Staatsrecht, 17. Aufl. 1969
[20]) so Hesse (2)
[21]) Maunz-Dürig-Herzog, Leibholz-Rinck

Trotzdem werden inzwischen einzelne positive Ansätze sichtbar [22]). Weitergehende Untersuchungen in dieser Richtung werden erst in neuerer Zeit durchgeführt.

4.1. Informationsrecht und Datenschutz

Die Sachverhalte, die entsprechend der Forschungsbreite des Gutachtens potentielle Gegenstände eines sog. Datenschutzgesetzes des Bundes sind, stellen sich als inhaltlich sehr verschiedene Probleme dar. Beispielsweise geht es bei der sog. „privacy"-Problematik um den Schutz des einzelnen wie von Gruppierungen, wobei die Regelungen aus den Grundrechten zu entwickeln sind; dagegen ist es eine Frage des allgemeinen Demokratieverständnisses und des Grundsatzes vom sozialen Rechtsstaat, ob und wie das gestörte „Informationsgleichgewicht" (Simitis) zwischen Regierung und Parlament, oder etwa die Sammlung von reinen Sachinformationen gesetzlich zu regeln ist. Gemeinsam ist beiden Problemen die Tatsache, daß es in beiden Fällen um die *rechtliche Würdigung von Information geht.* Es ist bislang ungeklärt, ob alle derartigen Rechtsprobleme, die man unter dem Oberbegriff *„Informationsrecht"* zusammenfassen könnte, auch Gegenstand des Datenschutzes sind. Man wird sich überlegen müssen, wo Datenschutz innerhalb eines Informationsrechts zu lokalisieren ist.

Doch fehlt bislang jeder Ansatz einer allgemeinen informationsrechtlichen Systematik mit der Folge, daß die benötigten allgemein informationsrechtlichen Gesichtspunkte für dieses Gutachten eigens erarbeitet werden mußten.

4.2. EDV-Recht

Diese Situation tritt durch die Möglichkeiten der automatisierten Informationsverarbeitung in ein neues Stadium — das kritische Stadium.

Die Gesellschaft ist aufgerufen, all das, was sich mit dem plakativen Ausdruck „Chancen und Gefahren der EDV" verbindet, in ein allgemein verbindliches Wertsystem einzubauen. Dieses Wertsystem wird in unserem sozialen Rechtsstaat in erster Linie vom Recht bereitgestellt. Das Recht hat also die Aufgabe, die Chancen und Gefahren sinnvoll gegeneinander abzuwägen und dann für alle verständliche Regeln aufzustellen. Auf diese Aufgabe ist das Recht im Bereich der Informationsverarbeitung derzeit noch nicht vorbereitet: Der zu regelnde Bereich betrifft Sachverhalte, mit dem sich das Recht bisher noch nicht befaßt hat, ja es fehlt an einer Terminologie, die zugrunde gelegt werden könnte.

Nach langen Jahren der Stagnation beginnt sich nunmehr auch die Rechtswissenschaft mit den rechtlichen Problemen zu beschäftigen, die im Gefolge des erhöhten Einsatzes elektronischer Rechenanlagen in Staat und Wirtschaft auftreten können. Diese Entwicklung ist nur zu begrüßen.

Während man in den Anfangstagen der Automation noch glaubte, sich über die Zulässigkeit automatischer Verwaltungsakte und deren mögliche Verfassungswidrigkeit streiten zu müssen [23]), war mit dem Fortschreiten der Automatisierungsbemühungen ein Ausschlagen des Pendels in genau die entgegengesetzte Richtung zu beobachten: Die öffentliche Verwaltung, allenthalben von der Arbeitslast erdrückt, hatte die EDV, mit ihr neue Techniken der Arbeitsbewältigung, als ein Mittel entdeckt, das die Probleme einer überlasteten Verwaltung lösen könnte. Man sah die großen Chancen, die die EDVA bei der Erledigung von Massenarbeiten, Planung, Freisetzung latenter produktiver Verwaltungskräfte verwirklichen könnte.

Die neu entstehenden Rechtsfragen der EDV sah man dabei freilich nicht, sieht man einmal von einigen urheberrechtlichen Veröffentlichungen ab.

Das änderte sich schlagartig mit Ankündigung des Bundesdatenbankprojektes und des Wunsches der Verwaltung, die Verwaltungsintegration durch Vergabe von Personenkennzeichen zu fördern. Wieder schlug das Pendel der Erörterung, stark beeinflußt von kulturpessimistischem Gedankengut, auf die andere Seite aus: Vor allem die Publizistik sah den „großen Bruder" auf Bonn marschieren, den Moloch Staat zu einem Leviathan Hobbes'schen Ausmaßes heranwachsen. Die dadurch hervorgerufene Beunruhigung der Öffentlichkeit dauert an. Das zeigt exemplarisch etwa der Widerstand der britischen Bevölkerung gegen die letzte Volkszählung.

Die juristische Öffentlichkeit in Deutschland erfuhr von den großen Gefahren und Rechtsproblemen, die mit dem Einsatz elektronischer Rechner verbunden sind, erstmals durch die vorzügliche Monographie Kamlahs: Seine umfassende Analyse der amerikanischen Diskussion über die Gefährdung des sog. „Right of Privacy" durch Einsatz moderner technologischer Verfahren hat die juristische Öffentlichkeit wachgerüttelt. Freilich sind seine Ergebnisse für die deutsche Diskussion nur bedingt verwendbar wegen des starken zivilistischen Ansatzes und der Tatsache, daß das deutsche Recht das Verhältnis von Zivil- und öffentlichem Recht anders sieht.

In dieser Situation kamen zwei Entscheidungen des Bundesverfassungsgerichts (BVerfG) gerade zur rechten Zeit: In beiden Entscheidungen ging es um die Frage, inwieweit Informationen der Privatsphäre des einzelnen zuzurechnen seien. Beide Entscheidungen nehmen in der laufenden rechtswissenschaftlichen Diskussion zu recht einen breiten Raum ein. Freilich sind die vom BVerfG für die sog. „Privatsphäre" angebotenen Kriterien durchweg nicht sehr brauchbar. Der eigentliche weiterführende Ansatz war, daß Bezugspunkt für die rechtliche Diskussion nicht so sehr der Einsatz elektronischer Rechner sein kann, als vielmehr die Information selbst, unabhängig von dem Medium, auf dem sie gespeichert ist.

Wieder war es Kamlah, der die Diskussion um einen wesentlichen Beitrag bereicherte. Einmal zeigte er die Tragweite der verfassungsrechtlichen Bemühung zur Bestimmung der Privatsphäre auf. Zum anderen

[22]) so bei Stein
[23]) vgl. statt aller Zeidler, 493 f.

formulierte er die sog. „Entfremdungsregel", wonach eine Entfremdung der Informationen vom ursprünglichen Verwendungszweck verboten sei. Freilich gelang es auch Kamlah nicht, brauchbare Kriterien für die Erfassung der sog. Privatsphäre zu liefern. Podlech und Steinmüller versuchen sodann die Problematik in einen größeren, staatspolitischen Zusammenhang zu stellen. Es läßt sich heute feststellen, daß eine Klärung der strittigen Fragen bislang in keinem Punkt erreicht werden konnte. Bei dieser Ausgangslage kann es nicht verwundern, daß entsprechende Gesetze der Landesgesetzgeber die neu entstandene Problematik allenfalls in Ansätzen lösen konnten und wollten. Die Gesetze vermögen daher — wiewohl sehr verdienstvoll — letztlich nicht zu befriedigen, worauf Simitis neulich zutreffend hingewiesen hat.

Die Verfasser hoffen aber, daß sie dem Gesetzgeber die Hinweise haben geben können, die nach dem derzeitigen Stand der Forschung wie nach ihrem Können möglich waren.

III. Bedeutung der EDV in der Verwaltung

Gegenstand des Gutachtens ist der Datenschutz insgesamt ohne Spezialisierung auf die elektronische Datenverarbeitung. Dies ist gerechtfertigt durch die umfassende Bedeutung des Faktors Information in der Gesellschaft, der keineswegs auf die verschiedenen Formen der automatischen Informationsverarbeitung spezialisiert beschränkt ist. Dies ist erst recht gerechtfertigt durch die fundamentale Bedeutung der Information für die öffentliche und private Verwaltung. Denn Verwaltung „ist" Informationsverarbeitung.

Da derzeit die EDV die fortgeschrittenste Form der Informationsverarbeitung darstellt, zeigt sich so am deutlichsten,

— was die Bedeutung der Informationsverarbeitung überhaupt ist,

— welche Probleme dabei auftreten

— und wo die Ansätze ihrer Regelung liegen.

Es ist also in einem eigenen grundlegenden Abschnitt über die Bedeutung der EDV in der öffentlichen und privaten Verwaltung zu handeln.

1. Qualitative Veränderungen

Die Einbeziehung des Computers, also der automatisierten IV, in die öffentliche und private Verwaltung bedeutet eine *qualitative Veränderung* und Steigerung ihrer Effizienz, damit aber auch ihrer potentiell negativen Auswirkungen.

Zwar läßt sich ex post unschwer feststellen, daß bereits jede simple Kartei in der Hand eines Beamten ein primitives Informationssystem und jeder Aktentransport eine einfache Form der IV enthält, die durch EDV nur automatisiert wird. Doch diese Automatisierung bedeutet gerade die Ausschaltung des Menschen aus bestimmten Teilen des staatlichen und privaten Handelns und Entscheidens, und damit zugleich eine weitgehende Eliminierung menschlicher Grenzen und Unzulänglichkeiten. Diese Eliminierung menschlicher Grenzen zeigt sich vor allem in vier Punkten:

a) In der teilweisen Ausschaltung des *Zeitfaktors:* Die ungeheure *Schnelligkeit* der EDV, potenziert durch „real time"-Verarbeitung, erlaubt es, Informationen in einer Zahl zu verarbeiten, die bisher aus zeitlichen Gründen nicht möglich war.

b) In der teilweisen Ausschaltung des *Raumfaktors:* Die Möglichkeit des Direktzugriffs, potenziert durch Datenfernverarbeitung, erlaubt es, Informationen auch unabhängig von ihrem Aufbewahrungsort allerorten zu verarbeiten *(„integrierte* DV").

c) In der teilweisen Ausschaltung der menschlichen Unzuverlässigkeit: Die sehr viel höhere *Genauigkeit* erlaubt es, Informationen auch dann zu verarbeiten, wenn menschliche Fehlerquellen dies bisher verhindert hätten.

d) In der teilweisen Ausschaltung der begrenzten menschlichen Aufnahme- und Verarbeitungsfähigkeit: Die — wenigstens grundsätzlich — unbegrenzte Speicherungs- und Kombinationsfähigkeit des Computers, potenziert durch die zunehmende Realisierung lernender Automaten, erlaubt eine Erhöhung der *Komplexität* der IV — und damit die Lösung bisher unlösbarer Probleme —, die den Menschen zum ersten Male mit der Möglichkeit konfrontiert, daß er bisher nicht voraussehbare und voraussagbare Ergebnisse durch EDV erhält.

2. Kein bloßes Verwaltungsmittel

Es trifft also nicht den Kern des Problems, wenn der Computer schlicht als „Verwaltungsmittel" (Jaumann) oder seine Besonderheit als „informationsverarbeitendes Verwaltungsmittel" (Steinmüller) hervorgehoben wird: Er erscheint in dieser Terminologie als beliebig handhabbares, neutrales Handwerkszeug ohne grundsätzliche Bedeutung.

Die EDV bewirkt und wird bewirken — so viel darf gegenüber bagatellisierenden Auffassungen mit Nachdruck behauptet werden — eine *Revolution* des staatlichen und unternehmerischen *Handelns,* eine tiefgreifende Veränderung der staatlichen wie der wirtschaftlichen *Organisation,* zugleich aber gibt es kaum eine Erfindung der Neuzeit, die weniger *Sachzwänge* zur Folge hat, als die EDV — entgegen vielfach geäußerten Behauptungen.

3. Computer als Denk- und Lernsimulator

Es ist durchaus irreführend, den Computer lediglich als neue Maschine in die Reihe der *technischen* Errungenschaften des Menschen zu stellen. Das übersähe seine *Eigenart.* Sie kann letztlich darauf zurückgeführt werden, daß der Computer als höchst effizienter *Denk- und Lernsimulator* das System „Verwaltung" in einem bisher nicht vorstellbaren Maß zu optimieren geeignet ist.

Die EDV scheint etwas prinzipiell Neues in der Entwicklung des Menschen darzustellen. Zum ersten Mal nämlich lernt der Mensch ein Arbeitsmittel zu konstruieren (eine „Prothese" im kybernetischen Sinn), das seine Denkfunktion teilweise nachmacht, also extern simuliert. Dieses neue Arbeitsmittel wird den Menschen ebenso verändern wie andere Arbeitsmittel, etwa das Feuer, Rad, die Schrift oder die Kraftmaschine. Wie das Feuer den Lebensraum erweiterte, das Rad den Bewegungsraum, die Buchstaben das Gedächtnis und die Kraftmaschine die physische Kraft, so verstärkt nun der Computer das menschliche Denken. Er ist „Denkprothese" und Denkverstärker, dies aber in zweifacher Hinsicht.

Zunächst ist er Verstärker rationalen, also analytischen Denkens. Man vergleiche die Rückholung von Apollo XIII; sie war nicht so sehr ein technischer Triumph als vielmehr ein Triumph des Computers.

Der Computer wird aber auch in naher Zukunft ein vielleicht ebenso effektiver Verstärker kreativen, also schöpferischen Denkens sein, da er „lernen" wird, das nichtrationale, kreative Denken des Menschen zu simulieren. Ansätze hierzu sind u. a. die Lernmatrix von Steinbuch, aber auch einschlägige software, wie sie etwa von der Heidelberger Gruppe für Systemforschung entwickelt wird.

Das bedeutet: Ebenso revolutionierend wie die Einführung der Kraftmaschinen (Auto, Fabrik, auch noch die Atommaschine) wird die Einführung der Denkverstärker sein. Vielleicht auch wird die Denkmaschine der bloßen Kraftmaschine ebenso überlegen sein, wie das Denken der bloßen Kraft überlegen ist. Darum kann man denjenigen zustimmen, die behaupten, daß der Computer wahrscheinlich für den Menschen folgenreicher sein wird, als alle Erfindungen der letzten Jahrhunderte.

Zum zweiten erlaubt der Computer, in bisher nicht vorstellbarem Ausmaße menschliches *Lernen zu simulieren.* Er ist nicht nur Denkprothese, sondern zugleich Lernsimulator. Menschliches Lernen vollzieht sich zunächst individuell im Individuum, kollektiv durch die Ansammlung, Tradition und Optimierung von Erfahrungen (Informationen) in Institutionen, Schulen und Bibliotheken.

Individuelles und kollektives Lernen vollzieht sich systemtheoretisch als *Modellbildung:* Im Lernenden, sei es eine Person oder eine Institution, wird beim Lernen durch Kombination von gespeicherten Informationen ein Modell der jeweiligen Außenwelt gebildet. Dabei ist es gleichgültig, ob sich die Speicherung individuell im menschlichen Gedächtnis, institutionell in der Organisationsstruktur behördlicher oder privater Unternehmen oder kollektiv in Karteien, Bibliotheken und Massenmedien objektiviert.

Umwelt-Modelle haben dreifache Funktion:

— Sie erlauben die Reduktion der Umweltkomplexität (Luhmann) zwecks leichterer und besserer Entscheidungsfindung;

— sie begründen die Möglichkeit, mit der Wirklichkeit über den Umweg des Modells zu experimentieren, hypothetisch verschiedene Möglichkeiten einander gegenüberzustellen und die beste auszuwählen (= Einbezug der Planungsebene in die Verwaltungsautomation);

— sie schließen zugleich unerwünschte Störungen, z. B. Dritte aus der Planung und Entscheidungsfindung aus — die wichtige, wenngleich meist unberücksichtigte Nebenwirkung.

4. Informationssysteme als Modelle

a) EDV als informationelles Modell

Die EDV erlaubt es, ein informationelles Modell von Menschen und Menschengruppen, Sachen und Sachkomplexen anzufertigen. Solche Modelle sind etwa die geplanten staatlichen oder wirtschaftlichen automatisierten Informationssysteme. Modelle haben die Eigenart, daß man mit ihnen experimentieren kann. Man kann mit ihnen all das tun, was man mit dem Original, das abgebildet wird, nicht tun kann oder nicht tun darf. (Möglicherweise kommt das daher, daß schon die Information selbst in ihrem semantischen und pragmatischen Aspekt als Modell für das, worüber sie informiert, interpretiert werden kann.) Jedenfalls liegt hierin eine wesentliche zweite gesellschaftliche Bedeutung der EDV als informationelles Modell der Gesellschaft oder ihrer Teile.

b) Informationssysteme als Bevölkerungsmodell

Ein dichtes Netz von miteinander vermaschten computerunterstützten Informationssystemen (ungenau oft Datenbanken genannt) überzieht in naher Zukunft das Staatsvolk. Dieses Netz ergibt eine abstrakte informationelle Superstruktur, die wichtige Elemente der Bevölkerung in Datenform repräsentiert. Dadurch entsteht ein teilrationales Abbild, ein „Modell" der Bevölkerung, wobei es technisch keine Schwierigkeit macht, sie als ganze oder in ihren Gruppen oder in einzelnen Personen zu erfassen.

c) Informationssysteme als Sach- und Verhaltensmodelle

Beachtung verdienen auch die Sachmodelle, besonders bei Monopolen. Wenn etwa die Bundesbahn die Frachtbriefe mit Absendern und Empfängern speichert, so erhält sie bei entsprechender Auswertung zutreffende Modelle für die Sachströme der Wirtschaft auf der Schiene, leicht zu verwenden für Planungsentscheidungen, aber auch zuungunsten des Kraftverkehrs; im übrigen bleiben alle Sachströme namentlich identifizierbar. Ebenso kann die Post durch Aufzeichnung der geführten Telefon-

gespräche (Nummern) eines oder vieler Benutzer (entpsrechend über weiterentwickelte optische Belegleser auch über Adresse und Absender von Briefen) zutreffende Informationen über das Intimverhalten, politische Tendenzen, Konkurrenzverhältnisse usw. erhalten — falls dies vom Recht erlaubt und politisch erwünscht ist. Technisch besteht jedenfalls keine unüberwindliche Schwierigkeit.

d) Bedeutung des Modellbegriffs: Experimentierfeld und Planungsinstrument

Nun muß doch etwas genauer angegeben werden, welche Funktion ein kybernetisches Modell hat. Ein solches Modell hat wenig mit Malerei zu tun, vielmehr simuliert es „etwas", nämlich das sogenannte Original, für einen bestimmten Zweck. So kann ein Plastikklumpen das menschliche Gehirn für einen Unfallforscher simulieren, der Autozusammenstöße analysieren will.

Wesentliche Funktion des Modells ist:

1. Ein Modell ist immer nur für einen *bestimmten Zweck* geeignet. Der Plastikklumpen hilft etwa einem Psychologen wenig, der das menschliche Gehirn untersuchen will.
2. Man kann mit einem Modell experimentieren, d. h. man kann mit ihm das anstellen, was mit dem Original, dem menschlichen Hirn, zu teuer, unmöglich oder verboten ist.

Die Bereitstellung eines informationellen Modells der Bevölkerung ergibt neben der Möglichkeit der Beeinflussung erstmals die Möglichkeit wissenschaftlich berechenbarer Planungsentscheidungen aufgrund der vorgegebenen, vom Politiker bestimmten Ziele. Solche Ziele sind etwa, eine bestimmte Regierung am Ruder zu halten, das Bevölkerungswachstum zu stabilisieren, oder die Inflation zu stoppen oder anzutreiben, und viele andere mehr. Für diese Ziele braucht man Planungsgrundlagen. Ein leistungsfähiges Informationssystem stellt sie bereit.

Im nächsten Ausbaustadium wird die Planung selbst über Großrechner neu organisiert und damit im Sinne eines modernen Managements rationalisiert. Schließlich werden auch die Unterziele von diesem Rationalisierungsprozeß erfaßt und endlich sogar variable Ziele optimiert. Als Experimentierobjekt und Planungsinstrument wird das IS zum Machtfaktor ersten Ranges in der Hand seines Herrn.

5. Informationssystem als Machtfaktor für den Kundigen

Da ein Informationssystem ein Modell der Bevölkerung ergibt, kann man mittels des IS mit ihr all das experimentell vornehmen, was man mit der Bevölkerung selbst nicht tun kann oder darf, sofern nur das Modell für diese Art von Experimenten geeignet ist. Damit wird die Bevölkerung insoweit transparent und berechenbar; sie wird experimentierfähig. Man kann auch hypothetische Daten angeben und dann hypothetische Bevölkerungen berechnen, um erwünschte oder befürchtete Entwicklungen steuern zu können, wie es allerorten schon für Wahlanalysen geschieht (Beispiel: Kennedy-Wahlfeldzug). Die potentiell völlige Erfassung der Bevölkerung gibt dem untersuchenden Modellsubjekt (z. B. einer Regierung) wissenschaftlich zuverlässige Informationen, etwa zur Beeinflussung in einem gewünschten Sinn, oder zur Aussonderung bestimmter Volksgruppen, z. B. Juden. Gegenmechanismen gegen diese Möglichkeiten sind bisher nicht ausgebildet. Die bisherige Datenschutzgesetzgebung reicht hierfür nicht aus. Nicht nur individueller Schutz der Privatsphäre, sondern und vor allem Minderheitenschutz ist gefordert. Demokratie im westlichen Verständnis ist wesentlich Minderheitenschutz. Das parlamentarische System ist auf diese Aufgabe noch nicht vorbereitet, muß sich ihr aber stellen.

Ein Modell ist, wie erwähnt, vorwiegend für den geeignet, der es entwirft; es ist nicht nur Modell-wovon, sondern auch stets Modell-wofür. Der Psychologe kann mit dem Plastikklumpen nichts anfangen, wohl aber der Unfallforscher, der das Modell konzipiert hat. Überträgt man das unter gewissen hier nicht zu erörternden Modifikationen auf die staatliche Wirklichkeit, so ergibt sich: In den USA, in der UdSSR, in der Bundesrepublik Deutschland wie in der DDR werden in seltener Einmütigkeit Informationssysteme für die jeweiligen Staatsregierungen und Staatsverwaltungen errichtet. So wird etwa das Bayerische Informationssystem nach den bisherigen Planungen bis 1980 fertiggestellt sein. Weil solche Informationssysteme für die Regierung und Verwaltung bestimmt sind, sind sie — cum grano salis — ungeeignet für andere; denn sie sind Modell-für-jemand, hier für die Regierung bzw. Verwaltung. Sie sind also deswegen ungeeignet für andere Staatsorgane, etwa Parlamente. Darin besteht ja gerade das Wesen des Modells, daß es Modell von etwas für jemanden ist. Da Information aber Macht ist, bedeutet ein Regierungsinformationssystem eine Entmachtung des Parlaments, falls dem Parlament nichts Gleichwertiges kompensatorisch zu Gebote steht.

Darüber hinaus bedeutet es die Zementierung der jeweiligen Regierung, sei sie schwarz, rot oder braun. Ein Informationssystem ist wertfrei und dient jedem, der darüber verfügen kann. Eine Regierung im Besitze eines effektiven Informationssystems muß sich darum schon sehr ungeschickt anstellen, wenn sie noch gestürzt werden soll. Andererseits wäre es mehr als kurzsichtig, wenn eine Regierungspartei die Planung der künftigen IS so auslegt, daß sie — einmal Opposition geworden — nur mehr schwer in die Regierungsverantwortung zurückkehren kann, weil sie — durch geeignete Organisation — die Opposition von allen wichtigen Informationen ausschloß.

Hierzu kommt verstärkend ein Funktionswandel des modernen Parlamentarismus selbst. Die „Volksvertretung" ist überwiegend, wenigstens in der Bundesrepublik Deutschland, von Beamten und Industrievertretern besetzt, also einerseits von der Regierung und der Verwaltung, andererseits von

der Wirtschaft. Damit wird der für eine parlamentarische Demokratie konstitutive Interessengegensatz zwischen Regierung und Parlament bis zur Wirkungslosigkeit abgeschwächt; auch andere Bevölkerungsgruppen, soweit sie nicht der Wirtschaft zugeordnet werden können, sind unterrepräsentiert. Dadurch wird die Kontrollfunktion des Parlaments lahmgelegt und die Gesetzgebungsfunktion regierungstreu. Die für den Staat der Neuzeit typische Gewaltenteilung hört auf, effektiv zu sein, wie Politologen längst festgestellt haben. Die Einführung eines einseitigen Regierungsinformationssystems verstärkt nur diese Entwicklung. Denn es stellt vor allem Führungsinformationen für die Regierung bereit; für Kontrollinformationen dagegen ist es nicht bestimmt, da es als Führungsinstrument in der Hand der Regierung ausgelegt ist. Es gibt keine neutrale (benutzerunabhängige) Information.

6. Datenschutz ist ein politisches, kein technisches Problem

Für die öffentliche und private Verwaltung bedeutet dies: Sie wird weit über bisher Bekanntes hinaus zu einem *„lernenden System"*, einem „Mensch-Maschine-Kommunikations-System", bei dem arbeitsteilig Mensch und Maschine je nach ihrer spezifischen Fähigkeit zur Optimierung der Verwaltung zusammenwirken.

Mensch und Maschine stehen sich nicht mehr gegenüber, sondern bilden ein komplexes System bislang unbekannter Leistungsfähigkeit, obendrein mit der Fähigkeit der Selbstoptimierung. (Damit bekommt die sog. „Verwaltungsreform" eine völlig neuartige dynamische Komponente!) Freilich — *wohin* die Optimierung geht, in Richtung einseitiger technokratischer Effizienzerhöhung, bloßer ökonomischer Rationalisierung oder mit dem Ziele eines verstärkten sozialstaatlichen Bürgerservice, ist damit noch nicht entschieden.

Denn: Welche Teile menschlichen Denkens dem Computer überlassen werden und wie diese Teilautomatisierung organisiert wird, ist im wesentlichen *menschlicher Entscheidung überlassen.* Mit anderen Worten: Die Folgen des Einsatzes der EDV im staatlichen und privaten Bereich sind zwar eine ungeheure Erhöhung der Schnelligkeit, Genauigkeit, Komprimiertheit und Komplexität öffentlicher wie privater IV, ist aber im übrigen weitestgehend *politischer Gestaltung zugänglich.* Ob also inhumane oder auch nur gesellschaftspolitisch unerwünschte Folgen entstehen, ist eine politische, keine technische Frage. Jede Berufung auf angebliche *Sachzwänge der Technik* dient nur dazu, diesen fundamentalen Sachverhalt zu verschleiern.

Angewandt auf den Datenschutz: DSch ist ein politisches (und abgeleitet: organisatorisches und finanzielles), kein technisches Problem; seine Lösung wird durch die Technik erleichtert, nicht erschwert.

Lediglich in der Kollision einer effizienten automatisierten IV mit veralteten Verwaltungsstrukturen und im damit verbundenen Widerstand staatlicher und privater Stellen gegen eine entsprechende Reorganisation liegt das Problem: die Reorganisation muß *automations- und zugleich verfassungsgerecht* sein. Das ist das eigentliche Problem des Datenschutzes. Es ist — das ist die Grundüberzeugung dieses Gutachtens — lösbar, wenn auch einige liebgewordene tradierte Vorstellungen aufgegeben werden müssen; *falls die Beteiligten des politischen Prozesses, vorweg Regierung und Parlament, einsehen, daß jede einseitige Informationskonzentration bei einer Änderung der politischen Verhältnisse zu ihren Ungunsten ausschlagen kann. Denn Information ist potentielle Macht.*

7. Datenschutz bei privater Informationsverarbeitung

Entsprechendes gilt, was nun nicht mehr weiter ausgeführt werden soll, für Informationssysteme *in privater Hand.* Auch hier haben Informationssysteme die Funktion des Denk- und Lernsimulators und dienen (qua kybernetisches Modell des Unternehmens und seiner Teile und Verflechtungen) als potentielles und potentes Experimentierfeld und Planungsinstrument.

8. Überregionale und überbetriebliche Verwaltungsintegration

Die vorläufig letzte und umfassendste Entwicklung auf dem Gebiet der EDV ist die überregionale (so im öffentlichen Bereich) bzw. überbetriebliche (im privaten Bereich) Verwaltungsintegration.

Zu ihrem Verständnis ist etwas auszuholen, da es sich um keine monokausale Entwicklung handelt, sondern aus einem Komplex von EDV-technischen, ökonomischen und institutionellen Ursachen entstanden ist (und vor allem weiter entsteht). Da diese Entwicklung erst in den Anfängen steht, aber vor größter prinzipieller Tragweite ist, weil sie die gesamte Staats- und Wirtschaftsorganisation verändert, sogar beide in einem bisher unbekannten Ausmaß zu verflechten sich anschickt, soll sie kurz erklärt werden.

Diese Erklärung ist dadurch belastet, daß sie vom derzeitigen Stand ausgeht und jederzeit durch — vor allem technische — Neuerungen überholt werden kann.

Gleichwohl muß sie vorgetragen werden, weil sie als die fortgeschrittenste Form der IV Grundlage der Topoibildung sein muß und damit des gesamten Datenschutzrechts.

Da im folgenden immer wieder auf die Probleme der Verwaltungsintegration einzugehen sein wird, hier nur kurz folgendes:

Integration bedeutet in der Konsequenz eine vollkommen neue Organisationsform (im weitesten Sinne) der Verwaltung. War bisher jeder Verwaltungszweig sein eigener Informant, so werden nun grundsätzlich alle von der Verwaltung benötigten Informationen — unabhängig von der Behördenaufteilung — nur noch einmal ermittelt (wobei die

Ermittlung arbeitsteilig organisiert sein kann), einmal erfaßt (hier gilt das gleiche), einmal gespeichert und — darauf kommt es an — vielfach verarbeitet, ausgetauscht, weitergegeben; schließlich werden sie nur einmal gelöscht.

Dies gilt freilich nur grundsätzlich und prinzipiell; die Praxis macht aus vielen Gründen, die teils technischer, teils finanzieller Art sind und laufend an Gewicht verlieren, Kompromisse mit diesem zunächst rein technokratischen Ideal, das darum erst in die bestehende Staatsorganisation einzupassen ist.

Entscheidend ist hierbei folgendes: Vom Standpunkt der einzelnen Behörde aus ermittelt sie grundsätzlich ihre Informationen nicht mehr selbst, speichert sie nicht mehr selbst — falls sie nicht gerade aus Zweckmäßigkeitsgründen diejenige Behörde ist, die für die jeweilige Information die Aufgabe der Ermittlung usw. arbeitsteilig übernommen hat. Die Information wird damit unabhängig von ihrem Ermittler, sie wird unabhängig vom Ort ihrer Erfassung und ihrer Speicherung, ja sie wird sogar unabhängig vom Ort ihrer Verarbeitung: Überall, wo sie gebraucht wird, steht sie zur Verfügung. Die Information wird — sozusagen — raum- und zeitunabhängig.

Die so geschilderte Integration kann nach dem derzeitigen Stand grundsätzlich in zwei Formen organisiert werden: Entweder wird die Aufgabe der Informationserfassung und -speicherung, evtl. sogar der Verarbeitung einer zentralen Behörde, Datenbank, Informationssystem oder ähnlichem übertragen, also einem überdimensionierten zentralen Dienstleistungsbetrieb, der die Verwaltungsfunktion „automatisierte Datenverarbeitung" zentral wahrnimmt. Diese Ausgestaltung entspricht etwa der älteren Auffassung, wie sie mit gewissen Modifikationen dem einen oder anderen Ländermodell zugrunde liegt. Die andere, neuere Auffassung geht dahin, die Möglichkeiten der Datenfernverarbeitung und moderner Organisationstheorie noch weitergehend fruchtbar zu machen. Sie macht ernst mit der (wenigstens grundsätzlichen) Zeit- und Ortsunabhängigkeit der Information, ermittelt, erfaßt und speichert die Daten bei der Behörde, wo sie anfallen, was impliziert, daß jede Behörde über einen Rechner „verfügt", organisiert aber die Datenverarbeitung so, daß die oben entwickelten Grundsätze der Integration gültig bleiben: einmal Ermittlung, einmal Erfassung, einmal Speicherung. Die Arbeitsteilung wird also auf die Spitze getrieben; die Zentralbehörde, bei der alle Fäden zusammenlaufen, wird zunächst überflüssig. Da jede Behörde über einen Rechner oder zumindest über ein Terminal verfügt, der nach ihren Bedürfnissen ausgelegt ist, vermag sie die dezentral erfaßten und gespeicherten Daten jederzeit und von jeder Stelle abzurufen und bei sich zu verarbeiten; sie kann sie auch dort, wo sie gespeichert sind, verarbeiten lassen. Entscheidend ist, daß der Datenaustausch und die Datenspeicherung nicht bei einer zentralen Behörde geschieht, sondern dezentral organisiert ist. Natürlich erlangt dieses weiterentwickelte (und nur scheinbar der bisherigen Behördenorganisation angepaßtere) Integrationsmodell erhöhte organisatorische Anstrengungen, ja geradezu informatorische Organisationskünste. Gleichwohl scheint ihm die Zukunft zu gehören. Die bisherige Zentralbehörde erleidet einen Funktionswandel: statt „Spinne im Netz" ist sie nur noch eine Schalt- und vor allem Kontrollstelle ohne eigene Verarbeitungskompetenzen. Dieses letztere Modell dürfte darum auch den Bedürfnissen des Datenschutzes besonders entgegenkommen (vgl. unten C. X).

Ähnliche Entwicklungen scheinen sich — mutatis mutandis — auch auf dem wirtschaftlichen Sektor anzubahnen; da freilich die Dinge weniger überschaubar sind, fehlt es naturgemäß an empirischem Material. Doch zwingen die heute erkennbaren ökonomischen und EDV-technischen Tendenzen zu der Annahme, daß auch dort die Entwicklung gleichgerichtet verlaufen wird — ein aus dem Gesichtspunkt der Machtzusammenballung und des Bürgerschutzes höchst unerfreulicher Gedanke, mag er auch den beteiligten Unternehmen und Konzernen unter dem Gesichtspunkt der Verwaltungsvereinfachung, Kostenminimierung noch so erfreulich erscheinen.

Es wird noch vieler Überlegungen bedürfen, ehe alle diese Probleme gesetzgebungspolitisch und gesetzgebungstechnisch bewältigt sind; es spricht einiges dafür, daß es eine Aufgabe auf vorläufig unabsehbare Zeit sein wird.

IV. Terminologie

Die hier zugrunde gelegte Terminologie ist gemäß den methodischen Vorentscheidungen unter I. 1. die der Rechtsinformatik und der Rechtsinformationswissenschaft. Sie ist deshalb eigenständig und von der Begrifflichkeit der EDV unterschieden, die teils der Mathematik, der Informatik, der Technik, der Betriebswirtschaftslehre und anderen Disziplinen entnommen ist.

Für das vorliegende Gutachten wird eine vereinfachte Terminologie zugrunde gelegt, die auf größtmögliche Verständlichkeit und Einfachheit abzielt.

Terminologisch sei für das folgende — zunächst noch ohne weitere Begründung — festgelegt:

1. Information

— einer der vieldeutigsten Begriffe fast aller Wissenschaftsdisziplinen [1]) — sei undefiniert zugrunde gelegter sog. Grundbegriff. Allgemein umfaßt er [2]) jede *Wiedergabe von Sachverhalten und Sachverhaltskomponenten* (z. B. Namen, Zahlen). Für diese Untersuchung ist es notwendig, in Übertragung von

Kategorien der Semiotik (d. h. der Lehre von den sprachlichen Zeichen) folgende vier „Ebenen" der Information einzubeziehen:

— syntaktische

— semantische

— pragmatische

— sigmatische Ebene.

Diese vier Ebenen tragen den rechtlich relevanten Fragestellungen Rechnung:

— *Wie* wird es gesagt? (syntaktisch) — wichtig für die technische Seite

— *Was* wird gesagt? (semantisch) — wichtig für die (juristische usw.) Interpretation

— *Für wen* wird es gesagt? (pragmatisch) — wichtig für Informationssysteme und die Interessen ihrer „Benutzer" [3]).

— *Auf welchen Gegenstand* bezieht sich das Gesagte?

Für die *rechtliche* Betrachtung (namentlich der öffentlichen IS) ist besonders wichtig ein Begriff der Information, der die ersten drei Ebenen einbezieht:

Information ist in diesem Sinne ein von einem Empfänger aufgenommener Sachverwalt oder eine Sachverhaltskomponente, geeignet, das Verhalten oder den Zustand des Empfängers zu beeinflussen.

Informationsverarbeitung (IV) ist jede Zustandsänderung einer Menge von Informationen, von der Informationsermittlung bis zur Informationslöschung. Diese „Stadien" oder Phasen der IV sind im Teil B. II. zu bestimmen.

Informationsrecht umfaßt die Menge aller Rechtsnormen (geltender, vergangener und zukünftiger), die Informationen oder ihre Verarbeitung zum Gegenstand haben (objektiver Begriff). Daneben gibt es das *Informationsrecht im subjektiven Sinn,* also das subjektive (öffentliche oder private) Recht eines Rechtssubjekts auf Information.

2. Daten

sind im wesentlichen „durch Zeichen(folgen) fixierte oder zur Fixierung bestimmte Informationen" [4]) oder, unter dem Gesichtspunkt der IV: Daten sind alle Informationen innerhalb des Prozesses der Datenverarbeitung.

Datenverarbeitung ist

1. der *Prozeß* der Informationsverarbeitung mit Hilfe von Daten;
2. die einzelnen *Schritte* dieses Prozesses (Datenermittlung, -erfassung, . . ., -löschung: s. u.);
3. das *Ergebnis* dieses Prozesses;
4. die *Organisation* dieses Prozesses [5]).

Im folgenden ist vor allem 1. und 2. von Belang:

Elektronische DV umfaßt richtiger alle Formen automatisierter DV (und sollte darum besser ADV oder AIV heißen), also: DV mit Hilfe von EDVA.

Automatisiert ist sie dann, wenn sie mit Hilfe von Automaten (wichtigster Fall: Computer) durchgeführt wird, also unter Ausschluß des Menschen aus dem fraglichen Teilprozeß der IV.

EDVA (Elektronische Datenverarbeitungsanlage) ist die technische Realisierung der EDV, kurz der „computer", „Rechner", u. ä., prinzipiell also ein spezieller Automat.

3. Information oder Datum?

Vorwiegend ist im folgenden von Information (statt „Datum") die Rede. Die *Begründung* liegt zunächst darin, daß nicht nur die Elektronische *Daten*verarbeitung, sondern jede, auch die manuelle oder mechanische, *Informations*verarbeitung Gegenstand des Gutachtens ist. Die Assoziation der EDV sollte vermieden werden. Vor allem aber ist „Information" gegenüber „Datum" der weitere Begriff, dessen Zugrundelegung aus wissenschaftlichen Gründen geboten erscheint (Informatik, Informationswissenschaften), da er gegenüber dem technischen (syntaktischen) Begriff des Datums die Einbeziehung der pragmatischen Ebene (Information-für-wen?) erlaubt. Darum sind

— Information und Datum,

— IV und DV,

— Informationserfassung usw. und Datenerfassung

im folgenden nicht austauschbar.

---

[1]) Wersig/Meyer-Uhlenried, 202

[2]) hierzu Flechtner, 69 ff.; Steinmüller (1), 9, 23; Klaus, 565

[3]) Im wesentlichen lassen sich drei Interessenkreise feststellen:
1. Interesse, Informationen zu sammeln und für eigene Zwecke zu verwerten;
2. Interesse, Informationen weiterzugeben;
3. Interesse, Informationen zurückzuhalten = nicht preiszugeben.

Diese Interessen lassen sich jeweils mannigfach weiter konkretisieren: in wirtschaftliche Interessen (geschäftliche Belange, Erhaltung einer Marktmacht etc.) etwa bei Auskunfteien und Verlagen, gemeinnützige Interessen und privatnützige Interessen (z. B. ein Privatmann macht sich zum eigenen Vergnügen Aufzeichnungen über das Privatleben Dritter oder über chemische Experimente). Besondere Beachtung verdienen hier die Interessen des Staates an bestimmten Informationen, soweit sie rechtlich begründet sind (Gestaltungsinteresse: z. B. Planung; Kontrollinteresse: Überwachung privater Informationsverarbeitung). Diese Dreiteilung ist ein durchaus tragfähiger systematischer Gesichtspunkt. Er ist gleichwohl für das folgende nicht als Gliederung zugrunde gelegt worden, weil — verglichen mit den wenig greifbaren Interessen — die einzelnen realen IS und die Eigentümlichkeiten ihrer IV ungleich präzisere Tatbestände sind. Selbstverständlich sind in diesem Rahmen die genannten Interessen zu berücksichtigen.

[4]) zu anderen Definitionen sowie zum folgenden: Steinmüller (1), 7 f.; Meincke, 12; Flechtner, 66 ff.

[5]) z. B. § 15 Bay. EDVG

4. Datenschutz (DSch)

Die Menge der Vorkehrungen zur Verhinderung unerwünschter Folgen von Informationsverarbeitung [6]; entsprechend dem Schutzobjekt ist zu unterscheiden zwischen DSch i. e. S. (Individualdatenschutz) und dem DSch i. w. S.

Datenschutzrecht: Die Menge der Datenschutznormen (geltender, vergangener, zukünftiger).

Unerwünscht ist jede Folge der IV, die den Zielen unserer Gesellschaft zuwiderläuft oder sie wenigstens gefährdet — sei es, weil die IV selbst unerwünscht ist, oder weil sie zwar erwünscht oder zulässig ist, aber mittelbar unerwünschte Folgen hat.

Diese *Ziele* sind vor allem niedergelegt im Grundgesetz der Bundesrepublik Deutschland; namentlich in den Grundentscheidungen dieser Verfassung, die sich bekennt zu einer rechts- und sozialstaatlich verfaßten, das Individuum und die gesellschaftlichen Gruppierungen (insbesondere Minderheiten) schützenden parlamentarischen Demokratie.

Datenschutzrecht i. e. S. (oder Recht des Individualdatenschutzes) umfaßt die Menge aller DSch-Rechtsnormen, die den Schutz des einzelnen oder von rechtlich geschützten oder zu schützenden gesellschaftlichen Gruppierungen zum Gegenstand haben.

Datenschutzrecht i. w. S. umfaßt die Menge aller sonstigen DSch-Normen.

Erläuterung:

Herkömmlich wird der Begriff des Datenschutzes zweifach eingeengt [7]; er umfaßt nur den

1. Schutz vor unerwünschter *elektronischer* Datenverarbeitung,
2. Schutz *des Bürgers,* also des (individualistisch verstandenen) einzelnen
   im Hinblick auf sein „right of privacy" [8].

Diese Beschränkung ist in drei Punkten zu eng; das Datenschutzrecht als Kehrseite der Datenverarbeitung

1. *schützt nicht nur den einzelnen,* sondern alle Rechtssubjekte, die (durch vorhandene oder künftige Rechtsnormen) eine geschützte Rechtsposition einnehmen, namentlich *alle gesellschaftlichen Gruppierungen,* die von der Entwicklung der modernen DV bedroht sein können, vor allem Minderheiten;
2. *schützt nicht nur vor automatisierter DV,* sondern vor jeglicher unerwünschter Informationsverarbeitung, auch wenn sie manuell (z. B. bei Detekteien) oder durch mechanische Hilfsmittel geschieht — bis hierher DSch i. e. S. —;
3. umfaßt nicht nur Vorkehrungen, die *unmittelbar* dem Schutz der Betroffenen dienen (z. B. Auskunftsrechte des Bürgers), sondern auch normative und institutionelle Auswirkungen auf die Staatsorganisation, ohne die ein DSch i. e. S. nicht möglich ist oder leerliefe — DSch i. w. S. (z. B. die Forderung nach einem effektiven parlamentarischen Informationssystem als Gegengewicht unerwünschter *Nebenwirkungen* der Regierungs- und Verwaltungssysteme, also exekutiver Informationsverarbeitung.

Das DSch-Recht i. e. S. umfaßt damit sowohl den Schutz des einzelnen wie gesellschaftlicher Gruppierungen vor unerwünschten Folgen jeglicher Art von IV (Recht des Individualdatenschutzes); das DSch-Recht i. w. S. dagegen umfaßt auch den Schutz innerstaatlicher Institutionen, etwa des Parlaments, oder des kommunalen Selbstverwaltungsrechts, der „hergebrachten Grundsätze des Berufsbeamtentums", bestimmter Grundrechte — sofern nicht die Möglichkeit einer Verfassungsänderung ins Auge gefaßt wird [9].

Die systematische Begründung, beide Rechtsgebiete unter einem Begriff zusammenzufassen, liegt darin, daß ohne DSch i. w. S. der Individualdatenschutz leerliefe oder gänzlich unmöglich würde.

Der DSch i. e. S., also vor allem der Schutz des Staatsbürgers, wird illusorisch, wenn er nicht zugleich durch Maßnahmen im staatlich-institutionalen Bereich abgesichert wird; umgekehrt können unerwünschte Einflüsse der EDV auf die Staatsorganisation (Datenschutz i. w. S.) ohne effektiven Individualdatenschutz nicht wirksam verhindert werden.

Datensicherung ist die Menge aller Maßnahmen (technischer, programmäßiger, organisatorischer, personeller und sonstiger Art) zum Schutz der Daten in ihrem Bestand und ihrer Organisation vor Störung, Verlust (durch Fehler, Katastrophen) und Mißbrauch (unberechtigte Verarbeitung).

Erläuterung:

Datensicherung schützt also nicht Rechtssubjekte (z. B. Bürger), sondern umfaßt alle Daten; also nicht nur solche, die Gegenstand des DSch sind, sondern auch reine Sachdaten; betrifft jedoch nicht *jegliche* IV, sondern nur *automatisierte* DV; ist nur in ihrem juristischen Aspekt Teil des DSch, insofern nämlich Datensicherung mittelbar auch dem DSch dienen *kann* (s. u. Exkurs). Diese rechtliche Normierung ist insoweit auch Teil des DSch-Rechts.

5. Systemtheoretische und informationswissenschaftliche Grundbegriffe

Ferner sind einige *systemtheoretische und informationswissenschaftliche Grundbegriffe* einzuführen:

[6] Steinmüller (1), 87 schlägt darum auch „Informationsschutz" vor, freilich ist die Bezeichnung „Datenschutz" bereits eingebürgert, und die Bezeichnung wird darum auch hier beibehalten.

[7] Zutreffend faßt dagegen Simitis (2), 675 ff. Datenschutz jede unerwünschte Datenverarbeitung, freilich unter Beschränkung auf elektronische Datenverarbeitung, und unterscheidet im übrigen — ähnlich wie hier — zwischen den beiden Bereichen des Datenschutzes.

[8] Dies ist Gegenstand des Buches von Kamlah „right of privacy".

[9] vgl. die Zusammenfassung (Teil C); z. B. DSchAmt des Parlaments als integrierender Teil des parlamentarischen IS; Grundrecht auf Information.

System ist jede Menge von Elementen und ihrer Relationen (z. B. „System" Behörde mit den „Elementen" Beamten und Angestellten und den rechtlichen oder informellen „Beziehungen", die im wesentlichen in Informationsströmen ihren Ausdruck finden).

Dynamisch ist jedes System, das mehr als einen Zustand einnimmt: es durchläuft einen *Prozeß* mit soviel *Schritten* wie Zuständen.

Da im folgenden nur von dynamischen Systemen die Rede ist, weil DSch sich ausschließlich auf dynamische Systeme bezieht (z. B. Behörden; Verwaltung; Informationssysteme), sei vereinfacht lediglich von „Systemen" gesprochen.

Informationssystem (IS) ist zunächst jedes System, das Informationen verarbeitet.

Erläuterung:

Dieser Wortgebrauch weicht teilweise von dem in der Betriebswirtschaftslehre und der Verwaltungsdatenverarbeitung Üblichen ab, ist also nicht auf Planungsinformationssysteme beschränkt, da sich das Gutachten allgemein mit den Fragen der IV in der öffentlichen und privaten Verwaltung zu befassen hat („Grundfragen" des Datenschutzes). Zwar werden IS überwiegend erst dann zu einem Problem des DSch, wenn sie sich der automatisierten IV bedienen; gleichwohl soll hier aus prinzipiellen Erwägungen jede Sammlung fixierter Informationen als Informationssystem bezeichnet werden, aus praktischen Gründen jedoch nur dann, wenn es umfassende Antworten auf gestellte Fragen ermöglicht. Denn nur für größere Informationssysteme besteht ein Regelungsbedürfnis. Im übrigen ist hervorzuheben, daß das Informationssystem bei richtiger Betrachtung [10]) auch die Benutzer umfaßt, d. h. diejenigen (natürlichen oder juristischen) Personen, die auf die Informationen des Systems verändernd einwirken (sie eingeben, abfragen, löschen).

Der häufig in diesem Zusammenhang gebrauchte Begriff *„Datenbank"* ist als terminus technicus für den Bereich der EDV festgelegt. Damit ist er in diesem Rahmen zu eng, einmal weil auch manuelle und mechanische IV erfaßt werden soll, zum anderen, weil er den Benutzer nicht als Systemelement enthält.

Modell ist die Abbildung eines Systems (z. B. der Bevölkerung) für einen Benutzer (z. B. Regierung).

Die praktische Bedeutung des Modellbegriffs besteht darin, daß EDVA sehr leistungsfähige Modelle speichern und optimieren können, so daß gewichtige juristische Probleme hinsichtlich der Auswirkungen auftreten.

6. Juristische und rechtspolitische Bezeichnungen

Schließlich seien noch folgende i. w. S. *juristische und rechtspolitische* Bezeichnungen festgelegt:

Verwaltung umfaßt auch die private (insbesondere unternehmerische) Verwaltung.

Öffentliche Verwaltung (i. w. S.) meint die Gesamtheit aller i. w. S. staatlichen Stellen, die Verwaltungstätigkeit ausüben — in Ausweitung des verwaltungswissenschaftlichen Sprachgebrauchs — sowohl die i. e. S. staatliche wie kommunale Verwaltung, gleich, ob sie die rechtsetzende, rechtsanwendende oder rechtskontrollierende Funktion ausübt (Legislative, Exekutive, Judikative).

Erläuterung:

Die staatlichen Stellen können sowohl organisatorisch selbständig (Behörden) als auch unselbständig sein. Wird im Teil C dann pauschal von der „Verwaltung" geredet, so ist darunter die Verwaltung im hier definierten weiten Sinn zu verstehen.

Öffentlich sei im übrigen jeder Gegenstand bzw. Sachverhalt (z. B. Behörde, Stelle, Datenverarbeitung), der den Angelegenheiten des Gemeinwesens oder seiner Mitglieder zu dienen bestimmt ist, sei er auch privatrechtlich organisiert.

Privat dagegen ist jeder sonstige Gegenstand bzw. Sachverhalt (z. B. privates Informationssystem).

Verwaltungstätigkeit ist jede Tätigkeit, die der Erfüllung materiell öffentlich-rechtlicher Aufgaben dient.

Erläuterung:

Eine Aufgabe gehört dann materiell dem öffentlichen Bereich an, wenn sie den Angelegenheiten des Gemeinwesens dient, gleich ob der Staat, um sie zu erfüllen, dem Bürger als Hoheitsträger oder als Leistungsträger gegenübertritt. Damit kommt es nicht darauf an, in welcher Rechtsform die Erfüllung der Aufgabe vorgenommen wird; auch die Aufgabenerfüllung in den Formen des Privatrechts ist nach dieser Definition materiell öffentlich-rechtliche Verwaltungstätigkeit. Nicht erfaßt sind dagegen rein fiskalische Aufgaben; hier ist der Staat einem Privaten gleich — und den für ihn geltenden Regelungen zu unterstellen.

Behörde ist jede organisatorisch selbständige Stelle, die Verwaltungstätigkeit ausübt.

Erläuterung:

Diese Definition entspricht der h. L. [11]) und ist auch in § 3 II LVwG von Schleswig-Holstein normiert. Staatliche Organisationseinheiten mit ausschließlich fiskalischen Aufgaben sind nach der Definition keine Behörden [12]).

Topoi schließlich — der Lösungsvorschlag dieses Gutachtens ist im wesentlichen nach Topoi geordnet — sind Problem- oder Sachbereiche, die einer gesonderten rechtspolitischen Betrachtung bedürfen. Sachlich handelt es sich dabei (im öffentlichen Bereich) um die Phasen des Informationsverarbeitungsprozesses, (im privaten Bereich) unter Berücksichtigung der Interessen der Beteiligten.

[10]) vgl. Szypersyki. Sp. 1513 f. — gilt allgemein —
[11]) statt aller Wolff (2), 65
[12]) so aber eine Mindermeinung, z. B. Forsthoff (1), 415

Teil B

Allgemeiner Teil des Datenschutzrechtes (Individualdatenschutz)

B. Allgemeiner Teil des Datenschutzes im engeren Sinne (Individualdatenschutz)

Der Datenschutz umfaßt den Schutz vor Gefahren aus der öffentlichen wie der privaten Verwaltung. Bedroht ist vor allem der einzelne in seiner „Privatsphäre"; analoges gilt für Personenmehrheiten.

Dieser Bereich ist umfaßt vom Datenschutz i. e. S., dem hier sog. Privatdatenschutz (in diesem Teil B des Gutachtens kurz „DSch" bzw. „DSchRecht" genannt).

Die Gefahren und die Schutzobjekte sind im wesentlichen dieselben, gleichgültig, ob die Bedrohung von öffentlicher oder privater IV ausgeht: stets droht der Einbruch in den Autonomiebereich der Person(enmehrheit).

Es ist darum sachlich gerechtfertigt, dem DSchRecht i. e. S. einen „allgemeinen Teil" voranzustellen, der die den beiden Sachbereichen gemeinsame Problematik erörtert. Dabei zeigt sich, daß der bisherige Ausgangspunkt der wissenschaftlichen Diskussion von der „Privatsphäre" unbrauchbar ist (I). Vielmehr kann eine Regelung des DSch's nur dort anknüpfen, wo auch die Gefährdung ihre reale Grundlage hat: an der Information und ihrer Verarbeitung (II). Sodann ist nach öffentlicher und privater IV zu differenzieren (III).

I. Die unbrauchbare „Privatsphäre"

Bei der Beschreibung der „Privatsphäre" führt die Erörterung der bisherigen Definitionsversuche zu dem Facit, daß angesichts der tatsächlichen und rechtlichen Gegebenheiten (2.) die vorhandenen Ansätze in der Literatur angesichts der Realität der „Privatsphäre" (3.2) für eine befriedigende Bestimmung des Regelungsobjekts nicht ausreichen (3.); die „Privatsphäre" hat ausgedient (4.). Auch der Versuch, sie durch andere Begriffe zu ersetzen (5.), ist zum Scheitern verurteilt.

1. Was ist „Privatsphäre"

Der dem Gutachten zugrunde liegende Sachplan erfordert eine allgemeine Erörterung des sog. „privacy"-Bereichs. Dieser Gegenstand sei hier zunächst folgendermaßen umschrieben: Der „privacy"-Bereich sei ein Feld, innerhalb dessen der Bürger Entscheidungen in eigener Verantwortung fällen kann und das gegen Einbrüche von staatlicher wie von privater Seite zu schützen ist. Dabei soll schon hier bemerkt werden, daß der einzelne sowohl allein als auch in und mit gesellschaftlichen Gruppierungen entscheidet und der Bereich der „privacy" somit beide Möglichkeiten umfaßt. Er soll im folgenden mit dem Wort „Privatsphäre" bezeichnet werden [1]).

[1]) Die Verwendung dieses Wortes in Anführungszeichen soll darauf hinweisen, daß es sich dabei nicht um eine inhaltliche Aussage, sondern nur um eine Benennung handelt. Die vorstehende inhaltliche Bestimmung weicht weitgehend von der bisher allgemeinen Bedeutung von Privatsphäre (vgl. z. B. Hubmann (1), 269) ab.

2. Gegebenheiten

Die Klärung dieses Schutzbereichs geht zunächst von einer Ist-Analyse der tatsächlichen und rechtlichen Gegebenheiten aus. Es folgt ein kurzer Abschnitt über die Schwierigkeiten dieser Erörterung. Anschließend werden in einer zweiten Ist-Analyse abstrakte, positive Umschreibungsversuche der „Privatsphäre" vorgestellt und kurz bewertet. Anschließend geschieht dasselbe mit kasuistischen Bestimmungsversuchen. Es folgt die Darstellung der bisher angestellten Versuche über die Bestimmung einzelner Schutzbereiche; die Bestimmung der Grenzen und der Verletzungsformen der „Privatsphäre" schließt sich an. Dann werden die gefundenen Möglichkeiten im Hinblick auf ihre Verwendbarkeit für ein Datenschutzgesetz untersucht. Die Bestimmung der sog. „Topoi" kann — per definitionem — erst bei der Behandlung konkreter rechtlicher Interessenlagen erfolgen.

2.1. Tatschächliche Gegebenheiten

Auch bisher hat es Stellen privater oder öffentlicher Art gegeben, die Informationen über Personen (hier im untechnischen Sinn gebraucht) erfaßt, gespeichert und verwertet haben. Die bei diesen Stellen angelegten Karteien erlaubten es jedoch nicht, ein umfassendes, aus vielen Einzeldaten zusammengesetztes Bild einer Person zu erhalten. Die physischen, technischen und organisatorischen Gegebenheiten ließen dies nicht zu.

Diese Lage hat sich mit Einführung der EDV grundlegend gewandelt: Jetzt wurden die technischen und organisatorischen Voraussetzungen für einen umfassenden Datenaustausch geschaffen; der Bürger muß damit rechnen, daß die von verschiedenen Stellen erfaßten Daten anderen Stellen zur Kenntnis gelangen, ohne daß er darauf Einfluß nehmen kann. Im Gegensatz zu den tatsächlichen Gegebenheiten, die für das Zugriffsrecht des Parlaments maßgebend sind, aktualisiert sich hier also das Problem im wesentlichen erst durch die Einführung der EDV.

Man muß für die Zukunft von Informationssystemen von Bund, Ländern und Gemeinden ausgehen, die untereinander und mit Informationssystemen der Wirtschaft verbunden sind und in denen Daten mit Hilfe der bald eingeführten Personenkennzeichen technisch von jeder Stelle abgerufen werden können. Auch ein Verbund privater und öffentlicher Informationssysteme erscheint nicht ausgeschlossen; mindestens ist ein Zugriff des Staates auf private Datenbanken nicht von der Hand zu weisen [2]). Auch der umgekehrte Fall ist denkbar. Die Verwaltung strebt durch die Benutzung der Informationssysteme Integration, Automation und Rationalisierung an [3]).

2.2. Rechtliche Gegebenheiten

Diese tatsächliche Lage wurde bisher durch folgende Normen geregelt:

2.2.1. Öffentliches Recht

Das Verfassungsrecht hat einen Bereich des Privaten weitgehend anerkannt und ihn in den Grundrechten angesiedelt [4]), vgl. unten zum Grundrecht auf Information.

Der Gesetzgeber hat diese Vorstellungen in einzelnen Normen des Verwaltungsrechts konkretisiert, freilich nur im Hinblick auf sehr spezielle Sachverhalte:

§ 22 Abgabenordnung

§ 12 Bundesstatistikgesetz

§ 44 IV. Außenwirtschaftsgesetz

§ 9 Kreditwesengesetz

§ 9 Lebensmittelgesetz [5]).

---

[2]) vgl. die Bemühungen der interministeriellen Arbeitsgruppe; weiter einen Brief der Firma Schimmelpfeng: Auch Behörden könnten zugreifen, falls sie abonniert sind.

[3]) vgl. Artikel 1 Bay. EDVG und Begründung I 1 zum EDVG von Baden-Württemberg.

[4]) vgl. BVerfGE DÖV 70, 204 und DÖV 69, 749; Maunz-Dürig-Herzog Artikel 1 R. 31; Evers, 38 ff.

[5]) Instruktive Aufzählung bei Düwel, 99 FN. 2; vgl. auch 97 FN. 1.

[6]) vgl. Kamlah (2), 361 ff.

[7]) vgl. Kamlah, a. a. O.

[8]) vgl. von Mangoldt-Klein, Artikel 35 Anm. V 5

[9]) Preuß. OVG 20, 448 und OLG Düsseldorf NJW 57, 1037

[10]) vgl. aber Begründung zum Bay. EDVG Artikel 14

[11]) vgl. aber § 182 des Entwurfs von 1962

Hierher zählen auch die sonstigen zahlreichen Geheimnisschutzvorschriften und Aussageverweigerungsrechte.

Vergleicht man diese Rechtslage mit dem Ausgangssachverhalt, so ergibt sich:

— Der Ausgangssachverhalt läßt den Schluß zu, daß der Faktor Information — und besonders Informationen über Personen — innerhalb der Verwaltung einen neuen, bisher unerkannten Stellenwert besitzt. Die Information rückt als solche in den rechtlichen Bereich [6]). Die angeführten Normen lösen diese generelle Frage nur für ihren Aufgabenbereich und sind deshalb nur hier brauchbar.

— Das BVerfG hat das Problem der rechtlichen Bewertung des Informationsfaktors erkannt. Da seine Beurteilungskriterien jedoch weitgehend zu unbestimmt sind [7]), ist ein klarer Lösungsansatz nicht in Sicht.

— Der Austausch von Informationen zwischen Behörden wird durch das Institut der Amtshilfe geregelt (Artikel 35 Abs. 1 GG). Für dieses Institut sind noch keine einheitlichen Rechtsgrundsätze entwickelt worden [8]). Klarheit scheint lediglich insoweit zu herrschen, als die ersuchte Behörde zu prüfen hat,

— — ob sie zur Vornahme von Amtshandlungen der ersuchten Art allgemein befugt ist,

— — ob die ersuchende Behörde eine Hilfeleistung dieser Art im allgemeinen beanspruchen kann [9]).

Daß bei dieser Prüfung der Gesichtspunkt einer möglichen Verletzung der „Privatsphäre" zu berücksichtigen ist, ist zum mindesten bestritten [10]).

2.2.2. Strafrecht

Da eine Generalnorm, die die allgemeine Pönalisierung der Verletzung der „Privatsphäre" zum Gegenstand hat, nicht existiert [11]), enthält das StGB nur einzelne Vorschriften, die Teile dieses Bereichs mit einzelnen Verletzungsformen verbinden:

§ 298 StGB

Geschützt wird hier die „Unbefangenheit des Wortes" (Gallwas), also das nichtöffentlich gesprochene Wort. Verletzungstatbestände sind die Aufnahme auf Tonträger, Gebrauchen oder Weitergabe an einen Dritten, Abhören.

§ 299 StGB

Geschützt wird das geschriebene Wort; Verletzungshandlung ist das unbefugte Öffnen des Briefverschlusses.

§ 300 StGB

Geschützt wird die Information aus dem Intimbereich einer Person, die jemand aufgrund seiner Berufsstellung erlangt. Verletzungshandlung ist die Weitergabe.

§§ 353 b, 353 c StGB

Geschützt wird primär das Vertrauen der Bevölkerung in die Verschwiegenheit staatlicher Stellen, sekundär aber auch die Privatinformation selbst [12]). Verletzungshandlung ist der Bruch von Dienstgeheimnissen und Geheimhaltungsvorschriften.

§§ 354, 355 StGB

Hier gilt das zuletzt Gesagte für den Bereich der Post.

Vergleicht man diese Rechtslage mit dem Ausgangssachverhalt, so ergibt sich:

— Der Bereich des Persönlichen umfaßt mehr Aspekte als die derzeit strafrechtlich erfaßten. Ein Ausweg für eine lückenlose Erfassung wäre entweder eine Generalnorm (hierbei wäre eine klare Subsumtion kaum gewährleistet; außerdem bestünden Bedenken, ob der Tatbestand konkret genug gefaßt ist) oder eine kasuistische Aufzählung (diese ist kaum zu leisten).

— Die relativ genau umschriebenen Verletzungshandlungen können den neu auftretenden Tatbeständen nicht gerecht werden. Beispielsweise ist das rechtswidrige Verfälschen oder Löschen von Daten nicht erfaßt.

2.2.3. Zivilrecht

Hier hat sich — besonders nach Verkündung des Grundgesetzes — das Institut des allgemeinen Persönlichkeitsrechtes als „sonstiges Recht" i. S. des § 823 Abs. 1 BGB herausgebildet [13]). Mangels einer allgemeinen Umschreibung haben sich Fallgruppen gebildet, die bestimmte Aspekte der Persönlichkeit im Zusammenhang mit einer Verletzungsform regeln [14]). Abgesehen davon, daß neue derartige Fallgruppen auftauchen können und die Aufzählung insoweit unvollständig wäre, ist in diesem Zusammenhang wichtiger, daß eine Verletzung nur in Verbindung mit einem Schaden rechtlich relevant wird. Schäden an der Persönlichkeit sind immaterielle Schäden, die nach § 253 BGB nur ausnahmsweise ersetzt werden (§ 847, § 1300 BGB). Die Rechtsprechung entgeht dieser Folge, indem sie bei Nicht-Ausreichen oder Unmöglichkeit der Naturalrestitution entgegen § 253 einen Geldersatz zuspricht [15]). Für diese Durchbrechung des § 253 sind allerdings keine klaren Prinzipien erkennbar [16]).

Vergleicht man diese Rechtslage mit dem Ausgangssachverhalt, so ergibt sich:

— Da ein Schaden Voraussetzung für einen Anspruch nach § 823 I ist, sich aber Persönlichkeitsschäden nur schwer feststellen lassen, ist das Schadensrecht nur ein unvollkommenes Regulativ.

— Da die Voraussetzungen für eine Durchbrechung des § 253 zu ungeklärt sind, um voraussehbare Regelungen abzugeben, kann von einer gesicherten Rechtslage gerade angesichts der neuen Sachverhalte keine Rede sein.

— Die Technik der Herausbildung von Fallgruppen bedarf längerer Zeit. Dies bedeutet ein Zurückfallen hinter die Schnelligkeit der technischen Entwicklung, was sich das Recht angesichts der gesteigerten Gefährdung der von ihm zu schützenden Rechtsgüter nicht mehr leisten kann.

2.2.4. Ergebnis

Der Vergleich der Rechtslage mit den zugrunde gelegten, tatsächlichen Verhältnissen ergibt eine weitgehende Diskrepanz, eine Unfähigkeit des bisherigen Rechts, mit seinen gegenwärtigen Mitteln auf den neuen Sachverhalt zu reagieren. Geht man von einer Schutzwürdigkeit der „Privatsphäre" aus, so ist ein Schutz mit den vorhandenen Möglichkeiten nicht zu garantieren; neue rechtliche Mittel bzw. eine Erweiterung der vorhandenen Mittel müssen an ihre Stelle treten. Ihre Bereitstellung kann nicht — oder nur teilweise — durch die Justiz geschehen, da sie wegen ihrer nachträglich korrigierenden Arbeitsweise nicht in der Lage ist, neu entstandene technischen Sachverhalte rasch in den Griff zu bekommen. Es handelt sich also um eine Aufgabe für den Gesetzgeber. Freilich ist die Aufgabe nicht leicht, wie ein Blick auf die bisherigen Versuche zeigt, den Schutzbereich „Privatsphäre" positiv zu bestimmen.

3. Ansätze zur positiven Bestimmung der „Privatsphäre" in der Literatur

Die rechtswissenschaftliche Literatur wählt verschiedene Wege, um das Rechtsgut zu bestimmen. Sie geht entweder von abstrakt-generellen Umschreibungen aus oder versucht, eine Kasuistik aufzustellen.

3.1. Generelle Bestimmungen

3.1.1. Im deutschen Recht

Der durch das zivilrechtliche Institut des *allgemeinen Persönlichkeitsrechts* abgedeckte Bereich wird vom BGH so umschrieben:

Gegenstand sei „jener innere Persönlichkeitsbereich, der grundsätzlich nur der freien und eigenverantwortlichen Selbstbestimmung des einzelnen untersteht und dessen Verletzung dadurch gekennzeichnet ist, daß sie in erster Linie sogenannte immaterielle Schäden, die sich in einer Persönlichkeitsminderung ausdrücken, erzeugt" [17]).

Öffentlich-rechtlich wird etwa folgendermaßen argumentiert: Gegenstand sei „die ureigenste *Intimsphäre*, die sich allen staatlichen, totalen Inquisitio-

---

[12]) so Dreher, M., § 353 b Nr. 1

[13]) Ob dies mit einer unmittelbaren Drittwirkung von Artikel 1 und Artikel 2 Abs. 1 GG (so die Rechtsprechung seit BGHZ 13, 334) oder mit einer Analogie zu „Leben, Körper, Gesundheit, Freiheit" in § 823 I BGB konstruiert wird (vgl. Medicus, 243), ist unerheblich. Die Frage der Drittwirkung ist also in diesem Zusammenhang für das Ergebnis unwichtig.

[14]) vgl. Erman - Weitnauer, Anhang zu § 12 Nr. 8

[15]) so erstmalig BGHZ 26, 349 ff. (Herrenreiter - Urteil)

[16]) vgl. Medicus, 244

[17]) BGHZ 26, 349

nen, Registrierungen und Tests wirksam entgegenstellt" [18]).

3.1.2. Im amerikanischen Recht (USA)

Da das nordamerikanische Recht den Unterschied zwischen privatem und öffentlichem Recht nicht in unserem Sinne kennt, sind seine Bestimmungsversuche von allgemeiner Bedeutung. Das *„Right of Privacy"* wird etwa bestimmt als das Recht des einzelnen, zu bestimmen, inwieweit eigene Gedanken und Gefühle anderen mitgeteilt werden sollen *(the right to share and to withbold* [19]). Eine andere Definition spricht vom Recht des Fürsichseins [20]), dem „right to be let alone" [21]).

3.2. Relativität der Privatsphäre

Alle genannten Versuche haben gemeinsam, daß sie offenbar davon ausgehen, die jeweilige abstrakte Umschreibung ermögliche es, die „Privatsphäre" genau zu umgrenzen und somit Verletzungen scharf feststellen zu können. *Das ist bisher nicht gelungen.* Der BGH erklärt nicht, wann eine Persönlichkeitsminderung vorliegt; Maunz-Dürig unterlassen eine griffige Bestimmung der Intimsphäre; die amerikanische Literatur verzichtet offenbar auf eine Erklärung, was unter eigene Gedanken und Gefühle fällt und welche Bereiche der Persönlichkeit dem „Fürsichsein" zuzuordnen sind. Kurz: Keiner dieser Versuche erlaubt eine klare Subsumtion des Sachverhaltes. Da aber gerade dies die Voraussetzung jeder praktikablen rechtlichen Regelung ist, ist bisher eine allgemeine begriffliche Klärung des Problemfeldes nicht möglich.

Für das Scheitern dieser — und wohl aller gleichartigen — Versuche lassen sich drei Gründe anführen:

Zunächst kann man davon ausgehen, daß die Beurteilung des Persönlichkeitswertes Inhalt des allgemeinen Bewußtseins ist [22]). Dieses Bewußtsein ist abhängig von Ort und Zeit; es ändert sich im Lauf der Geschichte besonders stark und schneller als andere zentrale Rechtsbegriffe. Daher ist eine positive Umschreibung problematisch, weil sie eine möglicherweise sehr kurzlebige, relative Ansicht verewigen würde.

Sodann ist das Verständnis von „Privatsphäre" aber nicht nur relativ zu Zeit und Ort, sondern auch zu seinen Trägern: Was A zu seiner „Privatsphäre" zählt, muß B noch lange nicht dazuzählen und umgekehrt. Was aber A gegenüber C offenbaren will, das will B unter Umständen C gegenüber geheimhalten und umgekehrt. Relativität der „Privatsphäre" heißt also: „Privatsphäre" gegenüber wem? Darum gilt *der Grundsatz der Relativität der „Privatsphäre"*, und daraus folgt die *Unmöglichkeit ihrer Definition.*

Es müssen also alle Versuche einer abstrakten Umschreibung aus logischen Gründen scheitern, da sie allen Trägern von „Privatsphäre" denselben Umfang ihres persönlichen Bereiches zuweisen würden, der der Wirklichkeit nicht entspricht. Entscheidend ist also, *wem gegenüber* die „Privatsphäre" zu wirken hat [23]). Diese Erkenntnis bedeutet ein Abgehen von der semantischen und ein Einbezug der pragmatischen Informationsebene in die „Privatsphäre" (Beziehungen zwischen den Informationen und ihren Erzeugern bzw. Benutzern [24]). Von dieser Problemverlagerung aus soll später die Bildung der Topoi versucht werden.

Schließlich mag die eigentümliche Unbestimmbarkeit der „Privatsphäre" damit zusammenhängen, daß ihre Schutzwürdigkeit in der Regel erst beurteilt werden kann, wenn sie bereits verletzt ist [25]). Eine Subsumtion, die ja den Tatbestand einer Verletzung erst erweisen soll, erscheint somit kaum zu bewerkstelligen. Nun könnte man versuchen, diese „Leerformel" durch allgemeine Gesichtspunkte aufzufüllen. Dafür kommt zunächst in Betracht: ein evtl. vorhandenes *allgemeines Vorverständnis von „Privatsphäre".*

Da dies davon abhängt, was jeder kraft seines Eigenverständnisses in seine „Privatsphäre" einbezieht, die Eigenverständnisse jedoch differieren, ist nur auf der unteren Ebene eines gemeinsamen, gesellschaftlich bedingten, von jeder Individualisierung abstrahierten Verständnisses eine Einigung zu erzielen. Unter diesem minimalistischen Gesichtspunkt des kleinsten gemeinsamen Nenners ist bisher der Strafgesetzgeber tätig geworden.

Der Nachteil dieses Gesichtspunktes ist, daß er oberhalb dieser Ebene nichts aussagt. Beispielsweise dürfte eine Umfrage über Urlaubsziele nicht jedermann als Verletzung seiner „Privatsphäre" betrachten [26]).

Auch existiert keine Norm, die in der Lage wäre, den Begriff mit Inhalt zu erfüllen. Die literarischen Verweisungen auf Artikel 1 oder Artikel 2 Abs. 1 GG sind dazu ungeeignet; sie bewirken nur eine Verlagerung des Problems auf die Umschreibung von Menschenwürde und allgemeinem Freiheitsrecht.

Somit verbliebe nur noch die Ausfüllung durch Hoheitsakt. Danach müßten Judikative oder Legislative für alle verbindlich eine Ausfüllung vornehmen. Doch sind gerade die Grundsätze, nach denen das zu geschehen hätte, noch nicht erarbeitet.

Selbst wenn es also gelänge, die oben angedeuteten Schwierigkeiten zu umgehen, müßte dieses Vorhaben aus logischen Gründen scheitern [27]) [28]).

---

[18]) Maunz-Dürig-Herzog, Artikel 1 N. 37
[19]) zitiert nach Kamlah (1), 97, der sich auf Warren und Brandeis bezieht
[20]) so eine deutsche Übersetzung von Evers, 7
[21]) zitiert nach Kamlah (1), 57
[22]) vgl. Hubmann, (1), 142
[23]) vgl. Kamlah, (2), 362
[24]) vgl. Steinmüller (1), 8
[25]) Evers, 43
[26]) vgl. aber BVerfGE 27, 1
[27]) vgl. Evers, 16
[28]) vgl. Podlech (2), 185 ff.

3.3. Kasuistische Bestimmungsversuche

3.3.1.

Einzelerfassung aller in Betracht kommenden Sachverhalte [29]). In Gesetzen gibt es sie im wesentlichen in zweifacher Form: Entweder handelt es sich um eine abschließende Aufzählung bestimmter Sachverhalte, oder es handelt sich um eine Aufzählung mit vorgeschalteter Generalklausel (die Aufzählung wird dann oft mit „insbesondere" eingeleitet). Im ersteren Fall ist das Gesetz nicht in der Lage, von sich aus auf neue Sachverhalte zu reagieren (bzw. eine Ergänzung würde zu umständlich sein), im letzteren Fall würde die Ausfüllung der Generalklausel der Judikative überlassen bleiben müssen, die in langer Zeitdauer erst Kriterien dafür entwickeln müßte. Beides spricht gegen eine kasuistische Regelung.

Ein anderer Vorschlag [30]) hält es dennoch für denkbar, daß sich Sachverhalte aufzählen lassen, deren Verwirklichung unter allen Umständen schwere, unzumutbare Eingriffe darstellen, die somit niemals rechtmäßig sein können. Solche Sachverhalte sind beispielsweise Informationen aus dem Sexualleben einer Person oder über das Klima einer Ehe. Diese Sachverhalte zu finden, erscheint dann realisierbar, wenn man von der Existenz eines allgemein vorhandenen Vorverständnisses von „Privatsphäre" ausgeht [31]). Im Verhältnis Staat — Bürger sind jedoch Eingriffe selbst in diesen Bereich möglich und rechtmäßig (Gesundheitsverwaltung, Strafverfolgung). Daher ist der Vorschlag allenfalls im Verhältnis Bürger — Bürger relevant. Hier erscheint es denkbar, daß es keine überwiegenden Interessen eines anderen Privaten rechtfertigen, Informationen aus dem Bereich dieses Katalogs zu erfassen und zu verwerten. Dieser Katalog ist vielleicht in einer Umfrage am sichersten zu ermitteln. Doch wäre auch er unbrauchbar: auch hier gälte die Relativität der „Privatsphäre".

3.3.2.

Ein weiterer Vorschlag geht von der „Provokation einer Kasuistik" [32]) aus. Er nimmt an, daß eine gesetzliche Kasuistik nicht zu erstellen ist. Die Menge der auftretenden Fälle müsse dennoch rechtlich bewältigt werden; dies könnte dadurch geschehen, daß diese Fälle von vornherein in gesetzliche Bahnen gelenkt werden, deren Rechtmäßigkeit sich mittlerweile herausgestellt habe. Verwaltung und Wirtschaft würden so gezwungen („provoziert"), eine von vornherein rechtlich faßbare Kasuistik herauszubilden.

Hier liegt ein Zirkelschluß zugrunde: Wenn die Kasuistik gebildet und gelenkt werden soll, dann muß das, was gelenkt wird, vorher erfaßt sein. Aber gerade die zu lenkenden Fälle sind in ihrer Vielzahl und Vielschichtigkeit unbekannt. Eine Regelung geht daher das Risiko ein, daß die in Unkenntnis des zu regelnden Problems statuierten Bahnen möglicherweise neben den regelungsbedürftigen Fällen liegen. Selbst wenn dies gelänge, wäre eine ständige, kurzfristige Optimierung des Gesetzes erforderlich (nämlich immer dann, wenn man glaubt, eine neue Fallgruppe erkannt zu haben); dies ist mit dem herkömmlichen Gesetzgebungsverfahren wohl nur schwer zu leisten. *Als Grund für ein Scheitern aller kasuistischen Versuche* muß auch hier wieder die Relativität der „Privatsphäre" genannt werden. Lediglich die unzulängliche Aufzählung von Sachverhalten, die — einem allgemein vorhandenen Vorverständnis von „Privatsphäre" entsprechend — mit Sicherheit Verletzungen der „Privatsphäre" bedeuten (die also insoweit nicht relativ sind!) ist hier als Ausnahme zu nennen.

3.4. Festlegen von Schutzbereichen

Als letzter inhaltlicher Bestimmungsversuch folgt jetzt noch das Festlegen von Schutzbereichen, d. h., die Aufspaltung der Persönlichkeit als ganzer in „Persönlichkeitsteile" [33]), die jeweils mit einem mehr oder weniger generalisierenden Begriff bezeichnet werden.

3.4.1. Im deutschen Zivilrecht

Im Anschluß an die von der Rechtsprechung herausgebildeten Fallgruppen [34]) werden diese als Schutzbereiche bereits feststehenden Inhalts bezeichnet. Für den noch nicht erfaßten Teil gilt der Grundsatz der Interessenabwägung. Besser erscheint die Bildung einander überschneidender anderer Schutzbereiche, wie sie Hubmann [35]) vorschlägt. Er unterteilt in:

— Das Recht auf Entfaltung der Persönlichkeit;

— Das Recht an der Persönlichkeit;

— Das Recht auf Individualität

und ordnet jedem Bereich eine Vielzahl von Einzeltatbeständen zu.

3.4.2. Im amerikanischen Recht

Kamlah [36]) unterscheidet hier folgende Schutzbereiche:

— Identitätsmerkmale;

— räumlicher Schutzbereich;

— private Daten und Tatsachen;

— psychische Phasen der Persönlichkeit.

Diese Unterteilung ist orientiert an bisher anerkannten Schutzbereichen. Fraglich ist jedoch die Vollständigkeit dieser Systematik.

---

[29]) vertreten von Dr. Beermann, MdB, in KEDV-Drucksache 14, 15

[30]) vertreten von Dr. Beermann, MdB, a. a. O., 19

[31]) vgl. oben 3.2.

[32]) Kamlah (3), 21. f.

[33]) vgl. Kamlah (1), 81

[34]) Namensschutz, Bildnisschutz, Schutz des gesprochenen Wortes, Zivilrechtlicher Ehrenschutz, Schutz des Privat- und Familienlebens, Briefe und Tagebücher, Persönlichkeitsschutz und Film, Urheberpersönlichkeitsrecht, Leben — Körper — Gesundheit — Freiheit; vgl. Erman - Weitnauer, Anhang zu § 12 Anm. 8!

[35]) Hubmann, 175 ff.

[36]) Kamlah (1), 82 ff.

3.4.3. Beurteilung

So unsicher es ist, ob diese Aufteilungsversuche etwas für eine normative Regelung hergeben, so bringen sie doch schon jetzt eine wichtige Einsicht:

In diese Schutzbereiche wird dauernd von privater oder staatlicher Seite aus eingegriffen. Manche Eingriffe werden als rechtmäßig, manche als rechtswidrig betrachtet. Damit ist die Verletzung des Tatbestandes allein nicht das entscheidende Indiz für eine Rechtsverletzung. Entscheidend ist vielmehr, ob für den Eingriff ein Rechtsgrund vorliegt oder nicht. Damit verschiebt sich das Problem grundlegend:

Gesucht werden in erster Linie nicht perfekte Tatbestandsabgrenzungen, sondern Rechtsgründe, die den Eingriff erlauben [37]). Für den weiteren Gang der Untersuchung ist diese Erkenntnis von ausschlaggebender Bedeutung. Gelingt es nämlich, diese Rechtsgründe präzis genug zu umreißen, dann ist damit ein großer Teil des Fragenbereichs erfaßt.

4. Ende der „Privatsphäre"

Die Möglichkeiten positiver Umschreibung des Inhalts der „Privatsphäre" sind damit erschöpft. Als Ergebnis steht fest: Eine positive Inhaltsbestimmung ist wegen der Relativität der „Privatsphäre" unmöglich. Nur eine minimalistische Einigung auf den „kleinsten gemeinsamen Nenner" ist theoretisch möglich, praktisch aber unbrauchbar, da die rechtspolitischen Erfordernisse eine umfassende Regelung verlangen. Übrig bleibt in diesem Zusammenhang noch, eine präzisere Beschreibung des Gemeinten durch andere Begriffe zu finden. Auch dieser Versuch schlägt fehl:

5. Ersetzung der „Privatsphäre" durch andere Termini:

Aus der Einsicht in die Relativität der „Privatsphäre" ziehen einige Autoren die Folgerung, diesen vagen Begriff durch einen weniger verschwommenen zu ersetzen. Hierfür bieten sich an: die „Privatheit", die „Erheblichkeit" und die „Identifizierbarkeit".

---

[37]) In Erkenntnis dieser Tatsache bestimmt Evers seine Schutzbereiche nach ihrer Geschütztheit vor Eingriffen.
[38]) vgl. Kamlah (1), 145 ff.
[39]) BVerfG DÖV 70, 204
[40]) Kamlah (2), 362
[41]) es taucht im EDV-Recht auch nirgends auf
[42]) vgl. Kamlah (1), 160 ff.
[43]) vgl. Kamlah, a. a. O.
[44]) Die zivilrechtliche Ausrichtung dieser Grenze macht ihre allgemeine Verwendbarkeit fraglich. Unter diesem Gesichtspunkt muß auch der allgemein-rechtliche Stellenwert des Buches von R. Kamlah betrachtet werden.
[45]) vgl. aber RGZ 80, 221: Sittenwidrig ist, was dem Rechtsgefühl aller billig und gerecht Denkenden widerspricht.

5.1. Privatheit [38])

Der Gegenbegriff zur Privatheit ist die Öffentlichkeit. Eine Verletzung der „Privatsphäre" liege nur dann vor, wenn die benutzten Informationen *nicht im Bereich der Öffentlichkeit* liegen. Um dies festzustellen, ist eine Begriffsbestimmung von „Öffentlichkeit" erforderlich. Das BVerfG [39]) versucht dies in diesem Zusammenhang folgendermaßen:

Öffentlich sei, was der Außenwelt zugänglich ist, zugänglich, was sich ohne Befragen der betroffenen Person über sie feststellen läßt.

Es ist von Kamlah [40]) treffend darauf hingewiesen worden, daß auch eine Verletzung der „Privatsphäre" in diesem so zugänglichen Bereich möglich ist. Das Kriterium ist somit unbrauchbar [41]).

Zudem läßt sich nicht generell festlegen, wann Öffentlichkeit vorliegt und wann nicht. Beispielsweise kann nicht gesagt werden, bei welcher Anzahl von kenntnisnehmenden Personen die Öffentlichkeitsgrenze erreicht ist. Vielmehr kommt es darauf an, ob der Betroffene von einer Öffentlichkeit ausgeht oder nicht; damit ist aber die Öffentlichkeit relativ zum Betroffenen. Diese Relativität bewirkt ihre Untauglichkeit als Grenzbestimmung.

Außerdem bringt die Gegenüberstellung der Begriffe Privatheit — Öffentlichkeit eine Gefahr mit sich: Begreift man Öffentlichkeit als demokratischen Funktionsträger und ordnet den Begriff somit dem Bereich staatlichen Funktionierens zu, so ließe sich Privatheit als der staatsfreie Bezirk festlegen. Der hier beschriebene Zustand wäre der des klassischen, vom liberalen Staatsmodell ausgehenden status negativus. Setzt man voraus, daß heute nicht mehr Abwehr des Staates, sondern Teilnahme am Staat das Problem ist, so fragt es sich, ob sich der bisherige Begriff der „Privatsphäre" zweckmäßigerweise überhaupt noch verwenden läßt.

5.2. Erheblichkeit [42])

Eine Verletzung der „Privatsphäre" liege nur vor, wenn die benutzte personenbezogene Information von „Erheblichkeit" für den Betroffenen ist. Erheblich sei das, was eine Person mit durchschnittlicher Empfindsamkeit als verletzend ansieht [43]). Die Erheblichkeitsschwelle hängt damit von Zeit, Ort und Person ab. Für sie gilt also das gleiche wie zur „Privatsphäre". Die Feststellung der Verletzung ist gleichbedeutend mit der Feststellung einer „Persönlichkeitsminderung" (BGH) und damit einer Einordnung in das Feld des Schadensersatzrechtes [44]). Die hier beschriebene Art und Weise der Feststellung ist dem deutschen Schadensersatzrecht jedoch fremd [45]); sie stellt nach unserer Ansicht einen bedenkenswerten Ansatz dar. Mit seiner Hilfe ist es möglich, die zeitlich und örtlich bedingten Schwankungen der Ausfüllung der „Privatsphäre" aufzufangen.

Die Erheblichkeit, verstanden als Sensibilitätsschwelle des Durchschnittsmenschen hinsichtlich Verletzungen seiner sog. Privatsphäre, wäre nur dann eine taugliche begriffliche Grenze, wenn sie

auch tatsächlich für alle Menschen verbindlich festgelegt werden könnte. Dies ist jedoch generell nicht durchzuführen: selbst so unerheblich scheinende Informationen wie Name und Wohnort können in gewissen Fällen bei der Weitergabe an bestimmte Stellen für den Betroffenen erheblich sein. Als Beispiel folgender Fall: Der Kriminaldirektor einer westdeutschen Stadt soll angeblich einem von der Kriminalpolizei Beschuldigten die Privatadresse des gegen ihn ermittelnden Beamten in der Annahme mitgeteilt haben, der Beamte solle wohl ein „Geschenk" erhalten. Der Beamte fühlte sich darauf in seiner „Privatsphäre" verletzt [46]).

Mit anderen Worten: Auch die Erheblichkeit entzieht sich nicht ihrer Relativierung durch den Betroffenen. Diese Relativität bewirkt ihre Untauglichkeit als Grenzbestimmung.

5.3. Identifizierbarkeit

Eine Verletzung der „Privatsphäre" liege nur dann vor, wenn die benutzte Information einen Schluß auf die betroffene Person zuläßt [47]), wenn diese Person dadurch identifizierbar wird [48]). Damit scheint eine Abgrenzung zu rein statistischen Daten getroffen, die in ihrer Pauschalierung im Endstadium der Aufbereitung keine Rückschlüsse mehr auf Einzelpersonen zulassen. Eine Verletzung bei der Erfassung soll durch § 12 des Bundesstatistikgesetzes verhindert werden, diese Grenzbestimmung erscheint zunächst einleuchtend: Ist kein Schluß auf eine Einzelperson möglich, dann kann die „Privatsphäre" nicht verletzt sein. Allerdings gilt die Umkehrung des Satzes nicht: Ist ein Schluß auf eine Einzelperson möglich, so ist damit noch nicht gesagt, daß ihre „Privatsphäre" verletzt ist. Die Identifizierbarkeit als Abgrenzungskriterium ist nicht überzubewerten [49]). Sie ist notwendiges aber keineswegs hinreichendes Merkmal.

Zudem zeigt die Berücksichtigung der technischen Möglichkeiten der modernen Informationsverarbeitung, daß sogar die zunächst so einleuchtende Abgrenzung zwischen „identifizierenden" und statistischen Informationen relativ ist [50]): Sie ist relativ zum jeweiligen IS, und nur insoweit ist dieses Kriterium brauchbar. Dies setzt aber die Berücksichtigung dieser technischen Gegebenheiten voraus, was auf dem bisher beschrittenen Weg nicht möglich ist.

Damit haben sich alle Kriterien und Umformulierungen der „Privatsphäre" als relativ, unbestimmbar und somit als unbrauchbar erwiesen. Das Reizwort „Privatsphäre" ist darum aus der wissenschaftlichen Diskussion des Datenschutzrechts auszuscheiden.

Es muß nach einem neuen Ansatz gesucht werden. Er besteht in der Anknüpfung an die Information und ihre Verarbeitung.

[46]) vgl. Frankfurter Rundschau vom 5. Februar 1971, S. 9

[47]) Kamlah (1), 155 ff.
Unklar ist den Verfassern jedoch, ob die Statistikwissenschaft nicht Methoden entwickelt hat, die Rückschlüsse auf Einzelpersonen in gewissem Umfang zulassen, selbst wenn die Urdaten gelöscht sind.

[48]) s. Kamlah (1), 147

[49]) Die Identifizierbarkeit taucht im EDV-Recht bereits auf: Hess. DatSchG (§ 5 III); CDU-Entwurf für Rheinland-Pfalz (§ 4 III), Begründung zu Artikel 14 des Bay. EDVG.

[50]) s. o.

II. Der neue Ansatz

Der bisherige Lösungsansatz der „Privatsphäre" ging aus von einem *Rechts*begriff, der, sofern er sich auf eine Realität bezog, mit dem rapiden „sozialen Wandel" in diesem Wirklichkeitsbereich nicht mehr fertig wurde. Der neue Ansatz knüpft an das Phänomen der Information und ihrer Verarbeitung an, also an einen *tatsächlichen* Prozeß; er geht also von einer (zugleich gesellschaftlichen wie „technischen") Realität aus.

Demgemäß sind, ehe die einzelnen Schritte des Informationsverarbeitungsprozesses näher bestimmt werden können, die einzelnen für den Datenschutz relevanten Arten der Information anzugeben (1.).

Die Einteilung der Informationen (1.1.) zeigt angesichts der Umwandelbarkeit der Informationsarten (1.2.) unter bestimmten Bedingungen (1.3.), daß die rechtliche Regelung nicht allein, wie bisher angenommen, an den Personeninformationen anknüpfen darf, sondern an den sog. Individualinformationen (1.4).

Diese Individualinformationen sind Gegenstand der für den DSch relevanten Informationsverarbeitung und ihrer einzelnen Phasen (2.), die für öffentliche wie private IV gleichermaßen gelten (3.).

1. Informationsarten

1.1. Grundeinteilung

1.1.1. Personen- und Sachinformationen

Informationen beziehen sich auf (eine oder mehrere) *Personen* oder/und (einen oder mehrere konkrete oder abstrakte) Sachverhalte; sie heißen dann *Personeninformationen, Sachinformationen* bzw. *gemischte Informationen.*

Zum Beispiel:

1. Hans Müller ist am 29. Mai 1924 geboren, oder: Bundeskanzler Brandt sagte in einem Interview:
2. Die Grundstücke an der Rheinstraße in Bonn sind durchschnittlich 2000 qm groß.

3. Hans Müller besitzt Grundstücke an der Rheinstraße in Bonn.

1.1.2. Individuelle und statistische Informationen

Die gemischte Information fällt aus der weiteren Betrachtung dieses Gutachtens heraus, da sie nach rechtlicher Betrachtungsweise entweder der Personen- oder Sachinformation zuzuordnen ist; für das DSchRecht ist sie überwiegend in ihrem Personenbezug relevant und darum bei der reinen Personeninformation ohne weitere Erwähnung mitbehandelt.

Diese Hauptarten von Information können sein:

1. individueller oder
2. statistischer Natur; also *individuelle* und *statistische Informationen;*

z. B. ist oben 1. Einzelinformation,
2. statistische Information.

Individuelle Informationen bezeichnen bestimmte Personen oder Sachverhalte, statistische dagegen Relationen und Eigenschaften von Personen- bzw. Sachverhaltsmehrheiten.

Demnach gibt es

1.1. individuelle Personeninformationen (z. B. oben 1.),

1.2. statistische Personeninformationen (z. B. „alle XY sind Volksschädlinge"),

2.1. individuelle Sachinformationen (z. B. das Grundstück in Bonn, Rheinstraße 20 ist 2000 qm groß),

2.2. statistische Sachinformationen (z. B. oben 2.)

1.1.3. Gruppeninformationen

Diese Einteilung wird dadurch kompliziert, daß der Schutzbereich des Privatdatenschutzes nicht nur den einzelnen, sondern und vor allem auch die schutzbedürftigen Gruppierungen (z. B. Minderheiten) umfaßt. Auf sie beziehen sich die (individuellen oder statistischen) *Gruppeninformationen.*

Z. B. „NPD-Mitglieder sind durchschnittlich 35 Jahre alt";

„Die XY-GmbH wird von Bankrotteuren geleitet";

‚Kriegsdienstverweigerer sind „links"'.

Gruppe in diesem Sinn ist jede identifizierbare Personenmehrheit die vor öffentlich oder privater IV rechtlich zu schützen ist [1]).

Ihrer Natur nach handelt es sich um *statistische* Informationen mit der Besonderheit, daß sie sich auf eine Mehrheit von Personen beziehen.

Rechtlich sind sie im wesentlichen den Individualinformationen gleichzubehandeln, sofern im folgenden nichts besonderes angeführt ist.

[1]) Strenger Maunz-Dürig-Herzog Artikel 9 Nr. 19: „Interessenbestimmter privater Zweckverband, dessen Gründung, Tätigkeit und Auflösung grundsätzlich der Disposition der Mitglieder" unterliegt.

1.1.4. Einbeziehung bestimmter statistischer Informationen

Unter Umständen können rein statistische Informationen schwer diffamierend sein, auch wenn sie nicht auf konkrete Einzelpersonen bezogen werden können.

Z. B. „Die Anwohner der Moselstraße sind zu 90 % syphilitisch", „DKP-Wähler", usf.

Es handelt sich dabei um nichts anderes als um Gruppeninformationen, mit der Besonderheit, daß sie ohne Zusatzinformationen nicht auf Einzelpersonen rückführbar sind, sie sind rechtlich den Individualinformationen gleichzustellen.

1.2. Umwandelbarkeit der Informationsarten: Das Problem der Zusatzinformation

Grundlage für die weitere Untersuchung ist die *Erkenntnis der Umwandelbarkeit aller Informationen.* Das soll für hier nur an den beiden wichtigsten Fällen begründet werden:

Sach- und statistische Informationen können nämlich durch geeignete *„Zusatzinformationen"* in personenbezogene Informationen umgewandelt werden.

Wenn etwa die Sachinformation lautet:

„Dieser Edelstein ist der größte der Welt" und die gemischte Personeninformation „X hat das PKZ NN",

sodann beide sinngemäß verknüpft werden, entsteht die personenbezogene Information:

„X hat das PKZ NN und ist Eigentümer des größten Edelsteins der Welt."

Oder etwa die statistische Information:

„Juden sind auszuweisen",

„Studenten stehen politisch links"

wird verknüpft mit der Personeninformation:

„X ist Jude",

„Y ist Student"

so entsteht die personenbezogene Information:

„X ist Jude und auszuweisen"

„Y ist Student und links".

Mit anderen Worten:

1.2.1. Personenbezogene Informationen

Jede Sachinformation kann syntaktisch mit Personeninformationen verknüpft werden:

Sie wird dadurch zur personenbezogenen Information umgewandelt

z. B. (2.1.) + (1.1.) = Hans Müller, geb. am ..... besitzt das 2000 qm große Grundstück in Bonn, Rheinstraße 20

(Alle gemischten Informationen — oben (3.) — sind dieser Art).

Da die Klasse der Personeninformationen Unterklasse der personenbezogenen Informationen ist, seien im folgenden Personen- und personbezogene Informationen allgemein als *„personenbezogene Informationen"* (pI) zusammengefaßt.

1.2.2. Individualisierbare Informationen

Jede statistische (auch Gruppen-) Information kann syntaktisch mit Einzelinformationen verknüpft werden.

Sie wird dadurch zur individualisierbaren Information umgewandelt.

z. B. (2.) + (1.1.) = Die Grundstücke gehören Hans Müller.

oder: (1.2.) + (1.1.) = Der Jude Hans Müller ist Volksschädling.

Da die Klasse der Einzelinformationen als Unterklasse der individualisierbaren Informationen aufgefaßt werden kann, seien beide zusammen im folgenden als „individualisierbare Informationen" (iI) bezeichnet.

Diese Umwandelbarkeit betrifft Personen- wie Sachinformationen gleichermaßen.

Es gibt demnach individuelle, individualisierbare und statische Person-, personenbezogene und Sachinformationen; also die Kombinationen 1.1, 1.2, 1.3; 2.1., 2.2., 2.3., 3.1., 3.2., 3.3. (vgl. Schaubild).

1.2.3. Individualinformationen

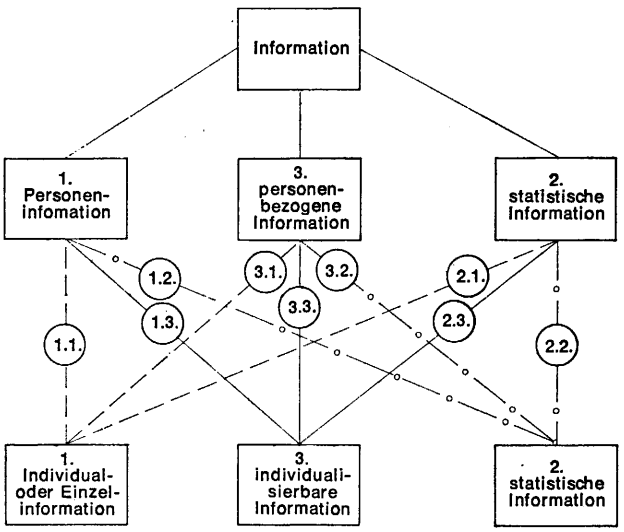
Besonders wichtig sind im folgenden die individualisierbaren, personenbezogenen Informationen (Kombination 3.3).

Für sie sind die Bezeichnung *„Indiviualinformationen"* festgelegt und als Rechtsbegriff vorgeschlagen.

Denn sie ist der Hauptschutzgegenstand des DSch-Rechts i. e. S.

Aus praktischen Gründen seien ihnen im folgenden auch ohne ausdrückliche Erwähnung die **Gruppeninformationen** gleichgestellt (einschl. der auf Gruppen beziehbaren sog. *„gruppenbezogenen" Informationen,* analog oben 1.2.1.).

Damit ergibt sich folgendes Schaubild:



1.3. Bedingungen der Umwandlung

Die tatsächliche Umwandelbarkeit hängt von der jeweiligen Struktur des IS ab.

Eine Umwandlung, die im einen IS möglich ist, ist im anderen unmöglich.

Die technischen Bedingungen hierzu sind — zugeschnitten auf den wichtigsten Fall, die EDV —:

- — genormte Daten (sie müssen zueinander passen),
- — geeignete hard- und software, bei Koppelung von IS Kompatibilität beider,
- — Einführung des Personenkennzeichens (PKZ), später entsprechend des Gruppen- und Sachkennzeichens,
- — spezielle Verknüpfungssoftware, die diese Datenverknüpfungen generell oder in Einzelfällen erlaubt,
- — organisatorische usw. Vorkehrungen zur Aktualisierung dieser vier Voraussetzungen.

Bei Kenntnis (Offenlegung) der Struktur eines IS ist in jedem Einzelfall eindeutig feststellbar, ob eine Individualinformation verarbeitet wird/wurde oder nicht.

1.4. Rechtliche Bedeutung

Die rechtlichen Konsequenzen sind entscheidend:

DSch i. e. S. kann nicht auf Personeninformationen allein beschränkt werden. *DSch bezieht sich* vielmehr *auf alle Individualinformationen.*

Gegenstand des DSch sind demnach grundsätzlich

1. alle Personeninformationen,
2. alle personenbezogenen Informationen,
3. alle individualisierbaren (statistischen Personen- oder personenbezogenen) Informationen,
4. alle Gruppen(-bezogenen) Informationen;

kurz: *die Individual- und Gruppeninformationen.*

Irrelevant sind demnach für den DSch alle übrigen Informationen:

1. alle reinen Sachinformationen,
2. alle rein statistischen Informationen (mit der oben 1.1.4. bezeichneten Ausnahme).

„Rein" sind sie dann, wenn sie nach der konkreten Organisation des IS, in dem sie gespeichert sind, nicht „umwandelbar", sind (oben 1.2., 1.3., d. h. nicht auf konkrete Personen(-gruppen) bezogen werden können.

Dies bedeutet für den Streitfall:

Der Bürger ist gegenüber den im allgemeinen schwer durchschaubaren IS in Beweisnot. Die Kenntnis der Struktur des IS ist dagegen dem Träger des IS bekannt.

Es spricht demnach die tatsächliche Vermutung für das Vorliegen einer Individualinformation.

Dem Träger des IS (dem Beklagten) obliegt es, diese Vermutung zu widerlegen.

Dieses zunächst anscheinend so schwierige Problem ist also prozessual ohne weiteres lösbar.

Freilich verlangt der Nachweis vom Richter einige Kenntnisse, die er sich aber — wie üblich — durch Sachverständige und vom zuständigen Kontrollorgan (s. u.) erbringen lassen kann.

2. Die Phasen der Informationsverarbeitung

Das bisherige Ergebnis lautet:

Der Begriff der Privatheit bzw. der Privatsphäre ist für das DSchRecht ungeeignet. Vielmehr ist an den Begriff der Information anzuknüpfen: Gegenstand des DSch sind nur Individualinformationen (einschl. der gruppenbezogenen Informationen). Sie sind in der Realität jeweils eindeutig bestimmbar.

Damit ist ein Ansatz gewonnen, der von einer sozialen Realität ausgeht. Er ist nun weiterführend zu konkretisieren.

Der „Faktor Information" als solcher ist irrelevant; erst die *Informationsverarbeitung* konstituiert die Information als Individualinformation; sie begründet darum die spezifischen Gefährdungen. Deshalb liegt hier der „Ort des Problems"; ihr wendet sich die weitere Untersuchung zu.

Dabei zeigt sich, daß die IV eine typische Struktur aufweist (Struktur verstanden als regelmäßige Wiederkehr gleicher Zustände des Prozesses der IV, 2.1.); sie zu bezeichnen bietet sich eine abgewandelte EDV-Terminologie an (2.2.); ihre einzelnen Phasen (2.3.) bilden die Grundlage der rechtlichen Regelungen: sie führen zu den gesuchten Problemkreisen, den „Topoi", der IV in der öffentlichen und privaten Verwaltung.

2.1. Die Struktur der IV

Verwandlung, gleich welcher Art, ist immer zugleich auch Informationsverarbeitung — was immer sie sonst noch sein mag. Formulierung eines Gesetzes, Erlaß eines Verwaltungsakts, Verkündung eines Urteils, polizeiliche Recherchen, Vorbereitung und Durchführung einer unternehmerischen Entscheidung — alle diese Handlungen enthalten IV irgendwelcher Art, auch wenn dabei kein Wort gesprochen wird. Auch wenn eine Ampel auf Grün schaltet oder der Lehrling einen Aktenberg wortlos auf den Schreibtisch seines Chefs häuft, wird Information verarbeitet, hier als Informationsveränderung (Ampel) bzw. Informationsaustausch (Akten).

Diese Informationsverarbeitung in öffentlicher und privater Verwaltung vollzieht sich in der Aufeinanderfolge von Schritten, Stadien oder Phasen. Diese Phasen können einzeln, in verschiedenen Kombinationen oder alle nacheinander auftreten. Die typische Folge der Schritte bildet den *Prozeß* der IV (Struktur der IV):

- — Informationsermittlung,
- — Informationserfassung,
- — Informationsspeicherung,
- — Informationsveränderung,
- — Informationsausgabe, insbesondere -weitergabe, -austausch, -verbund,
- — Informationslöschung.

Da diese Schritte bei jeder IV typisch wiederkehren (mögen auch gelegentlich einzelne Phasen ausfallen), haben sie grundlegende Bedeutung: in ihnen werden die Individualinformationen verarbeitet mit je spezifischen Auswirkungen und Gefährdungen für den Betroffenen.

2.2. Abgewandelte EDV-Terminologie

2.2.1. Unterschiede

Diese Bezeichnungen wurden bisher ausschließlich bei der EDV verwendet. Sie entstammen der Fachsprache der EDV (*Daten*verarbeitung), sind aber zu verallgemeinern und zu modifizieren auf jede Art der *Informations*verarbeitung.

Der Hauptunterschied zwischen der auf der syntaktischen Ebene verbleibenden EDV-Terminologie und der DSch-Begrifflichkeit ist die — aus rechtlichen Gründen erforderliche — *Einbeziehung der pragmatischen Ebene* (namentlich der Schutzrichtung in Richtung auf den Betroffenen); besonders deutlich wird dies etwa bei der Datenausgabe: sie ist technisch bloßer output (z. B. Schnelldrucker druckt aus); rechtlich dagegen umfaßt Informationsausgabe den output und das Merkmal der Zugänglichkeit für bestimmte Benutzer.

2.2.2. Bedeutung

Da die Kehrseite der IV der DSch ist, haben die Phasen der IV ebenso grundsätzliche Bedeutung für den Datenschutz: *Die Phasen der Informationsverarbeitung führen zu den Topoi,* den Problemkreisen und Schutzbereichen des DSchRechts. Denn die IV muß „begleitend" in allen Stadien des Prozesses auf mögliche Gefahren untersucht werden, soll der DSch umfassend und nicht lückenhaft sein.

Das ist bisher nicht erkannt und darum auch in den DSch-Regelungen der Länder noch nicht berücksichtigt worden. Die Stadien des IV-Prozesses sind die Grundlage dieser Untersuchung.

2.2.3. Legalterminologie

Die Zuordnung einer entsprechenden Terminologie ist nicht unproblematisch, da einige in Frage kommende Begriffe bereits durch die EDV-Gesetze der Länder festgelegt sind und nicht ohne Not abgeändert werden sollen:

Datenerfassung, -speicherung (HessDSchG § 3),

Datenaustausch (BayEDVG Artikel 4, 10 — Datenaustausch zwischen staatlichen/kommunalen und nichtstaatlichen Stellen),

Datenverbund (BayEDVG Artikel 7 — zwischen den EDVA und Datenbanken der Ministerien),

Datentransport (HessDSchG § 5),

Datenweitergabe (HessDSchG § 5),
-abruf (HessDSchG § 5),
-veröffentlichung (HessDSchG § 5),
-einsicht (HessDSchG § 5),
-zugriff (HessDSchG § 5).

Der folgende terminologische Vorschlag geht — wie auch sonst bisher — von „Daten" auf „Information" über und bezieht deren pragmatische Ebene (Beziehung der Information zu ihrem Benutzer) nach Möglichkeit ein, wie soeben begründet wurde.

2.3. Die Benennung der einzelnen Phasen

Zu beachten ist, daß im folgenden, wenn von „Informationen" gesprochen wird, immer nur Individual (einschließlich Gruppen-)informationen gemeint sind.

2.3.1. Informationsermittlung

umfaßt (Erst-)Beschaffung und Auswahl von Informationen. Beispiel: Polizeibeamter oder Detektiv recherchieren. Der bisherige technische Begriff der *Daten*ermittlung umfaßte das Erstellen der Urbelege sowie die Auswahl bereits beschaffter Informationen [2]). Unter rechtlichen Gesichtspunkten betrachtet, kommt es vor allem auf die Beschaffung an, etwa als Tatbestand des Eindringens in die „Privatsphäre" [3]).

2.3.2 Informationserfassung

ist das Übersetzen von Informationen in Daten [4]). Beispiel: Stanzen einer Lochkarte, Notieren eines Termins.

Der technische Begriff ist enger; er umfaßt das Übersetzen von Informationen in maschinenlesbare Daten oder ihre Direkteingabe. Der rechtlich bedeutsame Fall des Übertragungsfehlers wird unter Informationsveränderung erfaßt.

2.3.3. Informationsspeicherung

ist Aufbewahrung der erfaßten Informationen zur weiteren Verwendung [5]); z. B. auf Karteikarten, Magnetband (externer Speicher einer EDVA) oder im Kernspeicher (interner Speicher).

2.3.4. Informationsveränderung [6])

umfaßt die Umformung von Information

— *In syntaktischer Hinsicht* (hinsichtlich der Zeichenfolge); z. B. die Zeichenfolge „Herr Cohn" wird umgeformt in „rHre Chno", oder ein Zeichen kommt hinzu (anstatt „DM 100" „DM 1000") oder entfällt („DM 10") oder wird ausgetauscht („DM 101").

— *In semantischer Hinsicht* (hinsichtlich des Inhalts). Eine Inhaltsveränderung liegt vor, wenn die Information eine(n) andere(n) Sachverhalts-(komponente) bezeichnet als vorher. Z. B. „Ball" (als Tanzveranstaltung oder als Spielgegenstand — syntaktisch die gleiche Zeichenfolge!), oder die Zeichenfolge „Herr Cohn" wird zugeordnet der weiteren Zeichenfolge „besitzt die israelitische Staatsangehörigkeit" (Informationsverknüpfung).

— *In pragmatischer Hinsicht* (hinsichtlich der Beziehung zum Empfänger [Benutzer/Adressaten]); z. B. die inhaltlich gleiche Information „Bonn anerkennt DDR" löst bei Regierungspartei, Opposition und DDR je verschiedene Reaktionen aus; sie hat in den jeweiligen IS unterschiedlichen Stellenwert.

  Oder: „Müller hat Steuern hinterzogen" bedeutet für das Finanzamt und den Staatsanwalt je verschiedenes, löst darum unterschiedliche Rechtsfolgen aus.

  Oder: „Meier stellt Zahlungen ein" bedeutet für das Konkursgericht bzw. die Gläubiger je verschiedenes, löst verschiedene Reaktionen der Betroffenen aus.

— *In sigmatischer Hinsicht* (hinsichtlich der Beziehung zum Bezeichneten); z. B. IS berechnet vermutliches Wahlverhalten bei einer realen oder hypothetischen Bevölkerung.

Insbesondere fallen unter Informationsveränderung die verschiedenen Formen automatisierter Datenverarbeitung i. e. S.; z. B. Addieren, Subtrahieren usw., Vergleichen, Verknüpfen, Aggregieren.

Informationsveränderung kann also definiert werden als die Umformung von Informationen durch Änderung der fixierten Zeichenfolge, durch Informationsverknüpfung, durch Änderung des Inhalts und durch Zuordnung zu einem anderen Empfänger.

2.3.5. Informationsweitergabe [7])

ist *Informationsausgabe* [8]) einer eigenen Information an Dritte (eigen = selbst ermittelt).

Wird sie an unbestimmte Dritte weitergegeben (Presse, Öffentlichkeit), dann handelt es sich um *Informationsveröffentlichung* [9]).

Weitergabe innerhalb der (öffentlichen oder privaten) Verwaltung heiße *Informationsaustausch* [10]), bei integrierter Datenverarbeitung jedoch *Informationsverbund* [11]), sonst *Informationsweitergabe an (außenstehende) Dritte* (z. B. Parlament, Kunden).

---

[2]) Steinmüller (1), 75; Meincke, 35
[3]) Kamlah (2), 362
[4]) Meincke, 35; Steinmüller (1), 75
[5]) Meincke, 36
[6]) vgl. zum ganzen Steinmüller (1), 8
[7]) HessDSchG, ebd. — Die Terminologie ist für 2.3.5. besonders vereinfacht; zusätzlich wäre etwa zu unterscheiden zwischen den angeführten Begriffen und „Zugriff", „Transport", „Transfer", „Übertragung", „Abgabe" von Informationen bzw. Daten
[8]) Von der technischen Datenausgabe (output; vgl. Meincke, 37) unterscheidet sich die Informationsausgabe durch Einbeziehung der pragmatischen Ebene des Adressaten. Zum *Datentransport* vgl. HessDSchG § 5
[9]) HessDSchG, ebd.
[10]) BayEDVG, Artikel 4 und 10
[11]) vgl. BayEDVG, Artikel 7 „Datenverbund" — streng genommen handelt es sich dann nicht mehr notwendig um „Weitergabe" und „Austausch" sondern um Vielfachzugriff und Vielfachverarbeitung von einmal ermittelten, erfaßten und gespeicherten Informationen.

2.3.6. Informationslöschung

ist die endgültige Vernichtung erfaßter bzw. gespeicherter Informationen (z. B.: Brand zerstört „Spiegel"-Archiv). Der Unterschied zur Informationsveränderung besteht in der totalen Unbrauchbarkeit der gelöschten Informationen; die Informationsveränderung dagegen beinhaltet nur eine Einschränkung der Brauchbarkeit.

3. Öffentliche und private Informationsverarbeitung

Die Phasen der Informationsverarbeitung gelten gleichermaßen für jede Informationsverarbeitung, geschehe sie durch die öffentliche Verwaltung oder ein Industrieunternehmen. Gleichwohl ist für das folgende die Unterscheidung von Informationsverarbeitung durch öffentliche und nicht-öffentliche Stellen (öffentliche und private Informationsverarbeitung) grundlegend. Denn je nach dem gelten verschiedene Normen. Es muß dann festgelegt werden, welche Kriterien erfüllt sein müssen, um Informationsverarbeitung im öffentlichen oder im privaten Bereich zu lokalisieren, da im Hinblick auf das Datenschutzgesetz verschiedene Regelungsmaterien in Frage kommen und dementsprechend auch verschiedene Regelungsvorschläge gemacht werden. Es muß klargestellt werden, wer Adressat welcher Regelung ist.

3.1. Informationsverarbeitung durch öffentliche Stellen (kurz: öffentliche Informationsverarbeitung)

Informationsverarbeitung ist — im Sinne des Gutachtens — dann im öffentlichen Bereich lokalisiert, wenn sie durch eine öffentliche Stelle, d. h. im Rahmen einer Tätigkeit der öffentlichen Verwaltung geschieht (vgl. Definition). Eine Tätigkeit dient dann Zwecken der öffentlichen Verwaltung, wenn sie Angelegenheiten von Gemeinwesen und ihren Mitgliedern besorgt [12]). Darunter fällt nicht die Verarbeitung zum Zweck der Erhaltung von Finanz- und Verwaltungsvermögen des Staates, also die rein fiskalische Verwaltung [13]).

3.2. Informationsverarbeitung durch nicht-öffentliche Stellen (kurz: private Informationsverarbeitung)

Informationsverarbeitung ist — im Sinne des Gutachtens — dann im privaten Bereich lokalisiert, wenn sie nicht durch die öffentliche Verwaltung im eben festgelegten Sinne geschieht.

3.3 Erläuterung

Entscheidend für die Untersuchung ist der *Zweck*, für den Information verarbeitet wird, nicht die Rechtsform, in deren Rahmen sich die Verarbeitung abspielt. So ist eine öffentliche Stelle, die etwa im Rahmen der Leistungsverwaltung privatrechtlich tätig wird [14]) (und damit trotzdem Aufgaben des Gemeinwesens und seiner Mitglieder wahrnimmt) — erst recht, wenn sie privatrechtlich organisiert ist, etwa als GmbH — nicht einfach nur nach privatrechtlichen Kategorien zu messen. Vielmehr ist sie dann nicht im Vollgenuß der Privatautonomie und muß sich öffentlich-rechtlichen Bindungen unterwerfen [15]). Insbesondere ist die Verfassung bindend [16]). Da das Datenschutzgesetz aus der Verfassung entwickelt werden muß, ist auch die derart tätige Verwaltung daran gebunden.

In verstärktem Maß gilt das auch für *öffentliche Informationssysteme:* Es geht nicht an, daß der Staat sich durch privatrechtliche Organisation den öffentlich-rechtlichen Bindungen entzieht [17]). Umgekehrt kann nun der private Bereich die Informationsverarbeitung durch Privatpersonen sowie die rein fiskalische Verwaltung umfassen.

Der Adressatenkreis der jeweiligen Regelung ist somit festgelegt. Es sind öffentliche bzw. nicht-öffentliche Stellen, maW. die öffentliche bzw. private Verwaltung.

3.4. Alternative

Für die Unterscheidung von öffentlicher und privater Informationsverarbeitung kann auch auf die tatsächlichen Beherrschungsverhältnisse (statt auf die Zweckbestimmung) abgestellt werden. Öffentliche Informationsverarbeitung wäre dann jede Informationsverarbeitung im (überwiegenden) Herrschaftsbereich des Staates — in Anlehnung an arbeitsrechtliche Gedankengänge („Sphärentheorie"). In diesem Falle würde die Informationsverarbeitung eines vom Staat tatsächlich beherrschten Konzerns den Datenschutznormen des öffentlichen Bereiches unterliegen.

---

[12]) Wolff (1), 13; z. B. ist die (privatrechtlich organisierte) „Gesellschaft für Mathematik und Datenverarbeitung" (GMD) eine öffentliche Stelle in diesem Sinne

[13]) dazu Maunz-Dürig-Herzog, Artikel 1 N 135

[14]) Maunz-Dürig-Herzog, Artikel 1 N 111; Bay. VGH in Bay. VBL 56, 274

[15]) Wolff (1), 99

[16]) Maunz-Dürig-Herzog, Artikel 1 N 134; für Artikel 3 anerkannt durch BGHZ in JZ 59, 405 mit Anm. von Raiser

[17]) vgl. die im Fernsehurteil des BVerfG entwickelten Grundsätze (BVerfGE 12, 205)

III. Rechtliche Grundlagen des Individualdatenschutzes

Datenschutz wurde einleitend definiert als Schutz vor unerwünschter IV, d. h. vor allem: vor IV, die den Grundentscheidungen der Verfassung zuwiderläuft. Diese Grundentscheidungen sind auch die obersten Kriterien öffentlicher wie privater IV. Sie sind auch die Grundlage und Grenze des gesetzgeberischen Ermessens im Hinblick auf das DSch-Recht. Da die meisten Rechtsprobleme bei der Erörterung der Besonderheiten der öffentlichen und privaten IS [1]) einzuordnen sind, hier vorweg einige gemeinsame Hinweise auf

— die „zwei Säulen des DSchRechts" in Artikel 2 und Artikel 20 GG; (1.)

— die Gesetzgebungskompetenzen für DSch im öffentlichen wie im privaten Bereich; (2. und 3.)

— und ein Grundrecht auf Information; Exkurs I.

1. Die „zwei Säulen" des Datenschutzrechts

1.1. Staatsrecht — Quelle der obersten Kriterien für Informationsverarbeitung

Zwar enthält die Verfassung den Begriff Information nicht, doch ist sie am ehesten geeignet, Kriterien für die rechtliche Regelung der IV zu liefern. Verfassung und soziale Wirklichkeit stehen in engem Zusammenhang: Der soziale Wandel bringt Änderungen in der Verfassung und deren Verständnis mit sich und umgekehrt. D. h., die Verfassung wandelt sich im Laufe der Zeit [2]). Diese Fähigkeit, neue Realitäten zu erfassen, ist zwar dem Recht überhaupt gegeben, findet aber im Staatsrecht seine stärkste Ausprägung. Nur so vermag die Verfassung normative Kraft zu entfalten [3]). Daß allein die Verfassung oberste Kriterien für die IV zu geben vermag, zeigt folgende Überlegung: Die tatsächliche Bedeutung der IV ist in allen Bereichen der Gesellschaft offenkundig. Kriterien zur Beurteilung sämtlicher Aspekte und Auswirkungen der IV kann nur ein Rechtsgebiet enthalten, welches im Zentrum des sozialen Lebens steht und normierend auf Staat und Gesellschaft zugleich einwirkt. Die Mittel des Privatrechts reichen für soziale Tatbestände von solch umfassender Bedeutung nicht aus. Den genannten Anforderungen wird nur die Verfassung gerecht; nur sie nimmt als zentraler Bezugspunkt auf unser ganzes Leben Einfluß.

1.2. Grundrechte und Rechtsstaatlichkeit

Die obersten Kriterien der IV sind die

— Rechts- und Sozialstaatlichkeit,

— der Grundrechtskatalog als Grund und Grenze staatlichen sowie privaten Handelns.

Rechts- und Sozialstaatlichkeit einerseits und Grundrechte andererseits bilden darum die zwei Säulen des DSchRechts. Dies gilt im Grundsatz auch für den Kollektivdatenschutz. Dabei liegt, was den Individualdatenschutz betrifft [4]), das Hauptgewicht auf der Neuinterpretation der Handlungsfreiheit Artikel 2 Absatz 1 GG als Selbstbestimmungsrecht über das individuelle Persönlichkeitsbild und auf der rechtsstaatlichen Beschränkung der IV im Hinblick auf die Zuständigkeit der verarbeitenden Stelle.

Des weiteren muß jedoch differenziert werden: Die private IV unterliegt nicht dem rechtsstaatlichen Grundsatz der Gesetzmäßigkeit der Verwaltung. Die dem Bürger gegenüber dem Staat zustehenden Grundrechte entfallen weitgehend im Verhältnis zu privaten IS, wo sie nur eine eingeschränkte Wirkung entfalten, wie im Teil D näher ausgeführt wird. Hat aber der Bund überhaupt die Kompetenz, ein DSchGesetz zu erlassen?

2. Gesetzgebungskompetenz des Bundes für eine Regelung der Informationsverarbeitung durch öffentliche Stellen

Grundprinzip für die Verteilung von Gesetzgebungskompetenzen ist die Zugehörigkeit der Gesetzesmaterie zu einem bestimmten Rechtsgebiet. Zu untersuchen ist demnach unter 2.1., was Regelungsgegenstand eines Individual-Datenschutzgesetzes ist, ob die Gesetzesmaterie (2.2.) Gegenstand des materiellen Rechts (Bundeskompetenz gem. Artikel 73, 74 GG) oder (2.3.) des Verwaltungsverfahrensrechts (Bundeskompetenz gem. Artikel 84 Abs. 1, Artikel 85 Abs. 1 GG) ist oder ob die besondere Ausgestaltung des Regelungsgegenstandes (2.4.) eine über die in Punkt 2.2. und 2.3. gezeigte Kompetenzverteilung hinausgehende Lösung erfordert.

2.1. Regelungsgegenstand

Das Datenschutzgesetz enthält im wesentlichen Bestimmungen über den DSch in den verschiedenen Phasen der IV, namentlich bei Informationsermittlung, Informationsaustausch und Informationsweitergabe an Dritte. Betroffen sind sämtliche öffentliche Stellen, indem ihnen Beschränkungen auferlegt und Kontrollorgane eingerichtet werden. Als Kehrseite dazu erhält der Bürger subjektive öffentliche Rechte.

---

[1]) Teil C und D
[2]) dazu Lang, 267 ff., 271, 276; Bäumlin (3), 9
[3]) Hesse (2), 18
[4]) Teil C

2.2. Datenschutz und materielles Recht

Die Datenschutzregelung sieht Abwehr- und Schadensersatzansprüche des Bürgers hinsichtlich der Verarbeitung von Individualinformationen durch die öffentliche Verwaltung vor. Sie schafft damit Rechte des Bürgers gegenüber der Verwaltung und stellt daher materielles Recht dar.

Der Grundgesetzgeber hat die Gesetzgebungskompetenz für das materielle Recht in Artikel 70 bis 74 GG geregelt, wobei er in einem enumerativen Katalog von Gesetzgebungsgegenständen dem Bund die ausschließliche (Artikel 73 GG) bzw. konkurrierende (Artikel 74 GG) Gesetzgebungskompetenz zugewiesen hat. Fraglich ist nun, ob die angestrebte Datenschutzregelung in diese Mosaikkompetenz des Bundes eingepaßt werden kann.

Der Bund hat auf Teilgebieten der Datenschutzregelung bereits die gesetzgeberische Initiative ergriffen [5]), sowie speziell hinsichtlich der personenbezogenen Daten durch § 2 des Entwurfs eines Gesetzes über das Meldewesen (Bundesmeldegesetz). Allen diesen Regelungen ist jedoch gemein, daß sie nur einen bestimmten Teil der öffentlichen Verwaltung betreffen und einem bestimmten Rechtsgebiet zuzuordnen sind, das jeweils in Artikel 73 bzw. Artikel 74 GG aufgeführt ist und dementsprechend der jeweiligen Regelung als Kompetenzgrundlage dient. Kennzeichnend für die angestrebte Datenschutzregelung ist jedoch, daß sie nicht auf bestimmte Rechtsgebiete oder einzelne Verwaltungsbehörden ausgerichtet ist, sondern daß sie für alle Rechtsgebiete gelten soll, auf denen Verwaltungshandeln und damit Informationsverarbeitung stattfindet.

Die Datenschutzregelung schafft also Obersätze, materiell-rechtliche Richtlinien für das Verwaltungshandeln in seiner gesamten Variationsbreite, soweit es die oben angeführten Phasen der Informationsverarbeitung berührt. Damit wird aber auch deutlich, daß die Mosaikkompetenz des Bundes aus Artikel 73 und Artikel 74 GG nicht geeignet ist, eine Zuständigkeit des Bundes für die angestrebte generelle Regelung zu begründen; es handelt sich eben nur um ein unvollständiges Mosaik, das Lücken für die Gesetzgebungskompetenz der Länder offenläßt.

2.3. Datenschutz und Verwaltungsverfahrensrecht

Eine Gesetzgebungskompetenz des Bundes auf dem Gebiet des Datenschutzes könnte sich daraus ergeben, daß die Datenschutzregelung als Verwaltungsverfahrensregelung zu klassifizieren ist (Artikel 84 Abs. 1, Artikel 85 Abs. 1 GG). Nach einhelliger Meinung in der Literatur handelt es sich nur dann um Verwaltungsverfahren, wenn die Art und Weise, wie die Verwaltung tätig werden darf, geregelt wird. Werden jedoch Rechte und Pflichten des Bürgers geschaffen (materielles Recht), so handelt es sich nicht um Verwaltungsverfahren [6]). Danach stellt die angestrebte Datenschutzregelung, die, wie oben gezeigt wurde, auch materiellrechtlichen Charakter hat, insoweit keine Verwaltungsverfahrensregelung dar. Datenschutz wäre lediglich nach der Meinung des Rechtsausschusses des Bundesrates Verwaltungsverfahrensrecht, da dieser auch Bestimmungen darüber, ob und unter welchen Voraussetzungen Behörden tätig werden oder tätig werden können, zum Verwaltungsverfahren zählt [7]).

Selbst wenn man der Meinung des Rechtsausschusses des Bundesrates folgt, die wohl im Hinblick auf die damit verbundene Ausweitung des Zustimmungsrechts des Bundesrates erfolgt ist, ergibt sich keine Kompetenz des Bundes zum Erlaß einer generellen Datenschutzregelung. Die Literatur ist sich vielmehr einig, daß Artikel 84 Abs. 1 und Artikel 85 Abs. 1 GG nur eine Annexkompetenz zu Artikel 73 und 74 GG schaffen [8]). Das geht auch aus dem Wortlaut des Artikels 84 Abs. 1 und Artikels 85 Abs. 1 GG hervor, wo die Regelung des Verwaltungsverfahrens auf die Ausführung der Bundesgesetze durch die Länder als Auftrags- oder eigene Angelegenheit beschränkt ist.

Nachdem nun klargestellt ist, daß Artikel 84 Abs. 1 und 85 Abs. 1 GG keine über die in Artikel 73 und 74 GG bereits eingeräumten Kompetenzen hinausgehende Kompetenz schafft, eine Verwaltungsverfahrensregelung demzufolge ebenfalls nur lückenhaft sein kann, ergibt sich: Auch wenn man der Meinung des Rechtsausschusses des Bundesrats folgt, besteht keine Kompetenz des Bundes zu einer umfassenden Datenschutzregelung.

2.4. Lösungsvorschläge

Nachdem die bisherigen Überlegungen zu einer Verneinung einer umfassenden Bundeskompetenz in Sachen Datenschutz geführt haben, bieten sich folgende Lösungsmöglichkeiten an:

2.4.1. Ergänzung der Artikels 75 GG

Der Grundgesetzgeber könnte durch Ergänzung des Artikels 75 GG dem Bund die Gesetzgebungskompetenz zum Erlaß von Rahmenvorschriften über den Datenschutz einräumen. Die Wahrung der Rechtseinheit auf einem für den Bürger so bedeutsamen Gebiet, wie es der Datenschutz darstellt, fordert eine über das Gebiet eines Landes hinausgehende Regelung (Artikel 72 Ziff. 3 GG) und erfüllt damit den Vorbehalt des Artikels 75 Abs. 1 S. 1.

2.4.2. Gleichlautende Gesetze

Als weitere Möglichkeit, den Kompetenzschwierigkeiten zu entgehen, bietet sich ein Weg an, der bereits zum Erlaß eines Verwaltungsverfahrensgesetzes beschritten werden soll. Danach wäre der Entwurf des Datenschutzgesetzes durch Bund und

---

[5]) vgl. z. B. § 12 Bundesstatistikgesetz vom 3. September 1953 (BGBl. I S. 1314); § 44 Abs. 4 Außenwirtschaftsgesetz vom 28. April 1961 (BGBl. I S. 481); § 9 Kreditwesengesetz vom 10. Juli 1961 (BGBl. I S. 881)

[6]) so Maunz-Dürig-Herzog, Artikel 84 N. 29; Hamann-Lenz, Artikel 84 A 2; Schmidt-Bleibtreu-Klein, Artikel 84 N 5; Held, AÖR 80, 73

[7]) 95. Sitzung des Rechtsausschusses, Protokoll S. 5 ff. und Anlage 1 R 131/52 bei Behandlung des Deutschlandvertrages

[8]) Schmidt-Bleibtreu-Klein, Artikel 84 N. 6; Hamann-Lenz, Artikel 84 A 2

Länder gemeinsam zu erarbeiten mit dem Ziel, daß dieser Entwurf inhaltlich gleichlautend vom Bundestag als Bundesgesetz und von den Länderparlamenten jeweils als Landesgesetz erlassen wird. Damit wäre sichergestellt, daß auch dort eine bundeseinheitliche Regelung vorliegt, wo der Bund mangels Kompetenz keine Datenschutzregelung treffen kann.

3. Gesetzgebungskompetenz des Bundes bezüglich der Regelung der Informationsverarbeitung durch nicht-öffentliche Stellen

Die Regelung der Informationsverarbeitung nicht-öffentlicher Stellen berührte eine Mehrzahl von Rechtsgebieten, die alle für die Gesetzgebungskompetenz von Bedeutung sind. Die Klassifizierung der Gesetzesmaterie hinsichtlich ihrer Zugehörigkeit zu Rechtsgebieten ergibt sich aus der jeweiligen rechtlichen Wertung, die der Information zuteil wird.

3.1. Privatautonomie und Abwehransprüche

Die Regelung der Verfügungsbefugnis über Individualinformationen trägt mit Rücksicht auf ihre Zielrichtung, den jeweiligen persönlichen Verfügungsbereich auch hinsichtlich der Individualinformationen abzustecken, privatrechtlichen Charakter. Es handelt sich ebenso wie bei der Regelung von Schadenersatz-, Unterlassungs- und „Folgebeseitigungsansprüchen" materiell um Ergänzungen des bürgerlichen Rechts [9]). Die Bundeskompetenz ergibt sich deshalb aus Artikel 74 Nr. 1 i. V. m. Artikel 72 Abs. 2 Nr. 3 im Hinblick auf die Wahrung der Rechtseinheit, über die Grenzen eines Landes hinaus.

3.2. Gewerbliche und innerbetriebliche Informationssysteme

Interne zweckgebundene Informationssysteme (innerbetriebliche IS) sind unentbehrlich zur Organisation wirtschaftlicher Unternehmungen und bilden damit einen wesentlichen Bestandteil des wirtschaftlichen Lebens. Das gleiche trifft für die gewerblichen IS zu; ohne ihren Informationsbeitrag würden einige Bereiche der modernen arbeitsteiligen Wirtschaft lahmgelegt. Gesetzgeberische Regelungen über diese Informationssysteme fallen in das *Recht der Wirtschaft,* wobei die Gesetzgebungskompetenz auch bezüglich dieses Gegenstandes der konkurrierenden Gesetzgebung (Artikel 74 Nr. 11 GG) im Hinblick auf die Wahrung der Rechtseinheit (Artikel 72 Abs. 2 Nr. 3 GG) dem Bund zusteht.

3.3. Arbeitsrecht

Soweit dabei eine tarifvertragliche Regelung bezüglich vorliegender Arbeitsverhältnisse (i. S. des Arbeitsrechts) angesprochen wird, ergibt sich die Kompetenz des Bundesgesetzgebers aus Artikel 74 Nr. 12 i. V. m. Artikel 72 Abs. 2 Nr. 3 GG.

3.4. Informationsamt

Was die Aufsichtsmaßnahmen anbelangt (Amt für Datenschutz bzw. Informationsamt), so handelt es sich hier ebenfalls um einen Gegenstand aus dem Recht der Wirtschaft. Ebenso wie bei den vom Bundesgesetzgeber bereits getroffenen Regelungen z. B. der Bank- und Börsenaufsicht oder der Versicherungsaufsicht fallen unter das Recht der Wirtschaft auch öffentlich-rechtliche Vorschriften [10]).

3.5. Strafrecht

Der Bund hat schließlich auch die Kompetenz, Strafvorschriften für die Nichtbeachtung seiner gesetzlichen Regelungen zu erlassen, Artikel 74 Nr. 1 i. V. m. Artikel 72 Abs. 2 Nr. 3 GG. Gerade hinsichtlich der strafrechtlichen Folgen der mißbräuchlichen Informationsverarbeitung erscheint eine bundeseinheitliche Regelung im Sinne der Wahrung der Rechtseinheit und Rechtssicherheit dringend geboten.

3.6. Ergebnis:

Auf dem Gebiet der Informationsverarbeitung durch nicht-öffentliche Stellen liegt die Gesetzgebungskompetenz beim Bund.

[9]) Maunz-Dürig-Herzog, Artikel 74 N. 22
[10]) vgl. Maunz-Dürig-Herzog, Artikel 74 N. 77; BVerfGE 4, 13

Exkurs I: Grundrecht auf Information

Gibt es ein allgemeines Grundrecht des Bürgers auf Information, gegebenenfalls sogar gegen nicht-öffentliche Stellen? Die hier beigefügte Studie eines Mitarbeiters bejaht dies angesichts der Entwicklung der neuen computerunterstützten Informationssysteme: Die neue Wirklichkeit verlangt eine wirklichkeitsgerechte Interpretation der Verfassung.

1. Fragestellung

Staatliches Handeln, gleich ob rechtssetzender, rechtsanwendender oder rechtskontrollierender Natur, ist immer zugleich auch Informationsverarbeitung. Gegenstand der bisherigen Untersuchung war die Berechtigung öffentlicher und privater Stellen,

Individualinformationen zu verarbeiten, ohne die „Privatsphäre" des einzelnen zu verletzen. Fraglich ist, ob dieser Berechtigung auf seiten des Bürgers ein Recht entspricht zu erfahren, was in den einzelnen Phasen der IV durch öffentliche und private Stellen geschieht. Ob es ein solches „Recht auf Information" auf verfassungsrechtlicher Ebene in Gestalt eines *Grundrechts auf Information* gibt, ist zu untersuchen.

Im folgenden sind zunächst einige terminologische Festlegungen erforderlich (2.). Sodann wird in einer Bestandsaufnahme ein Überblick über die derzeit herrschenden Auffassungen in Rechtsprechung, Lehre und bestehenden Gesetzen gegeben (3.). Daraufhin wird die theoretische Forderung nach einem allgemeinen Grundrecht auf Information erhoben (5.), dessen dogmatischer Sitz zwar Artikel 5 GG ist (6.), der jedoch insoweit einer Neuinterpretation bedarf (7.). Weiter werden Ausführungen über die Ausgestaltung des Grundrechts (8.), den Träger (9.) und den Umfang des Grundrechts gemacht (10.). Schließlich werden in einem Abschnitt „Drittwirkung" (11.) die Konsequenzen der gefundenen Ergebnisse für die private Informationsverarbeitung behandelt.

2. Terminologie

2.1. Informationsrecht

Ausgehend von dem im Gutachten zugrunde gelegten Informationsbegriff versteht man unter einem „Informationsrecht" des Bürgers ein Recht auf Herstellung der Wahrnehmbarkeit und Zugänglichkeit gewisser Phasen staatlicher Informationsverarbeitung. Es ist ein subjektives öffentliches Recht auf Leistung von Informationen [1]) und umfaßt alle nicht allgemein zugänglichen Informationsquellen, die sich dem einzelnen gegenüber dem Staat erschließen, so z. B. das Recht auf Einsicht in nicht allgemein zugängliche Prozeßakten, Zugang zu nichtöffentlichen Verhandlungen, insbesondere Rechte auf Auskunft über staatliche Vorgänge. Wenn auch begrifflich ein Unterschied ist, ob der Bürger Zugang, Einsicht oder Auskunft verlangt, weil er in einem Fall ein „Gewährenlassen", im anderen Fall ein positives Tun fordert, so handelt es sich doch um eng miteinander verwandte Fallgruppen der Leistung von Information. Die Informationsleistung des Staates muß nicht in einem positiven Tun, sondern sie kann auch in einem Unterlassen bestehen. In jedem Fall macht der einzelne einen Anspruch auf eine Informationsleistung des Staates geltend.

Ein „Recht" des Bürgers (oder einzelner Gruppen) auf Leistung von Information könnte folgendes beinhalten:

— Anspruch auf *Zugang* zu Einrichtungen öffentlicher Stellen,

— Recht auf *Einsichtnahme* in Akten oder sonstige Unterlagen öffentlicher Stellen,

— Recht auf *Aufklärung* über Vorgänge staatlichen Geschehens,

— Recht auf *Auskunft* über Tätigkeiten öffentlicher Stellen,

— Anspruch auf *Benachrichtigung* (Kontrollmitteilung) über Vorgänge staatlicher Informationsverarbeitung allgemein,

— Ansprüche auf *Offenlegung* des Staatsgeschehens für den Bürger.

Dabei können die einzelnen Ausgestaltungen von Informationsansprüchen untereinander nach jeweiliger Situation ein Mehr oder Weniger bedeuten.

2.2. Grundrecht auf Information

Ein Grundrecht auf Information ist ein in der Verfassung verankertes subjektives öffentliches Recht auf Leistung von Information für den einzelnen oder bestimmte Gruppen. Als allumfassendes „Recht" verstanden, ließe es alle möglichen, oben genannten Informationsleistungen des Staates zu. Nach dem alten Verständnis eines Grundrechts als *Abwehr*recht gegen den Staat wäre ein Grundrecht auf Information nur in der Form eines unselbständigen Abwehranspruchs denkbar. Da sich das Verständnis der Grundrechte heute zu einem „Wert- und Anspruchssystem" gewandelt hat, dahin gehend, daß mit den Grundrechten nicht nur ein sog. „staatsfreier Raum" für den einzelnen verbrieft wird, sondern der Bürger (oder bestimmte Gruppen) aus ihnen positive Ansprüche gegen den Staat [2]) herleiten kann, ist ein Grundrecht *auf* Information schlechthin, d. h. *auf* alle möglichen Arten staatlicher Informationsleistungen, begrifflich durchaus denkbar und soll im folgenden erörtert werden.

3. Bestandsaufnahme

3.1. Gesetze

Das Wort „Information" fehlt im Grundgesetz. In einigen Bestimmungen ist das Verhalten des Staates in bezug auf Information des einzelnen Staatsbürgers geregelt: z. B. in Artikel 5 (Grundrecht der Meinungsfreiheit), Artikel 21 Abs. 1 Satz 3 GG (Pflicht der Parteien, über die Herkunft ihrer Mittel öffentlich Rechenschaft abzulegen) Artikel 42 GG (Grundsatz der Parlamentsöffentlichkeit). Verschiedentlich sind Informationsrechte des Bürgers vom Gesetzgeber normiert, so z. B. in § 34 FGG, § 299 II ZPO, § 175 II GVG. Im übrigen gibt es verstreute Informationsrechte verschiedenster Art; so im Aktienrecht (Auskunftrecht des Aktionärs), usf.

3.2. Rechtsprechung

In der Rechtsprechung wurden „Informationsrechte" des einzelnen bisher nur unter dem Gesichtspunkt des *Auskunftsbegehrens* behandelt.

[1]) vgl. v. Mangoldt-Klein, 240
[2]) Maunz-Dürig-Herzog, Artikel 1 N. 96

Nach einem Beschluß des 44. Deutschen Juristentags wird Auskunft heute allgemein als „die individuelle Tatsachenmitteilung oder unverbindliche Rechtsauskunft" bezeichnet und damit abgegrenzt von der Zusage oder Zusicherung (als hoheitliche Selbstverpflichtung der Verwaltung). Da den *rechtsuchenden* Bürger Information erfahrungsgemäß nur dann interessiert, wenn es um irgendwelche Rechtspositionen — um seine Ehre oder andere Rechte — geht, konzentriert sich die Rechtsprechung auf ganz bestimmte Fallgestaltungen, wie den „Denunziantenfall" in verschiedensten Ausformungen [3]), Einsichtsverlangen in Personal- und Prüfungsakten oder sonstige die Person des Antragstellers betreffenden Unterlagen, um Akteneinsicht im gerichtlichen Verfahren, Einsichtsbegehren innerhalb eines bestimmten Benutzungsverhältnisses.

Der andere denkbare Fall, daß der Bürger lediglich um der Information willen, aus rein politischem, historischem oder sonstigem nicht-rechtlichem Interesse Informationen begehrt, wurde von der Rechtsprechung bisher so gut wie nicht behandelt.

Die zur Frage des Auskunftbegehrens ergangenen Entscheidungen lassen sich auf drei Leitsätze zurückführen:

1. Ein allgemeines staatsbürgerliches Recht auf Information ist weder im GG noch in den Länderverfassungen (noch in irgendeinem einfachen Gesetz) ausdrücklich normiert.
2. Wenn nicht einer der vom Gesetzgeber ausdrücklich normierten Sonderfälle eines (Auskunfts-)Informationsrechts vorliegt, steht die Informationserteilung im pflichtgemäßen Ermessen der Behörde.
3. Bei der Ermessensentscheidung ist das private Interesse des Antragstellers gegen das öffentliche Interesse an der Geheimhaltung oder das übergeordnete Privatinteresse eines Dritten abzuwägen [4]).

Die Entscheidungsgründe konzentrieren sich jeweils auf den aktuellen besonderen Bezugspunkt des Falles. Ein verfassungsrechtlicher Bezug fehlt bisher bei der gesamten Rechtsprechung.

Soweit in vereinzelten Fällen Information aus politischen oder anderen Interessen, also „Information um der Information willen" verlangt wurde, haben die Gerichte nur die Situation des „passiv-rezeptiven Neugierwesens" berücksichtigt [5]).

[3]) vgl. die Zusammenstellung bei Perschel, 232
[4]) z. B. OLG Braunschweig DVBl 51, 441
[5]) vgl. Windsheimer, 146 m. w. Nachw.
[6]) zum Stand der Meinungen vgl. Windsheimer, 150 ff.
[7]) Windsheimer, 154
[8]) Windsheimer, 155
[9]) vgl. hierzu den vorzüglichen Aufsatz von L. Philipps, Recht und Information (erscheint demnächst in dem von A. Kaufmann herausgegebenen Band Rechtstheorie)
[10]) Windsheimer a. a. O.

3.3. Literatur

Die Literatur hat zunächst den dritten von der Rechtsprechung entwickelten Leitsatz zum Auskunftsrecht, nach und nach auch die beiden anderen Leitsätze in Zweifel gezogen [6]). Man ist sich in der Literatur heute darüber einig, daß die Behörde in ihrem Ermessen nicht völlig frei sein kann, daß eine demokratisch und rechtsstaatlich geführte Verwaltung Akteneinsicht nicht grundsätzlich verweigern darf; Anknüpfungspunkt bei Leitsatz 3 ist das berechtigte Interesse des Bürgers, wobei verschiedenste Auffassungen zur Güterabwägung zwischen Interessen des Betroffenen und öffentlichen Interessen bzw. Privatinteressen des Dritten vertreten werden. Zum 2. Leitsatz wird vielfach die Meinung vertreten, die Fragestellung müsse richtigerweise lauten, warum die Behörde im speziellen Fall die Akten geheimhalten dürfe, und nicht, weshalb der Antragsteller berechtigt sei, in die über ihn geführten Akten Einsicht zu nehmen [7]).

Zweifel bezüglich des ersten Leitsatzes führen zu der Fragestellung, ob es überhaupt eines besonderen Grundrechtes bedarf, um die Auskunfts- und Einsichtsrechte zu rechtfertigen. Denn grundsätzlich besteht die Vermutung zugunsten der Freiheit des Bürgers („In dubio pro liberate" [Uber]). Zwar fehlt auch bei den einzelnen Literaturmeinungen zu den von der Rechtsprechung entwickelten Grundsätzen zum Auskunftsbegehren der verfassungsrechtliche Bezug. Doch wurde von der Literatur wenigstens die andere Fallgestaltung gesehen, ein Informationsbegehren des Bürgers aus politischen, historischen oder sonstigen, nicht-rechtlichen, allgemein staatsbürgerlichen Interessen [8]). Wenn verschiedentlich der Durchgriff auf die Verfassung unternommen wurde, so immer nur in bestimmten Fallgestaltungen und Teilbereichen. Die Frage nach einem umfassenden Informationsrecht des Bürgers auf verfassungsrechtlicher Ebene wurde bisher nur vereinzelt gestellt [9]) und, wo dies geschah, abgelehnt [10]).

4. Systematisierung eines möglichen Grundrechts auf Information

4.1. Fallgruppen

In der Diskussion um das Informationsrecht lassen sich die Fallgruppen danach unterscheiden, ob sich das Informationsinteresse des auskunftsuchenden Bürgers auf den „geistigen Wert" der Information beschränkt, oder darüber hinausgeht. Diese Unterscheidung rechtfertigt folgenden Versuch einer Systematisierung eines möglichen Grundrechts auf Information:

1. Grundrecht auf Information — als Anspruch des einzelnen gegen den Staat auf Information aus staatsbürgerlichen, politischen, historischen oder sonstigen Interessen, z. B. aus bloßer Neugier.
2. Grundrecht auf Information, die der einzelne zur Verteidigung seiner Ehre in Anspruch nimmt.

Im ersten Fall könnte man von Grundrecht auf Information im weiteren Sinn, im 2. Fall von Grundrecht

auf Information im engeren Sinne reden. Als verfassungsrechtliche Grundlage kommt für die erste Fallgestaltung Artikel 5 Abs. 1 GG, für die zweite Artikel 2 Abs. 1 GG in Frage. Dabei kann es für diesen zweiten Fall dahinstehen, ob es sich wirklich um ein Grundrecht im technischen Sinne handelt. Fest steht jedenfalls soviel, daß es Fälle betrifft, die im wesentlichen als Folge von Eingriffen in die allgemeine Handlungsfreiheit des Artikels 2 Abs. 1 GG relevant werden. In einer weiter- und tiefergehenden Untersuchung wäre zu überlegen, welche systematischen und dogmatischen Zusammenhänge zwischen dem hier sog. Grundrecht auf Information im engeren Sinne und dem Grundrecht auf Information im weiteren Sinne bestehen. Für den Zweck des Gutachtens bedarf dieses Problem keiner Entscheidung, da sich daraus für den Gesetzgeber keine Konsequenzen ergeben.

4.2. Einbeziehung bisheriger Ergebnisse

Diese Einteilung ist auch durch die bisherigen Ergebnisse des Gutachtens gerechtfertigt: Das gesamte staatliche Handeln läßt sich als Informationsverarbeitung durch öffentliche Stellen begreifen. Soweit durch öffentliche Stellen Individualinformationen verarbeitet werden, geht es um Rechtspositionen des einzelnen. Wie bereits oben gezeigt, sind dem Bürger in den einzelnen Phasen der Verarbeitung von Individualinformationen, Kontrollmitteilungen über Löschungen und Austausch von Individualinformationen usw. zuzuleiten. Dogmatisch sind sämtliche Ausgestaltungen dieser Informationspflichten des Staates, die 2. Fallgestaltung betreffend, eine Folge des Prinzips der freien Entfaltung der Persönlichkeit und somit aus Artikel 2 Abs. 1 GG hergeleitet.

Bisher nicht behandelt wurde Fallgestaltung (1.): Der Bürger begehrt Information über staatliche Tätigkeit aus lediglich nicht-rechtlichem, z. B. staatsbürgerlichem oder politischem, historischem oder sonstigem Interesse, also ohne Bezug auf irgendwelche Rechtspositionen. Dabei soll zunächst — zum Unterschied zum bisherigen Gutachten — für diese Fallgruppe dahinstehen, auf welche Informationen — ob nur Sachinformationen oder auch Personeninformationen — ein solcher Informationsanspruch des Bürgers (oder bestimmter Gruppen) gerichtet sein kann.

Als verfassungsrechtliche Grundlage kommt im Gegensatz zu den Informationsrechten der 2. Fallgruppe Artikel 5 Abs. 1 GG in Frage. Die Unterscheidung in Fallgruppe 1 und 2 ist daher auch wegen der verschiedenen verfassungsrechtlichen Grundlagen — Artikel 5 GG und Artikel 2 GG — geboten.

4.3. Beschränkung der weiteren Untersuchung

Im folgenden soll nur untersucht werden, inwieweit unsere Verfassung ein Grundrecht auf Information im weiteren Sinne anerkennt. Danach fragt es sich, ob der einzelne oder gesellschaftlich anerkannte Gruppen ein subjektiv-öffentliches Recht gegen den Staat haben, Informationen aus staatsbürgerlichem und sonstigem, d. h. nicht-rechtlichem Interesse zu erfahren.

5. Postulat eines allgemeinen Grundrechts auf Information

5.1. Prinzip der Öffentlichkeit

Man spricht heute viel vom „Prinzip der Öffentlichkeit staatlichen Handelns", vom Erfordernis eines generellen „Ansichtig- und Einsichtigmachens", dem „Gebot prinzipieller Öffentlichkeit der staatlichen Tätigkeit" [11]).

Ein Staat, dessen Gewalt vom Volke ausgeht, ist so gut und schlecht wie seine Bürger [12]). Demokratisches Staatsleben beruht darauf, daß der Bürger vom Staatsgeschehen weiß und nach seinem Wissen handelt. Zwar folgt aus der Information über das staatliche Geschehen nicht zwingend, daß er sich danach verhält. Information über Vorgänge und Zusammenhänge im Staatsleben ist jedoch erste Voraussetzung für die Bewährung des Bürgers als Staatsbürger im demokratischen Staat.

5.2. Tendenzen

Die Entwicklung moderner demokratischer Staaten ist durch zwei Tendenzen gekennzeichnet, die sogar der aktiven Teilnahme des einzelnen Staatsbürgers am Staatsgeschehen entgegenwirken: Der Staat benötigt einerseits für seine Zukunfts- und Wirtschaftsplanung immer mehr Unterlagen über die Persönlichkeit des einzelnen Staatsbürgers und über das Verhalten der gesellschaftlichen Gruppierungen. Durch die Vielzahl und Komplexität von Verarbeitungsmöglichkeiten von Informationen, die der Einsatz von EDV dem Staat in der öffentlichen Verwaltung bietet, entsteht die Gefahr eines vom Staat „total erfaßten Individuums". Entsprechendes gilt für die gesellschaftlich relevanten Gruppierungen. Zum anderen wird der Staatsapparat durch den Einsatz moderner Informationssysteme bei der öffentlichen Planung immer komplizierter und für den einzelnen undurchschaubarer, mag er auch „an sich" — d. h. für den Insider — an Rationalität und damit an Transparenz gewonnen haben.

Diesem doppelten Ungleichgewicht im Verhältnis Staat — Bürger kann nur dadurch Rechnung getragen werden, daß dem gesteigerten Interesse des Staates an der Person des einzelnen auf seiten des Bürgers mehr Information über das Verhalten des Staates, also mehr Einblick in das Staatsgeschehen entspricht. Einem mit Hilfe moderner Informationsmittel optimal informierten Staat muß das Äquivalent eines „informierten Bürgers" entgegengesetzt werden.

Unter diesem Aspekt läßt sich die von der Literatur wiederholt ausgesprochene Forderung rechtfertigen, daß die Staatsgewalt „grundsätzlich alle Erschei-

[11]) vgl. Ridder (2), 36
[12]) Windsheimer, 21

nungen ihres Dispositionsbereichs der Kommunikation zugänglich machen muß" [13]).

Es ist zu untersuchen, wieweit das GG dieser Forderung Rechnung trägt, ob nach der Verfassung ein allgemeiner staatsbürgerlicher Anspruch auf Information bereits gegeben ist oder erst vom Gesetzgeber normiert werden muß.

6. Artikel 5 Abs. 1 GG als mögliche verfassungsrechtliche Grundlage eines Grundrechts auf Information — bisherige Ansätze

6.1. Rechtsgrundlage

Als mögliche verfassungsrechtliche Grundlage eines Anspruchs des Bürgers (oder einzelner Gruppen) auf Informationsleistungen des Staates kommt Artikel 5 Abs. 1 GG in Frage, der das Verhalten des Staates in bezug auf die Information des Individuums wenigstens in einzelnen Phasen verbindlich normiert. (Artikel 21, 42 GG, als Normen, die die Staatsorganisation regeln, scheiden als Ansatzpunkt für ein Grundrecht aus.)

6.2. Enge Auslegung

Artikel 5 Abs. 1 GG gewährleistet für jedermann die Freiheit der Meinungsäußerung und Meinungsbildung, und gewährt den Massenmedien darüber hinaus Pressefreiheit und die Freiheit der Berichterstattung.

Nach dem bisherigen Verständnis von Artikel 5 GG hat die öffentliche Gewalt eine vielseitige, umfassende Information aller Glieder der Gesellschaft dadurch zu gewährleisten, daß sie hindernd oder fördernd eingreift, wenn Rechte Dritter, der Bestand des Staates oder die Funktionsfähigkeit seiner Organe bedroht sind oder wenn wirtschaftliche oder soziale Mächte innerhalb oder außerhalb des Staates den freien Informationsaustausch gefährden [14]).

Artikel 5 Abs. 1 GG geht davon aus, daß sich die geistige Kommunikation zwischen den Individuen unabhängig vom Staat vollzieht. Die Mitwirkung des Staates beschränkt sich darauf, den freien Informationsaustausch unter den Individuen zu achten und gegebenenfalls zu verteidigen.

Diese herkömmliche restriktive Auslegung hält sich streng an den Wortlaut des Artikels 5 Abs. 1 GG [15]). Nach dieser Auffassung ergibt sich für eine Verpflichtung des Staates zu direkten Informationsleistungen an einzelne oder Gruppen kein Anhaltspunkt. Zu Informationsleistungen an das Individuum, zu einer Offenlegung des Staatsgeschehens für den einzelnen Bürger, ist der Staat nur *indirekt* verpflichtet, nämlich über die Massenmedien, die den einzelnen über das Staatsgeschehen informieren sollen. Indem der Staat die Freiheit der Presse und Berichterstattung gewährleistet, genüge er seiner Pflicht dem Bürger Einblick in das Staatsgeschehen zu gewähren, damit er seinen staatsbürgerlichen Pflichten in einer Demokratie genügen kann.

6.3. Kritik

An dieser Auffassung wird immer häufiger Kritik geübt, weil sie verschiedene in modernen Demokratien auftretende Probleme nicht lösen kann.

Die herkömmliche restriktive Interpretation des Artikels 5 GG geht von der Trennung Staat — Gesellschaft aus, die von neueren Staatsrechtstheorien abgelehnt wird [16]).

Nach der Darstellung von Hesse [17]) wird die Durchdringung von Staat und Gesellschaft durch den sozialen Rechtsstaat bewirkt. Der Staat habe sich heute nahezu in alle gesellschaftlichen Bereiche hinein ausgedehnt, weil er weitgehend Voraussetzung für die Existenz der Gesellschaft geworden sei. Umgekehrt hätten wirtschaftliche und soziale Kräfte den Staat in ihren Bann gezogen. Daher sei eine Unterscheidung Staat/Gesellschaft als reale Trennung beider Größen heute weder von der gesellschaftlichen Wirklichkeit her noch von Rechts wegen möglich (wobei allerdings nicht übersehen werden darf, daß eine Reihe von Vorstellungen und Begriffen mit dem geschichtlich gewordenen Gegensatz Staat/Gesellschaft eng verknüpft ist). Die Rechtssätze des GG stammen in ihrer gegenwärtigen Formulierung und Zielsetzung vielleicht etwas abgewandelt und neugefaßt — aus der Weimarer Zeit oder noch weiter zurückliegenden Epochen des deutschen Staatslebens. Die gesellschaftliche Entwicklung ist über die Lage, in der sie entstanden sind, vielfach hinausgewachsen. Vor allem ist das gesellschaftliche Leben in der Bundesrepublik Deutschland heute vom Pluralismus der Kräfte geprägt, dessen Wesen das freie Nebeneinander vieler Strömungen und Richtungen ist.

Die bisherige Sicht des Artikels 5 GG — hier Staat, dort Gesellschaft (bzw. Individuum) — ist in Anbetracht dieser Erscheinungsformen des heutigen gesellschaftlichen Lebens zu extrem individualistisch. Sie trägt den verschiedenen Strömungen und Richtungen des Meinungsflusses, die von bestimmten sozialen Gruppierungen — wie Verbänden, Parteien, Interessengruppen aller Art — ausgehen, nicht Rechnung. Diese Institutionen außerhalb der Staatsorganisation, die sog. „intermediären Gewalten" [18]), versuchen die öffentliche Meinungsbildung zu steuern, indem sie in verstärktem Maße Einfluß nehmen auf die Massenkommunikationsmittel und auf diese Weise die Information des einzelnen gefährden [19]).

---

[13]) Windsheimer, 42
[14]) Maunz-Dürig-Herzog, Artikel 5 N. 82 ff.; v. Mangoldt-Klein, Artikel 5 N. II 3
[15]) Maunz, 113; Hamann-Lenz, Artikel 5 Nr. A 2
[16]) vgl. etwa Hesse (1), 70
[17]) a. a. O.
[18]) vgl. Windsheimer, 26. Die „Intermediären Gewalten" sind also insofern mit den bereits mehrfach erwähnten gesellschaftlichen Gruppen identisch.
[19]) Das ist seit dem Gutachten der „Günther-Kommission" auch in das Bewußtsein einer breiteren Öffentlichkeit gedrungen.

7. Versuch einer Neuinterpretation des Artikels 5 GG

7.1. Veränderte Stellung des Individuums

Damit ist auch die dem Artikel 5 GG zugrunde liegende Sicht des Individuums zu einseitig. Sie geht aus von der für die Rechtsauffassung des 19. Jahrhunderts typischen Vorstellung, daß das Recht lediglich die Freiheitssphären von Individuen gegeneinander abzugrenzen habe, und daß Gesetz und hoheitlicher Akt als Eingriff in die Freiheit immer legimitiert sein müßten aus dem Schutz der Freiheit anderer. Nicht berücksichtigt wird dabei die Eingliederung des Individuums in verschiedene Systeme, nicht nur im staatlich-politischen Bereich, sondern auch im sonstigen gesellschaftlichen Leben. Durch die Bindung des einzelnen in komplizierten, für ihn undurchschaubaren Systemen wird sein Freiheitsstatus gegebenenfalls ebenso geschwächt wie durch staatliche Eingriffe, weil er sich mangels genügenden Wissens von seiner Stellung im System von den Zusammenhängen und Auswirkungen nicht frei entscheiden kann.

Ein zeitgemäßes Rechtsverständnis muß dieser im Verhältnis zu den sozialen Gewalten veränderten und geschwächten Stellung des Individuums Rechnung tragen. Der einzelne muß seine durch Ungewißheit über die Struktur von Systemen eingeschränkte Freiheit dadurch wiedergewinnen, daß ihm das Recht Mitbestimmungs- und Informationsrechte bezüglich dieser Systeme gewährt — also nicht nur gegenüber dem Staat, sondern ebenso (oder noch mehr) gegenüber den anderen sozialen Gewalten.

7.2. Versuch einer Neuinterpretation

Die bisherige restriktive Auslegung des Artikels 5 GG hält deshalb einer Kritik auf die Dauer nicht mehr stand. Wenn der Staat sich darauf beschränkt, den Meinungsaustausch unter den Individuen zu schützen und zu achten und den Massenmedien den Informationsaustausch zwischen Individuum — Staat überläßt, ohne die Wirkungen der genannten Strömungen — wachsender Einfluß intermediärer Gewalten, Konzentrationsbewegungen bei den Massenmedien — einzubeziehen, können die Folgen für die Freiheit der Meinungsbildung und -äußerung des Individuums wie für die Freiheit der Presse und Berichterstaatung nicht ausbleiben. Darum soll eine Interpretation des Artikels 5 Abs. 1 versucht werden, die die angeführten gesellschaftlichen und staatlichen Entwicklungstendenzen berücksichtigt.

7.2.1. Objektive Auslegungsmethode

Anknüpfungspunkt ist der Wortlaut des Artikels 5 Abs. 1 [20]). Nach allgemeinen juristischen Auslegungsgrundsätzen kommt es auch bei der Auslegung von Verfassungssätzen auf den objektiven Sinn an (objektive Auslegungsmethode); maßgeblich ist, wie die Rechtssätze im Zeitpunkt der Auslegung zu verstehen sind (verstanden werden müssen), nicht wie sie von ihren Urhebern verstanden worden sind [21]). Die Gedanken des Gesetzesurhebers können dabei nur Anhaltspunkte neben anderen sein.

7.2.2. Wandlung der Massenmedien

Nach dem bloßen Wortlaut ist keineswegs klar, daß der Staat positive Informationsleistungen an den einzelnen erbringen muß. Der objektive Sinngehalt des Artikels 5 Abs. 1 GG ist jedoch vor dem Hintergrund unserer gegenwärtigen gesellschaftlichen und politischen Verhältnisse zu ermitteln. Danach hat der Staat die Freiheit der Meinungsbildung und Meinungsäußerung des einzelnen zu gewährleisten. Das bedeutet mit anderen Worten, er hat dafür zu sorgen, daß sich der einzelne, — unbehindert von Einflüssen Dritter — eine Meinung über die gesellschaftlichen und staatlichen Verhältnisse bilden und diese auch äußern kann. Insbesondere muß er sich eine eigene Meinung über das Staatsgeschehen machen dürfen und können.

Zu diesem Zweck kann sich der einzelne ungehindert aus „allgemein zugänglichen Quellen", d. h. zunächst über die Massenmedien unterrichten. Der Bestimmung des Artikels 5 Abs. 1 3. Alternative („... sich aus allgemeinen zugänglichen Quellen ungehindert zu unterrichten ...") liegt die Vorstellung zugrunde, daß die allgemeinzugänglichen Quellen dem Informationsanspruch des Bürgers auch genügen. Wie aber, wenn die Massenmedien ihrer Rolle als Informationsmittler zwischen Staat und Individuum nicht mehr genügen, weil sie vielleicht einseitig von intermediären Gewalten in *ihrer* Meinungsbildung beeinflußt werden, weil durch Konzentration der Einrichtungen bei wenigen privaten Geschäftsleuten eine gegenseitige Kontrolle vieler Meinungen nicht mehr gewährleistet ist, oder weil eine Information über die Massenmedien zur Unterrichtung des Bürgers über die immer komplizierteren staatlichen Vorgänge nicht mehr ausreicht?

Es ist derzeit sehr fraglich, ob die Massenmedien auf die Dauer unter dem Einfluß der intermediären Gewalten ihrem Auftrag als Informationsmittler zwischen Staat und Individuum genügen können. Wegen einer gewissen strukturellen Schwerfälligkeit sind sie durchaus solchen Gefährdungen ausgesetzt. Zwar sollte z. B. bei der Presse die privatrechtliche Struktur die Vielfalt des Angebots der Meinungen und damit auch die Freiheit der Meinungen garantieren. Beängstigende Konzentrationsbewegungen und der ständig wachsende Einfluß einiger weniger Personen und Konzerne im Pressewesen bestätigen, daß auf die Dauer die privatrechtliche Struktur der Presse als Korrektiv und Garant für die Vielfalt und Freiheit der Meinungen nicht mehr ausreicht.

7.2.3. Notwendigkeit neuer Informationsquellen

Wird aber die Freiheit der Meinungsbildung des einzelnen durch Einflüsse Dritter maßgeblich gestört, reichen also die „allgemein zugänglichen Quellen" umfassende und unbeeinflußte Information des Individuums nicht mehr aus, so bleibt dem Staat nichts anderes übrig, als selbst tätig zu werden und entweder neue „allgemein zugängliche Informations-

[20]) vgl. v. Mangoldt-Klein, N. A II 2 zu Artikel 5
[21]) Maunz, 49 ff.; Klug, 139

quellen" zu schaffen oder unmittelbar Informationsleistungen an das Individuum selbst zu erbringen. Denn das Grundrecht der freien Meinungsäußerung und Meinungsbildung läuft leer, wenn der Staat nicht für das Funktionieren des freien Meinungsaustausches und der ungehinderten (und ungetrübten) Unterrichtung durch Gewährleistung allgemein zugänglicher Quellen Sorge trägt. Seine Achtungs- und Schutzfunktion muß in ein positives Tun umschlagen, sobald für den freien Austausch und die freie Bildung der Meinungen der Staatsbürger die gesellschaftliche Grundlage fehlt.

7.3. Der Zusammenhang mit anderen Verfassungsnormen

Nach allgemeiner Auffassung [22]) kommt Artikel 5 GG als Grundrecht der Meinungsfreiheit zentrale Bedeutung zu als der Grundlage für das Funktionieren demokratischen Staatslebens in der Bundesrepublik Deutschland überhaupt. Der Inhalt der Meinungsfreiheit erschöpft sich nach diesem neueren Verständnis von Artikel 5 GG nicht darin, daß der einzelne das Recht hat, seine Meinung frei zu äußern und zu bilden und daß die Rolle der Staatsgewalt dabei darauf beschränkt ist, den freien Informationsaustausch zu achten und gegebenenfalls zu schützen. Der eigentliche Wert, den Artikel 5 GG realisieren will, ist die Denkfreiheit. Artikel 5 GG gewinnt diese zentrale Bedeutung für das Funktionieren demokratischen Staatslebens, wenn man ihn im Zusammenhang mit anderen Normen der Verfassung sieht, die das Informationsverhalten des Staates normieren. Das BVerfG hat wiederholt festgestellt, daß das Verfassungsrecht nicht nur aus einzelnen Sätzen der geschriebenen Verfassung bestehe, sondern aus „gewissen sie verbindenden, innerlich zusammenhaltenden allg. Grundsätzen und Leitideen, die der Verfassungsgeber, weil sie das vorverfassungsmäßige Gesamtbild geprägt haben, von dem er ausgegangen ist, nicht in einem besonderen Rechtsakt konkretisiert hat [23]). Aus der Existenz solcher Verfassungsgrundsätze folgt, daß die einzelnen Verfassungsbestimmungen nicht mehr isoliert betrachtet und allein aus sich heraus interpretiert werden können. Danach ist es zulässig, die Normen, die das Informationsverhalten des Staates regeln zu einer „Gesamtschau" [24]) zu verbinden, um daraus weitere Gesichtspunkte für die Interpretation des Artikels 5 Abs. 1 GG zu gewinnen.

7.3.1. Artikel 21 und 42 Grundgesetz

Neben Artikel 5 Abs. 1 GG beziehen sich nur Artikel 42 Abs. 1 und 3 GG und Artikel 21 Abs. 1 GG auf die Information der Allgemeinheit.

Artikel 21 GG besagt, daß die Parteien bei der politischen Willensbildung des Volkes mitwirken.

Artikel 42 GG verankert den Grundsatz der Parlamentsöffentlichkeit.

Artikel 42 Abs. 1 GG verpflichtet den Staat, ein Stück seiner selbst der allg. Wahrnehmung preiszugeben. Artikel 42 Abs. 3 GG („Wahrheitsgetreue Berichte über die öff. Sitzungen des Bundestags und seiner Ausschüsse bleiben von jeder Verantwortlichkeit frei") stellt die Verbindung zwischen Artikel 42 Abs. 1 und Artikel 5 Abs. 1 GG insofern her, als er die Kommunikation des Staates durch die Träger der staatsfreien Kommunikation gewährleistet. Artikel 21 Abs. 1 Satz 4 GG („Die Parteien müssen über die Herkunft ihrer Mittel öffentlich Rechenschaft geben") verlangt vom Staat, von ihm unabhängige Dritte, die Parteien, zu verpflichten, sich der Allgemeinheit darzustellen.

Diese Normen sind nicht abschließende, unabhängig nebeneinander stehende Spezialregelungen, Ausprägungen eines allg. Grundsatzes, von dem der Verfassungsgeber ausgegangen ist, ohne ihn ausdrücklich zu formulieren.

In der Literatur werden die genannten Bestimmungen in Verbindung mit Artikel 5 GG zwar restriktiv ausgelegt, doch wird zugleich anerkannt, daß darüber hinaus Bindungen für die Staatsgewalt bestehen, die sich aus der der jeweiligen Zweckrichtung der Normen ergeben. Diese „Zweckrichtung" bei Artikel 42 GG und Artikel 21 GG [25]) besagt, daß es nicht genügt, wenn der Staat den freien Austausch von Meinungen toleriert, also hier dem einzelnen freien Zutritt zu den Parlamentssitzungen gewährt. Vielmehr muß der Staat *selbst* etwas tun, um das Staatsgeschehen für den einzelnen transparent zu machen. Das bedeutet, daß die einschlägigen Normen das Informationsverhalten des Staates zwingend auf ein bestimmtes, einzuhaltendes Maß festlegen (etwa im Hinblick auf die Form der Publizität in Artikel 42 Abs. 1 GG, auf die Art und Weise des Informationsempfangs des einzelnen bei Artikel 5 Abs. 1 Satz 1, zweiter Halbsatz GG — mindestens aus allgemein zugänglichen Quellen, bezüglich des Informationsgehalts bei Artikel 21 Satz 4 GG — mindestens Rechnungslegung bezüglich der Finanzquellen); daß darüber hinaus die Verfassung zwar nichts zwingend vorschreibt, was aber nicht bedeutet, daß sich die Staatsgewalt willkürlich verhalten kann. Sie ist vielmehr in ihrem darüber hinausgehenden „Informationsverhalten" gegenüber dem einzelnen an die Verfassungssätze gebunden, die den Wertgehalt des GG bestimmen.

7.3.2. Demokratieprinzip

Ein solcher dem Wertgehalt des GG bestimmender Verfassungssatz ist das in Artikel 20 Abs. 2 GG verankerte *Demokratieprinzip* [26]). In einer repräsentativen Demokratie — wie der Bundesrepublik Deutschland — ist das Volk — als Gesamtheit der Bürger — zwar Träger der Staatsgewalt, an der Ausübung der Staatsgewalt jedoch nur durch die Mitwirkung seiner „Aktivbürger" in Wahlen und Abstimmungen beteiligt. Unbeschränkt ist dagegen die Mitwirkung der einzelnen Bürger an der politischen Willensbildung. Wegen dieser Beschränkung des Bürgers in seiner aktiven Mitwirkung im Staatsge-

---

[22]) Stein, 117; Windsheimer, 64; BVerfGE 7, 208 und 12, 125
[23]) BVerfGE 2, 280, 380
[24]) Windsheimer, 36
[25]) vgl. Windsheimer, a. a. O.
[26]) BVerfGE 1, 14

schehen — im Vergleich zur unmittelbaren Demokratie — kommt in der repräsentativen Demokratie der freien geistigen Kommunikation erhöhte Bedeutung zu. Allgemeine Zugänglichkeit und Öffentlichkeit der freien Kommunikation ist das Medium, in dem sich die politische Willensbildung vollzieht [27]).

Die Grundentscheidung für die repräsentative Demokratie bedeutet deshalb zugleich eine Entscheidung für die Meinungsfreiheit, Pressefreiheit, für eine vom Staat unabhängige Bildung der öffentlichen Meinung. Eine freie Meinung über das Staatsgeschehen kann sich der einzelne nur bilden, wenn er weiß, was geschieht. Eine freie geistige Kommunikation erfordert daher Information über das Staatsgeschehen. D. h., der Staat muß dafür sorgen, daß sich der gesamte öffentliche Bereich (auch Körperschaften und Anstalten des öffentlichen Rechts) der Öffentlichkeit erschließen läßt. Das bedeutet, daß der Staat dem Individuum gegenüber unter Umständen zu eigenen Informationsleistungen verpflichtet ist, wenn der bisherige Informationsaustausch zwischen Staat und Individuum mittelbar über die Massenmedien den Anforderungen einer modernen repräsentativen Demokratie nicht mehr genügt.

7.3.3. Sozialstaatsprinzip

Es bleibt zu fragen, ob nicht das Sozialstaatsprinzip (vgl. Artikel 20 Abs. 1, Artikel 28 GG) bei aller gebotenen Vorsicht auch zur Begründung der hier vorgetragenen Ansicht mit herangezogen werden kann: Zwar betrifft dieses Prinzip vor allem „die Verpflichtung (des Staates) zur Hilfeleistung in sozialen Notlagen" [28]), stellt also vor allem für die Wirtschaftspolitik bestimmte Grundsätze auf. In seinem Grundgedanken, der erstmals von H. Heller [29]) formuliert wurde, geht es jedoch davon aus, daß die formal gleiche Freiheit aller sehr leicht zum Recht des Stärkeren werden kann, wenn die sozialen Machtverhältnisse unberücksichtigt bleiben. In dieser Grundbedeutung erscheint das Prinzip über den Bereich der Wirtschaft hinaus auf Fälle der vorliegenden Art hin ausbaufähig, wenn man sich einmal dahin geeinigt hat, daß „die Mitverantwortung des Staates für die Beteiligung seiner Bürger" [30]) nicht nur den wirtschaftlichen Bedarf umfaßt. Damit ist die Notwendigkeit für positive Informationsleistungen des Staates an den Bürger in dem Augenblick gegeben, in dem die gesellschaftlichen Verhältnisse wegen Einflüsse und Entwicklungen, (die der Verfassungsgeber noch nicht gekannt hat), eine ungehinderte Information des Individuums und einen unbeeinflußten Informationsaustausch nicht mehr ohne weiteres zuläßt.

[27]) Nach Windsheimer, 40 ist sie die „nicht-organisierte letzte Instanz der Demokratie".
[28]) Stein, 175
[29]) zit. nach Stein, 175
[30]) Stein, a. a. O.
[31]) vgl. in diesem Zusammenhang die Literatur zum „stillen Verfassungswandel", etwa Maunz, 58; v. der Heydte, 461, 466; BVerfGE 2, 401 und 3, 422.
[32]) S. 158
[33]) Steinbuch (1), 282
[34]) Windsheimer, 159

7.4. Bedeutungswandel des Artikels 5 GG

Die Heranziehung der Normen des GG, die das Informationsverhalten des Staates regeln, sowie des Demokratie- und Sozialstaatsprinzips bedeutet für die Interpretation des Artikels 5 GG:

Die Freiheit der Meinungsbildung und Meinungsäußerung gewinnt im Zusammenhang mit Artikeln 21, 42 GG und im Licht dieser den Wertgehalt der Verfassung bestimmenden Verfassungsansätze zentrale Bedeutung für das Verfassungsleben überhaupt (als eine Grundnorm demokratischen Staatslebens). Wenn Artikel 5 Abs. 1 mit Hilfe dieser „elementaren Verfassungssätze" interpretiert wird, dann ist Artikel 5 GG auch den Erfordernissen eines demokratischen Staates der Gegenwart sowie dem der heutigen Zeit entsprechenden Menschenwürdegehalt des Artikels 1 Abs. 1 GG anzupassen: Artikel 5 GG darf nicht länger restriktiv vom Wortlaut her interpretiert werden. Aus dem Demokratie- und Sozialstaatsprinzip sowie aus Artikel 1 Abs. 1 GG läßt sich eine Verpflichtung des Staates zu positiven Informationsleistungen an das Individuum vertreten. Man spricht bei Artikel 5 GG in der Literatur von einem *Bedeutungswandel* zu einer zentralen Norm der Verfassung [31]). Im Ergebnis bleibt festzuhalten: Artikel 5 GG gewährt dem Bürger (und bestimmten Gruppen) einen Anspruch auf unmittelbare, positive Informationsleistungen, damit also ein Grundrecht auf Information.

8. Ausgestaltung eines Grundrechts auf Information

Welche Ausgestaltung ein grundrechtlicher positiver Anspruch des Bürgers auf Information (gegen den Staat) erfährt, hängt von der Entwicklung der staatlichen Einrichtungen und der gesellschaftlichen Lebensbedingungen ab. In gewissem Sinne läßt sich ein solcher Informationsanspruch bereits heute realisieren, entgegen der Auffassung Windsheimers [32]), der die Realisierung eines solchen Rechts nur unter einer von zwei Bedingungen für denkbar hält; entweder die Mehrheit der Staatsbürger macht von diesem Recht keinen Gebrauch, oder der Staat schafft Einrichtungen, etwa zentrale Informationsbanken [33]), mit deren Hilfe das Bedürfnis einer wahrhaft informierten Gesellschaft befriedigt werden könnte [34]).

8.1. Beispiele

Die neueste Entwicklung in der öffentlichen Verwaltung beweist gerade das Gegenteil. Es ist kein Zufall, wenn in der Kommunalverwaltung, besonders in größeren Städten (z. B. Köln), aber auch auf Landesebene (z. B. Hessen) sog. allgemeine Auskunftstellen für den Bürger errichtet werden, wo der einzelne ohne Nachweis eines besonderen Interesses Auskunft über Fragen der öffentlichen Verwaltung oder des Staatsgeschehens allgemein erhalten kann, soweit nicht Interessen Dritter oder das Staats- oder Amtsgeheimnis entgegenstehen. Die Praxis beweist

oft ein gewisses Gespür für gewisse Notwendigkeiten.

8.2. Informationsinteresse

Bei der Frage nach dem „Wie" der praktischen Verwirklichung des grundrechtlichen Anspruchs des Bürgers auf Information sind zunächst die Interessen des Bürgers im Hinblick auf die einzelnen Phasen staatlicher Datenverarbeitung zu berücksichtigen. Sie beziehen sich vor allem auf Sachinformationen. Bei der Verarbeitung von Sachinformationen durch öffentliche Stellen ist für den Bürger die Phase der Ermittlung wohl kaum von Interesse, ebensowenig das Erfassen. Am meisten interessiert ihn zu wissen, was öffentliche Stellen an Sachinformationen speichern, was mit Informationen im weiteren geschieht, an welche anderen Stellen sie weitergegeben werden, ob an andere Behörden oder an Dritte; somit sind für den Bürger bei Sachinformationen insbesondere die Phasen der Speicherung, Veränderung, Weitergabe und Austausch sowie Löschung von Bedeutung.

8.3. Befriedigungsformen dieses Interesses

Entsprechend den technischen Möglichkeiten ist an verschiedene Formen zu denken, in denen die Informationspflicht des Staates gegenüber dem Bürger befriedigt werden könnte:

- Auskunftserteilung über das Staatsgeschehen über allgemeine Auskunftsstellen;
- Zugang zu gewissen staatlichen Einrichtungen; diese könnten auch als „allgemein zugängliche Informationsquellen" i. S. von Artikel 5 Abs. 1 GG erklärt werden;
- direkte Informationen, Aufklärung über das Staatsgeschehen an den einzelnen, wobei sich der Staat der Massenmedien bedienen kann;
- Schaffung neuer Informationsmittler zwischen Staat und Individuum bei fortschreitender Entwicklung der Technik;
- Errichtung von Informationsbanken für den Bürger (als allgemein zugängliche Informationsquellen im Sinne des Artikels 5 Abs. 1 GG) [35].

Weitere Formen eines Informationsaustausches zwischen Staat und Bürger sind bei fortschreitender Technisierung der Verwaltung denkbar.

8.4. Realisierungsmöglichkeit

Bei der Realisierung des verfassungsrechtlichen Informationsanspruchs des Bürgers ist der gegenwärtige Stand der öffentlichen Verwaltungseinrichtungen und dabei auch die Frage der Finanzierung eventuell zu schaffender staatlicher Informationseinrichtungen zu berücksichtigen. Die erwähnte bahnbrechende Entwicklung in der Kommunalverwaltung — Errichtung von Auskunftszentren für den Bürger — ist zugleich richtungsweisend. Beim gegenwärtigen Stand der öffentlichen Verwaltung ist die Errichtung allgemeiner Auskunftsstellen für den Bürger auf breiterer Basis in der gesamten öffentlichen Verwaltung durchaus möglich, ohne daß dadurch der staatliche Finanzhaushalt zu sehr beansprucht würde. Schließlich soll die gesamte öffentliche Verwaltung dem Bürger dienen. Auch ein unmittelbares Herantreten des Staates an den Bürger mit Informationen über das Staatsgeschehen wäre ohne allzu großen Aufwand möglich. Dabei kann sich der Staat der bestehenden Kommunikationsmedien bedienen. Diese Form der Kommunikation wird von den Parteien bereits praktiziert. Zu dem bisherigen Zustand der Informationsvermittlung durch die Massenmedien zwischen Staat und Individuum besteht der grundlegende Unterschied, daß der Staat die öffentliche Meinungsbildung über die Erscheinungen in seinem Bereich nicht den Massenmedien überläßt, sondern selbst tätig wird und Informationen aus seinem Bereich selbst, über seine Behörden an das Individuum heranbringt. Damit wäre der Anfang gemacht für einen „bürgernahen Service", der als oberstes Ziel der Verwaltungsreform genannt wird. Von dem Fortschreiten der Verwaltungsreform wird es abhängen, wann dem Bürger ein zentrales Informationssystem zur Verfügung stehen wird, mit deren Hilfe das Informationsbedürfnis einer informierten Gesellschaft vollends befriedigt werden kann.

9. Träger des Informationsanspruchs

9.1. Bürger

Träger des Grundrechts auf Information ist zunächst jeder Bürger. Die an den einzelnen unmittelbar vom Staat erbrachten Informationsleistungen sollen dazu dienen, daß er — durch mehr Wissen über den Staat — seinen staatsbürgerlichen Pflichten besser genügen und aktiv am demokratischen Staatsleben teilnehmen kann.

9.2. Gruppen

Anspruch auf Information haben gleicherweise auch Gruppen, Interessenverbände, Parteien, die nicht im Bundestag oder Landtag vertreten sind. Gerade von dieser Seite ist ein stärkeres Interesse an allen möglichen Sachinformationen zu erwarten als vielleicht vom einzelnen Bürger, der u. U. zu träge ist, um von seinem Informationsrecht häufig Gebrauch zu machen. Es läßt sich denken, daß der Obstzüchterverband XY z. B. Informationen über den Baumbestand in der Bundesrepublik haben möchte, daß die Partei Z, die in den Landtag kommen möchte, bestimmte statistische Unterlagen über die Bevölkerungsstruktur im Land B wünscht, daß der Sportverein V. wissen möchte, wie viele Sportvereine in einem bestimmten Gebiet tätig sind, wie viele Mitglieder sie haben u. ä. Die Reihe der Beispiele ließe sich beliebig fortsetzen. Es soll nur verdeutlicht werden, daß derlei Interessengruppen ein vermehrtes Interesse an Informationserteilung haben werden und in diesem Sinne der grundrechtliche Anspruch auf Informationserteilung erst Gewicht erhält.

[35] vgl. schon Steinmüller (1), 84

10. Umfang des Informationsanspruchs und der zu erteilenden Informationen

Bei der Frage, wieweit der Staat bei der Informationserteilung an den Bürger (bzw. bestimmte Gruppen) gehen darf, d. h. welche Informationen der einzelne (oder bestimmte Gruppen) vom Staat vernünftigerweise verlangen kann, ist zurückzugreifen auf die beiden Unterscheidungen zwischen Personen und Sachinformationen einerseits, Informationsansprüche aus rechtlichem und nichtrechtlichem Interesse andererseits. Informationsansprüche aus besonderem Interesse (wegen Gefährdung bestimmter Rechtspositionen des Bürgers) betreffen vorwiegend Individualinformationen (des einzelnen oder eines Dritten). Insofern wurden diese Informationsansprüche bereits verfassungsrechtlich Artikel 2 Abs. 1 GG zugeordnet. Informationsansprüche aus nichtrechtlichem (staatsbürgerlichem, politischem, historischem oder sonstigem) Interesse — verfassungsrechtlich aus Artikel 5 GG begründet — können Personen oder Sachinformationen zum Gegenstand haben, sowohl individueller wie statistischer Art.

Anfragen an zuständige Behörden und Auskunftsstellen werden oft gemischter Natur sein, d. h. Informationswünsche sowohl aus rechtlichem (zur Geltendmachung bestimmter Rechtspositionen) oder aus allgemeinem, d. h. staatsbürgerlichem Interesse, gerichtet auf Personen — oder Sachinformationen oder auf beide. Da es dem Bürger lediglich darum geht, daß ihm die gewünschte Information erteilt wird, ist es Aufgabe des zuständigen Verwaltungsbeamten zu prüfen, ob und aufgrund welcher Rechtsnorm er die gewünschte Information geben darf, und in welchem Umfang.

Dem Gesetzgeber bleibt es überlassen, inwieweit er auf der verfassungsrechtlichen Grundlage der Artikel 2 Abs. 1 und 5 Abs. 1 GG die *gesetzlichen Voraussetzungen* für die erforderlichen Informationseinrichtungen schafft.

11. „Drittwirkung"

Artikel 5 Abs. 1 GG gehört unbestritten zu den Grundrechten, die auch Rechtswirkungen im außerverfassungsrechtlichen Bereich, sog. Drittwirkung entfalten [36]).

Wenn auf der Grundlage des Artikels 5 Abs. 1 GG ein Grundrecht auf Information (i. e. S.) angenommen wird, dann muß auch ein solches Grundrecht Drittwirkung haben.

Die Drittwirkung von Grundrechten ist jedoch nur relevant für bereits geltende Rechtsvorschriften. Die Grundrechte wirken mittelbar in die Privatrechtsordnung hinein, indem vom Richter unbestimmte Rechtsbegriffe und Generalklauseln des Privatrechts am Wertgehalt des GG gemessen und damit vom Verfassungsrecht her ausgefüllt werden [37]).

Bei zu erlassenden Rechtsvorschriften bedarf es keiner eigentlichen Drittwirkung. Denn der Gesetzgeber kann Gesetze so fassen, daß sie verfassungsrechtlichen Gesichtspunkten Rechnung tragen. Bei dem Entwurf eines Datenschutzgesetzes muß darum der Gesetzgeber den Gedanken der Drittwirkung eines Grundrechtes auf Information berücksichtigen. Wegen der Gleichartigkeit der Auswirkungen von Informationssystemen im privaten und öffentlichen Bereich empfiehlt es sich, bei der Regelung privater Informationssysteme die entwickelten Gesichtspunkte für öffentliche IS miteinzubeziehen.

[36]) v. Mangoldt-Klein, Vorb. zu Artikel 5 Nr. A II 4 d
[37]) Maunz, 99

Exkurs II: Datensicherung

1. Problematik des Datenschutzes unter dem Aspekt des Einsatzes der EDV

1.1. Allgemeines

Im Gutachten ist bewußt von Informationsverarbeitung und nicht von Datenverarbeitung gesprochen worden, nicht zuletzt, um die Problematik der synonymen Verwendung von IV, ADV, DV, EDV und Computer zu umgehen, bzw. um Abgrenzung und Definition zu ermöglichen.

Dabei erfolgt diese landläufige synonyme Verwendung in gewissem Sinne zurecht:

Bedeutsames Mittel der Informationsverarbeitung und wichtigstes der ADV ist der Computer, bzw. wird es werden.

Bundesmeldegesetz, die Länderinformationssysteme[1]) und die Wirtschaft sehen die EDV als Organisationsmittel vor.

Am „Siegeszug" des Computers ist nicht zu zweifeln. Wenn also Datenschutz effektiv werden soll, muß er speziell im Hinblick auf den Einsatz des Computers realisierbar sein. Ist es schon immer ein Problem, Lebenssachverhalte im Gesetz so zu formulieren, daß Entwicklungen das Gesetz nicht obsolet machen, besteht diese Schwierigkeit ganz besonders für den Bereich der Technik. Gerade die EDV befindet sich in einer ausgesprochen schnellen Entwicklung. Bestand schon immer ein Dilemma „Recht und Fortschritt" [2]), so ist dies erst recht für sich schnell

[1]) Bayerisches Informationssystem; Großer Hessenplan; u. a.
[2]) Steinmüller (1), 3

entwickelnde Gebiete der Technik zu beobachten. Dabei ist nicht nur eine ständige Fortentwicklung der Computer*technik* zu verzeichnen [3]), sondern auch ein rapides Zunehmen der Anzahl und der Qualität der zu automatisierenden *Aufgaben* [4]).

1.2. Recht und technischer Fortschritt

Will der Datenschutz nicht leer laufen, muß er effektiv und praktikabel sein. Folgende Bedingungen sind dabei zu erfüllen:

1. Um wirkungsvoll zu schützen, muß er den spezifischen Gefahren der EDV Rechnung tragen.
2. Die Forderungen dürfen nicht auf eine Unmöglichkeit des Computereinsatzes oder eine wesentliche Erschwerung hinauslaufen, müssen also die „Chancen" wahren [5]).
3. Er muß dem technischen Fortschritt Rechnung tragen, d. h. zukunftssicher sein (weder die Entwicklung hemmen noch durch sie obsolet werden).

Die geistige Grundhaltung, die zur Formulierung solcher Tatbestände erforderlich ist, ist nicht typisch für den Juristen. Sie muß offen für den technischen Fortschritt sein [6]), den neuen Sachverhalten Rechnung tragen [7]), ohne sich dabei nur von den Gegebenheiten die Handlungsweise aufzwingen zu lassen.

Der neue Sachverhalt ist hier die qualitativ neue Dimension der Information durch den Einsatz der EDV [8]).

Das Recht hat auch steuernde Funktion und darf sie nicht durch neue Entwicklungen verlieren [9]). Gerade der Computer befindet sich aber in einer äußerst raschen Entwicklung und ist überhaupt ein neues Medium.

Der Computer ist „Chance und Gefahr" zugleich [10]). Der Datenschutz soll die Gefahr bannen, ohne die Chance zunichte zu machen. Um dem Datenschutz in diesem Sinne zur Geltung zu verhelfen, also die Anforderungen des Datenschutzes beim Einsatz der EDV realisierbar und praktikabel zu gestalten, muß man untersuchen, welche Gegebenheiten der Computer mit sich bringt.

1.3. Gegebenheiten des Einsatzes der EDV

Aus den Planungen der verschiedenen Anwendungsfälle in Verwaltung und Wirtschaft kann eindeutig eine Entwicklung zur *integrierten Datenverarbeitung* festgestellt werden [11]). Ohne auf die Fragen des Verhältnisses von technischer und organisatorischer Integration und ihrer verschiedenen Varianten und der von ihr erfaßten Gebiete eingehen zu wollen [12]), sollen die Wesensmerkmale der Integration herausgestellt werden, so wie sie sich derzeit darstellen:

1. Zusammenfassung der Arbeiten verschiedener Stellen in einem Arbeitsablauf [13]),
2. möglichst Einmal-Führen der Datenbestände [14]),
3. viele Benutzer verkehren mit dem System [15]) (Datenfernverarbeitung, time-sharing),
4. Möglichkeiten der Auswertung der Datenbestände unter verschiedenen Aspekten [16]) durch Vollständigkeit der Daten und Komplexität des Systems.

Etwas abstrakter: Intergration ist Aufhebung der Arbeitsteilung [17]) und damit eventuell des Ressorts- bzw. Gewaltenteilungsprinzips.

Theoretisch gibt es Integration ohne elektronische DV. In der Praxis wird die Integration durch die Möglichkeiten der EDV geprägt [18]):

— Großspeicher mit kurzen Zugriffszeiten und wahlfreiem Zugriff (Random),

— times-haring (Teilnehmerrechnersysteme),

— Datenfernverarbeitung,

— optimierter Einsatz des teuren Mediums Computer durch Vermeidung von Mehrfacharbeiten.

Isolierte und ressortgebundene EDV ist nicht nur teuer, läuft also einem Grundgedanken der Rationalisierung — der Kostensenkung — zuwider, sondern verhindert es auch, eine Fähigkeit des Systems auszunutzen, die Zweck des Einsatzes ist:

> durch repräsentative, aktuelle und schnelle Auswertungen zu qualifizierten Führungs- und Planungsentscheidungen zu kommen [19]).

Bei isolierter Automation mit EDV kann nicht die Vollständigkeit der Datenbestände und damit nicht die Komplexität erreicht werden [20]), die Grundlage für repräsentative Auswertungen sind.

Dabei baut die Integration als eine Phase der Entwicklung der DV auf die erste Phase, die Automation einzelner Gebiete, auf [21]). Sie gewinnt ihre Daten aus der operativen Ebene, z. B. dem Verwaltungsvollzug, der in der ersten Phase automatisiert wurde.

---

[3]) z. Z. 3. Generation, integrierte Schaltkreise in Monolithtechnik
[4]) z. B. Funktionskatalog der KGSt; Scheubel, 19 ff.
[5]) bisher wenig bekannt bzw. erkannt; vor allem amerikanische Literatur „Computer and Privacy" vorhanden
[6]) Steinmüller (1), 3
[7]) Luhmann (4), 31
[8]) Siemens AG (1), 2; Meincke, 34; Jakob, 23
[9]) Steinmüller (1), 4
[10]) vgl. den Titel des Aufsatzes von Simitis: Chancen und Gefahren der EDV
[11]) EBMeldeG, Bayerisches Informationssystem, Großer Hessenplan, Management — Informationssysteme (MIS)
[12]) vgl. Steinmüller (1), 71 ff.; Definition bei Meincke, 32
[13]) Meincke, 30; Auernhammer (1), 23
[14]) Siemens AG (1), 41
[15]) IBM, 6; Klett, 100; Ruggles, 101; Giloi, 6
[16]) Meincke, 32; Klett, 98; Giloi, 4
[17]) Steinmüller (1), 71
s. auch Hessische Zentrale für Datenverarbeitung, 10: Grundforderung 2
[18]) Meincke, 26: „quantitative Steigerung der Möglichkeiten"; Steinmüller (1), 74: „eigentlicher Motor"; Hessische Zentrale für Datenverarbeitung, 11, Grundforderung 7
[19]) Siemens AG (1), 2; Meincke, 75
[20]) Hessische Zentrale für Datenverarbeitung, 10
[21]) Scheubel (1), 19

Deutlich kommen beide Ziele des EDV-Einsatzes im Bayerischen EDV-Gesetz in Artikel 1 zum Ausdruck [22]).

Als *Ergebnis* kann festgestellt werden:

Die Integration ist ein Phänomen, das neue Kontroll- und Steuerungsmechanismen erfordert, da die alte Form der Arbeitsteilung entfällt.

Durch die Erledigung mehrerer zusammenhängender Arbeiten in einem Schritt werden z. B. Normierungen erforderlich, da viele Stellen mit dem gleichen System arbeiten [23]). Die einzelnen Daten werden möglichst verschlüsselt, um Speicherplatz zu sparen und sie operabel zu machen.

Ihre Komplexität gewinnt die Information durch die potenzierte Möglichkeit der Auswertung in integrierten Informationssystemen [24]).

Dem Grad der Komplexität entspricht die potentielle Bedrohung des einzelnen [25]). Für die „sensitivity" einer Information ist der Kontext entscheidend, in dem sie zuerst eingegeben wurde und in dem sie später benutzt wird [26]). Daraus resultiert die Qualität der Information für Planung und Entscheidung, aber auch die Transparenz der in den Datenbeständen erfaßten Objekte.

Unter dem Gesichtspunkt des Datenschutzes ist deshalb zu fragen, welche Möglichkeiten bestehen, vor den negativen Folgen der IV zu schützen, wobei die spezifischen Gefahren des Computer-Einsatzes zu berücksichtigen sind. Kennt man diese Gefahren, kann man Möglichkeiten aufzeigen, sie zu bannen.

Im folgenden sollen deshalb die spezifischen Gefahren des Computers dargestellt werden.

1.4. Notwendigkeit der Datensicherung

Information mit Hilfe des Computers ist teuer: Große Datenbestände erfordern viel Speicherplatz, aufwendige Programme benötigen große Rechenwerke (Zentraleinheiten). Durch Verschlüsseln der Daten wird deshalb versucht, möglichst wenig Speicherplatz zu belegen. Der Umfang der Programme wird möglichst klein gehalten. Die Benutzerzeit soll möglichst gering sein.

Um Fehler verhindern bzw. erkennen und korrigieren zu können, müssen Anlagen, Programme, Daten umfangreicher sein. U. U. sind weitere Maßnahmen erforderlich (Organisation, Personal).

Das bedeutet, daß Sicherheit das System noch teurer macht. Aus diesem Grund wird in der Wirtschaft abgewogen:

> Gewicht von Schäden und Mißbrauch gegenüber den Kosten für Sicherheit [27]).

Ob diese Abwägung zulässig ist, wenn der Schaden in einem Eingriff in grundrechtlich geschützte Güter, wie das Persönlichkeitsrecht, besteht, kann hier nur als Frage erörtert werden. Im Rahmen dieser Untersuchung geht es darum festzustellen, welche Folgen das Fehlen von Sicherheitsvorkehrungen haben kann, so daß Maßnahmen zur Sicherung erforderlich sind.

Es wird davon ausgegangen, daß Verwaltung [28]) und Wirtschaft [29])) personenbezogene Daten in Datenbanken so speichern, daß sie nach verschiedenen Kriterien ausgewertet werden können. Da sich viele Stellen mit den gleichen Objekten — Personen — befassen, werden diese Daten nur einmal so geführt, daß jede Stelle die bei ihr anfallenden Daten erfaßt und abspeichert. Der Abruf bzw. die Auswertung erfolgt ebenfalls von verschiedenen Stellen [30]).

Bei jedem Umgang mit einem Datum bestehen Fehlermöglichkeiten (Erfassung, Speicherung, Übertragung, Verarbeitung und Ausgabe); zudem können Unberechtigte versuchen, Zugang zu den Daten zu erhalten.

Die Frage nach der Berechtigung erhält zwei Komponenten:

1. ob der betreffenden Stelle/Person überhaupt der Umgang mit dem Datum erlaubt ist,
2. ob der Umgang in dem Zusammenhang mit der Suchfrage, dem Kontext erlaubt ist (u. U. nur zusammen mit anderen Daten [31]) oder anderen Suchfragen). Denn für die Bedeutung eines isolierten Datums ist der Zusammenhang, in den es im System gestellt wird (z. B. Bezeichnung des Datenfeldes, Art der Datei) und in dem es wiederauffindbar ist, maßgebend.

Während grundsätzlich das Interesse des die Daten Verwaltenden darüber bestimmt, wie sicher sein System sein soll, hat bei den personenbezogenen Daten ein Außenstehender, der durch die Daten „erfaßte" Mensch, ein Interesse an der Richtigkeit, Vollständigkeit der Daten und dem Schutz vor unberechtigtem Umgang. Dieses „Interesse" wird als generelle Datenschutzproblematik im Gutachten behandelt. Für den Bereich der Erfassung in EDV-Systemen können die Forderungen nach Richtigkeit, Vollständigkeit und unberechtigtem Umgang durch entsprechende Sicherungsmaßnahmen erfüllt werden.

1.5. Definition [32])

Datensicherung ist die Menge aller Maßnahmen — technische, programmtechnische (hard- und softwaremäßig), organisatorische, personelle und sonstige —, die die Daten in ihrem Bestand und in ihrer Organisation vor Störung und Verlust (durch Fehler und Katastrophen) und unberechtigtem Umgang (Miß-

---

[22]) „... zur rationellen Erledigung automationsgeeigneter Aufgaben und zur Gewinnung von Planungsinformationen und Entscheidungshilfen."
[23]) z. B. Einführung eines PKZ, einheitliche Datensätze
[24]) Meincke, 26
[25]) Giloi, 4
[26]) Miller, 1231; Giloi, 7; Meincke, 34 und 75
[27]) vgl. Kraushaar/Vollmeyer, 31
[28]) Einwohnerwesen, Finanzwesen, Grundstücke
[29]) Personaldatenbank, Kunden, Lieferanten
[30]) s. auch oben 1.3.
[31]) Prinzip der Vollständigkeit; s. a. Miller, 1216
[32]) Meincke, 73; Steinmüller (1), 87

brauch) während aller Phasen der Datenverarbeitung schützen.

2. Maßnahmen der Datensicherung und rechtliche Regelung

2.1. Derzeitiger Stand in der Literatur

Die derzeitige Behandlung der Datensicherung ist durch zwei Merkmale gekennzeichnet:

1. Der Begriff wird unterschiedlich gebraucht.
2. Die Notwendigkeit und Bedeutung werden generell gering eingeschätzt, zumindest in Deutschland (anders in den USA) [33]).

2.1.1. Zum Begriff

Im DV-Lexikon [34]) werden Ausführungen zu Fehlern bei der Datenübertragung und Verlust beim Speichern der Daten gemacht. Die Sicherung vor unberechtigtem Umgang ist hier nicht berücksichtigt.

Dieser Problemkreis wird terminologisch meist entweder unter „Datenschutz" [35]) oder unter „Datensicherheit" [36]) behandelt. Die Studie „BIS" [37]) führt unter der Überschrift „Sicherung gegen Mißbrauch" Berechtigungsprüfung, räumliche und materielle Sicherstellung an, sowie Kontrollen der Programme.

„Hessen 80" enthält Ausführungen zum Datenschutz [38]), äußert sich aber nicht zur Datensicherung.

Im Bayerischen Rahmensollkonzept der Arbeitsgruppe Grundbuchdatenbank wird eine hohe Zuverlässigkeit der Anlage angenommen [39]). Als Probleme, die unter Datensicherung fallen, werden Datenerfassung, Programmtests und Berechtigungsprüfung genannt.

Eine Übersicht über Datensicherheit [40]) enthält nichts zum Thema Zuverlässigkeit der Systeme, den Schutz vor Katastrophen. Zwangsläufig — bedingt durch die Zielgruppe [41]) — erscheint auch die sonstige Darstellung etwas verkürzt (Datenschutz für betriebliche Daten), weil das Interesse des Betriebs bzw. des Benutzers an der Geheimhaltung im Vordergrund steht, nicht das des durch die Daten erfaßten Menschen. Andere Veröffentlichungen beschränken sich nur auf die Fehlermöglichkeiten [42]).

Bei Steinmüller findet sich der Versuch, Datenschutz und Datensicherung in ein systematisches Verhältnis zu bringen und begrifflich abzugrenzen [43]). Es stellt sich aber die Frage, ob diese Einteilung der Sache heute noch gerecht wird und ob sie praktikabel ist, was noch erörtert werden muß.

Insgesamt ist festzustellen, daß das Problem Datensicherung selten umfassend und im Verhältnis zum Datenschutz, wie er im Gutachten verstanden wird, systematisch dargestellt wird.

2.1.2. Notwendigkeit und Bedeutung der Datensicherung für den Datenschutz

Hier findet sich vor allem amerikanische Literatur, die die Prüfung von Berechtigungen und sonstige Sicherungen vor Mißbrauch im Hinblick auf die privacy-Problematik behandelt [44]). Die übrigen Bereiche, z. B. Fehler der Maschine, der Programme und des Personals werden nicht unter diesem Blickwinkel (Datenschutz, besondere Datensicherheit bei personenbezogenen Daten, Richtigkeit) erfaßt. Dabei überlagern sich die beiden Aspekte — physikalische Sicherheit vor Fehlern und Katastrophen und logische Sicherheit vor Mißbrauch —, wenn man die konkreten Maßnahmen betrachtet:

Der Schreibring [45]) am Magnetbandgerät schützt vor fehlerhaftem wie vor mißbräuchlichem Überschreiben von Dateien.

Dateierklärungen [46]) auf dem Magnetband oder der Magnetplatte sichern sowohl vor fehlerhaftem wie unberechtigtem Zugriff.

Eine Archivierung von Originalen oder Duplikaten in vor Katastrophen wie Wegnahme sicheren Räumen dient ebenso dem Verwalter der Datei wie dem von den Daten erfaßten Bürger unter dem Gesichtspunkt der Geheimhaltung wie der Rekonstruktion.

Die Entstellung eines Datums durch Fehler (des Programms, der DVA, der Leitung) kann dieselbe Wirkung haben wie bewußtes, mißbräuchliches Ändern durch Unberechtigte:

Das Datum ist unrichtig.

In beiden Fällen würde z. B. bei der Verwaltung der Bürger einen Anspruch auf Berichtigung haben [47]).

Ergibt sich aus Datenschutzrecht ein Anspruch auf Vollständigkeit der Daten, können Daten sowohl durch technische als auch personelle Fehler, ebenso durch Katastrophen wie unberechtigten Umgang gelöscht sein, so daß der Bürger betroffen ist.

Wenn der Bürger ein Auskunftsrecht hat [48]), die Daten zwischen Behörden ausgetauscht werden [49]), wohl immer mehr ein Systemverbund kommen wird, muß immer die Richtigkeit der Übertragung sicher-

---

[33]) z. B. Brandt, 97; Westin (2), 27; Miller (u. a.) bei Senate Hearings
[34]) C. Schneider (2)
[35]) Schulze
[36]) IBM: Betrachtungen zur Datensicherheit in DV-Systemen
[37]) Siemens AG (1), Bayerisches Informationssystem
[38]) Hessische Zentrale für Datenverarbeitung
[39]) I/18, s. a. I/34
[40]) IBM: Betrachtungen über Datensicherheit
[41]) Das Management
[42]) Kraushaar/Vollmeyer, 27 ff.
[43]) Steinmüller (1), 87; es wird zwischen Datenschutzmaßnahmen (technischen und juristischen) und Datensicherungsmaßnahmen unterschieden, S. 88.
[44]) Miller, 1207
[45]) Westin (2) 27 f.; mechanische Vorrichtung, die — an der Magnetspule angebracht — die Lösch- und Schreibelektronik des Gerätes freigibt.
[46]) Etikett, das zur Identifikation von Dateien und zum Schutz gegen Überschreiben auf dem Magnetband aufgebracht ist
[47]) BMeldeG § 18, I
[48]) EBMeldeG § 18, I
[49]) EBMeldeG § 16, I

gestellt sein, ebenso die Berechtigung überprüft werden [50]).

Je größer die Datenbestände sind, auf die potentiell zugegriffen werden kann, und je mehr Teilnehmer ein System hat, um so wichtiger werden die Maßnahmen zur Sicherung vor Fehlern und Mißbrauch [51]).

Speziell die Berechtigungsprüfung wird um so wichtiger, je qualitativ hochwertiger die Information ist, die das System vermitteln kann [52]). Die Datensicherung gehört deshalb notwendig zum Datenschutz und erhält unter dem Aspekt des Datenschutzes eine besondere Bedeutung.

2.2. Problematik normativer Gestaltung

Wie schon eingangs erwähnt, ist die Computertechnik in einer sehr raschen Entwicklung. Die Computerisierung, also der zunehmende Automationsgrad, steigt ständig, und zwar sowohl in Verwaltung wie Wirtschaft. Das bedeutet aber, daß einerseits die Bedrohung der „Privatsphäre" ständig zunimmt, andererseits eine Regelung, die davor schützen will, sich einer stark im Fluß befindlichen Materie annehmen muß. Abgesehen von der grundsätzlichen Frage, inwieweit der Jurist überhaupt in der Lage ist, den technischen Fortschritt in Normen zu regeln, stellt sich das rechtstheoretische Problem, einerseits die Tatbestände nicht zu generell, andererseits nicht zu speziell werden zu lassen.

Eine Regelung der Datensicherung muß sich deshalb an die prinzipiellen Bedingungen des Computers und seines Einsatzes halten. Von der Konzeption des Computers her, ausgehend von seiner Eigenschaft als Automat, bieten sich als Anknüpfungsstellen

input,

output,

(Steuer)programm, Speicherung

an [53]). Hinzu kämen Standardanforderungen über die Organisation von Rechenzentren (mit Terminals), personelle Maßnahmen wie Ausbildung, Arbeitsteilung u. ä. Es ist aber zu bedenken, daß sich diese Anknüpfungsstellen im Zuge des Aufbaus von integrierten Systemen verschieben bzw. entfallen. D. h., daß entweder gewisse Schnittstellen [54]) oder Nahtstellen definiert werden müssen, oder die Regelung so abstrakt formuliert wird, daß dieses Problem nicht auftritt.

2.3. Gewinnung von Kriterien der gesetzlichen Regelung

Die rechtliche Regelung muß Kriterien enthalten, die eine begriffliche und inhaltliche Erfassung des Gebiets ermöglichen, da das Vorschreiben einzelner Maßnahmen nicht ausreichen kann.

Voraussetzung für die Bildung solcher Kriterien ist eine Systematik. Im Prinzip bieten sich folgende Aspekte der Argumentation an:

1. ausgehend von der Beschaffenheit des Computers, von der Arbeitsweise der Organisation usw., oder
2. vom Datenschutz ausgehend, dann erst entsprechend Nr. 1.

Eine Systematik muß je nach Wahl von 1 oder 2 verschieden ausfallen: Die grundsätzlichen, prinzipiellen Ziele und Aspekte des Computereinsatzes sind: Effektivität und Wirtschaftlichkeit. Sie können den Zielen des Datenschutzes klar zuwiderlaufen [55]).

2.3.1. Betrachtung ausgehend vom Computer

Hierzu können ziemlich klar die möglichen Maßnahmen erkannt und nach dem Gebiet, auf dem sie vorgenommen werden, eingeteilt werden:

1. technisch
   a) hardware,
   b) software,
2. organisatorisch
3. personell

Beispiele:

1. a) Betriebssicherheit der Anlagen,
   b) Routinen zur Fehlererkennung, Berechtigungsprüfung,
2. Arbeitsablauf,
3. Auswahl, Einsatz, Arbeitsteilung, Kontrolle.

Ob sich diese Einteilung für eine gesetzliche Regelung eignet, hängt davon ab, ob sich ein rechtlicher Bezug zum Datenschutz und dessen Zielen herstellen läßt, da sich die Notwendigkeit der Regelung der Datensicherung aus dem Datenschutz ableitet.

2.3.2. Betrachtung ausgehend vom Datenschutz

Es könnte deshalb richtiger sein, die 2. Version zu wählen. Der Datenschutz soll die Gefahren, die der Computereinsatz mit sich bringt, erfassen. Es bietet sich an, die Maßnahmen nach dem Zweck, ihrem Ziel einzuteilen: gegen welche Gefahren sie sich richten und damit nach Problemkreisen vorzugehen.

1. Gefahr der Zerstörung, des Verlusts, der Entstellung von Daten
   (v. a. durch physikalische Einwirkung)
   z. B. Katastrophen (Wasser, Feuer) = von „außen"
   Fehler (Maschinen, Programme, Personen) = von „innen"
2. Gefahr des unberechtigten Umgangs (Mißbrauch) mit Daten
   Preisgabe, bzw. Zugriff (Ausgabe)
   Änderung und Eingabe (Verfälschung)

Diese Einteilung entspricht auch etwa der Definition von Meincke [56]). Es lassen sich 2 große Gruppen

---

[50]) EBMeldeG § 16, II
[51]) Giloi, 4
[52]) Miller, 1207
[53]) DIN — Entwurf Automat, DIN 19 233, November 1970; Fiedler (2), 434; Westin (2), 27; Miller 1212
[54]) d. h. Verbindungsstellen
[55]) Miller, 1211
[56]) Meincke, 73

erkennen, die weiter unterteilt werden können, z. B. nach technischen, organisatorischen, personellen Gesichtspunkten.

Die Unterscheidung von 1. und 2. erscheint sinnvoll, weil die Maßnahmen zur Verhütung z. T. verschieden und die Gefahren verschiedener Natur sind.

Im ersten Fall 1. ist es das Interesse, die Daten in der einmal gewollten Form solange zu erhalten, bis sie gewollt geändert oder gelöscht werden. Bis zu diesem Zeitpunkt soll die Zerstörung verhindert, der Verlust vermieden und Rekonstruktion ermöglicht werden.

Im zweiten Fall 2. geht es darum, nur den Berechtigten den Umgang mit den Daten zu gewähren.

Einmal ist demnach die formale Darstellung (in der Anlage selbst oder in externen Speichern) des Datums in Gefahr und dadurch erst der Inhalt, zum andern ist es die Kenntnisnahme von eben diesem Inhalt bzw. Veränderung durch Eingabe, die nur Berechtigten möglich sein soll.

Gemeinsam ist beiden Arten der Gefahr ihre Beziehung zur Integration:

— Je mehr Daten nur einmal geführt werden (im Zuge der Integration), um so schwerwiegender sind Zerstörung und Verlust.

— Je mehr Daten ein System enthält — ob zentral oder im Verbund ist wegen der Möglichkeiten der Datenfernverarbeitung unwichtig — um so größer wird die potentielle Bedrohung [57]) der Privatsphäre durch die damit ermöglichte Transparenz [58]) und um so wichtiger deshalb die „Richtigkeit" der Daten.

— Je vielschichtiger die Daten und ihre Bezüge in einem System sind und je mehr verschiedenartige Stellen [59]) mit den Daten arbeiten, um so wichtiger werden die Möglichkeiten der Überprüfung der Berechtigung und damit der Sperren.

2.3.3. Versuch einer Systematik

2.3.3.1. Zerstörung, Verlust, Entstellung

Im folgenden wird versucht, anhand dieser Einteilung in 1. und 2. eine systematische Übersicht über die Gefahrbereiche zu erstellen.

Während aller Phasen der DV muß gewährleistet sein, daß die Daten „richtig" sind. „Richtig" heißt hier, daß sie in der vom Bearbeiter gewollten Form erhalten bleiben.

Es soll zunächst nach den Ursachen der Gefahr unterschieden werden, denn zwangsläufig wird sich danach die Art der Maßnahme richten. Im Prinzip lassen sich zwei verschiedene Quellen feststellen. Das eine sind die Fehler des Systems und der sie bedingenden Faktoren (Mensch, Klimaanlage, Zeitablauf). Das andere sind Einwirkungen mit Gewalt von außen (Katastrophe).

a) Fehler

Nach der *Ursache* können Fehler der hardware, der software und des Menschen festgestellt werden, und zwar während aller *Phasen* der DV: Erfassen, Speichern, Verarbeiten, Ausgeben. Unterteilt nach der *Wirkung* des Fehlers gibt es Zerstörung, Verlust und Veränderung/Entstellung. Die möglichen *Gegenmaßnahmen* lassen sich nach ihrem Zweck und der Art der Realisierung unterteilen: Der *Zweck* kann bestehen in Verhinderung, Erkennung, Korrektur, Rekonstruktion; die *Arten der Realiserung* sind technische (hardware, software), organisatorische, personelle.

Es dürfte sinnvoll sein, diese Art der Unterscheidung vorzunehmen, da sie genereller Natur ist und die Aspekte enthält, die bei einer gesetzlichen Regelung zu berücksichtigen sind.

b) Katastrophen

Die Gefahr der Katastrophe richtet sich gegen die Datenbestände in der Anlage oder auf extremen Datenträgern (Magnetbänder, Magnetplatten, Lochstreifen, Lochkarten, Mikrofilm, Belege). Fehler des Systems aufgrund von Katastrophen, z. B. Stromausfall, fallen unter Gruppe 1, also die Fehler i. e. S. Die Fälle der Katastrophen betreffen die direkte, gewaltsame Einwirkung auf die Daten.

Nach dem Zweck der Gegenmaßnahmen kann man unterscheiden in Verhinderung und Rekonstruktion, nach der Art der Maßnahmen in räumliche und materielle Sicherstellung.

2.3.3.2. Unberechtigter Umgang mit Daten

Zunächst kann nach der Art des Umgangs unterschieden werden:

Erfassen	
Eingeben	input [60])
Speichern	storage [60])
Ausgeben	output [60])

Grundsätzlich kann die Maßnahme in einer Kontrolle bzw. Sperre oder in Protokollierung [61]) bestehen (Verhütung oder Registrierung).

Für die Differenziertheit der Kontrollen kommt es auf den Charakter bzw. die „sensitivity" [62]) des Datums an.

Es kann z. B. nach Grund- und Folgedaten unterschieden werden [63]), nach Identifikations- und statistischen Daten [64]). Für die Art der Realisierung der Berechtigungsprüfung bzw. der Sperren kann nach Art der Maßnahmen unterschieden werden:

hardware	(identification cards, Schlüssel für Terminal, Raum, Archiv, Schreibsperren),
software	(Benutzeridentifizierungsprogramm aufgrund Code [65]) oder Stimmab-

[57]) Westin (2), 27
[58]) Bigelow, 299
[59]) durch horizontale, vertikale, funktionale Integration
[60]) Westin (2), 27; Miller, 1212
[61]) EBMeldeG § 16 II
[62]) Miller, 1207: Speicherung hierarchisch entsprechend dem „level of content sensitivity"; Schulze, 3: „Informationsgehalt"
[63]) EBMeldeG
[64]) Miller, 1216
[65]) z. B. password, vgl. Schulze, 7

druck Dateiverwaltungsprogramme, die entsprechende Klassifizierung von Daten und Benützern zulassen),

organisatorisch (Betriebsablauf),

personell (Ausbildung, Überwachung).

Voraussetzung für ein Funktionieren der Benutzerprüfung ist der Ausschluß von Fehlern im Programm selbst, bzw. die Geheimhaltung der Codes usw.

Hier ist es vor allem das personelle Problem, da Programmierung, Tests, Operating und Wartung von Personal ausgeführt werden muß, das nicht mit dem Benutzerkreis identisch ist.

[66]) Blau, 8

[67]) von Tassel, 6: es bestehen kaum Möglichkeiten, Operator und Programmierer davon abzuhalten, sich Daten zu beschaffen; Freed, 87 Kriminelle Akte früherer Beschäftigter.

[68]) Speicherauszüge

[69]) Betriebssystem z. B.

[70]) IBM, 15 ff. und 39

[71]) Freed, 92

Es können falsche Daten als Festwerte „einprogrammiert" werden [66]), Sperren umgangen werden [67]). Gerade bei Tests können Dritte leicht unbefugt Daten einsehen [68]).

Dasselbe gilt für die Wartung, die bei Fehlern der Prüfprogramme oder damit in Beziehung stehenden Programmen [69]) damit arbeiten muß, um den Fehler finden zu können.

Entsprechend wichtig für die Möglichkeiten des Ausschlusses von Mißbrauch ist die Gestaltung des gesamten Systems und des Betriebsablaufs mit seiner Organisation [70]), bzw. eine Untersuchung der schwachen Punkte des Systems [71]).

2.3.4. Kriterien

Kriterium für die Beurteilung von Fehlerquellen ist die Zuverlässigkeit (Anlagen, Leitungen, Organisation, Personal).

Für die Gefahr der Katastrophen ist die örtliche Sicherheit entscheidend (bauliche Sicherheit).

Maßgebend für die Gefahr unberechtigten Umgangs ist die Systemauslegung.

Einteilung der Gefahren

Zerstörung/Verlust/Entstellung (1.)			**Mißbrauch (2.)**	
Fehler		Katastrophen	Kontrolle/Sperre Protokollierung	Art der Maßnahme
Ursache	hardware		input	
	software		storage	Art des Umgangs
	Personal		output	
Phase/Umgang	Erfassung		Grund-Folgedatum	sensitivity
	Speichern			
	Verarbeiten			
	Ausgeben			
Wirkung	Zerstörung			
	Verlust			
	Entstellung			
Zweck/ Maßnahme	Verhinderung			
	Erkennung			
	Korrektur			
	Rekonstruktion			
Realisierung	hardware			
	software			
	organisatorisch			
	personell			

a) Zuverlässigkeit

(mittlere Zeichenfehlerhäufigkeit) [72])

— bei Erfassung: Mensch 10^{-2}

— bei Übertragung:

Leitung	10^{-6}	(Standleitung)
einfache Übertragungssicherheit	10^{-3}	(Wählverbindung)
	10^{-11}	(Standleitung)
höchste Übertragungssicherheit	10^{-8}	(bei Wählleitungen)

— bei Verarbeitung:

Rechner	10^{-9}	

Hinzu kommen die das System bedingenden Faktoren, wie Klimaanlage und Stromversorgung, für die ähnlich wie bei den Computern die mittlere unterbrechungsfreie Betriebszeit Gradmesser der Zuverlässigkeit ist.

b) Örtliche Sicherheit [73])

Für den Grad der örtlichen Sicherheit kommt es auf die Art der Unterbringung an, sowie auf die möglichen Gefahren (Wasser, Feuer, Explosion, Einsturz, Brachialgewalt, Strahlungen).

c) Systemauslegung

Für den Grad der Sicherheit des Systems, vor unberechtigtem Umgang zu schützen, kommt es auf das Differenzierungsvermögen an, d. h. welche Möglichkeiten der Überprüfung der Berechtigung bzw. Sperre je nach Benutzer und betroffenem Datum (sensitivity) bestehen [74]).

Insgesamt können Systeme danach beurteilt werden, welcher Grad von Zuverlässigkeit und Sicherheit im Zusammenspiel der verschiedenen Kriterien im System enthalten ist oder mit dem System erreicht werden kann. Je nach Anwendungsfall muß die Gewichtung der verschiedenen Kriterien verschieden ausfallen. Ein gewisses Mindestmaß muß für den Einsatz von Systemen, die mit personenbezogenen Daten arbeiten, gewährleistet sein, entweder durch bereits im System enthaltene oder nachträglich zu schaffende Sicherheitsfaktoren. Dabei ist zu berücksichtigen, daß der Faktor mit der größten Fehlerhäufigkeit maßgeblich für die Gesamtfehlerhäufigkeit ist [75]).

d) Gesamtsicherheit

Grundsätzlich ist jedes System von Sicherungen nicht lückenlos, es können immer Fehler auftreten, es ist immer Mißbrauch möglich [76]). Die Konsequenzen, die daraus gezogen werden müssen, sind u. a.

— keine Daten mit höchst wichtigen, geheimen Daten in Systeme mit Vielfachzugriff auf die Dateien aufzunehmen [77]),

— gerade eine Zusammenfassung der Daten in integrierten Systemen zu einer „zentralen" Datenbank gibt die Möglichkeit effektiv und wirtschaftlich vertretbare Sicherungen einzubauen [78]).

— hohe Anforderungen an die Sicherheit der EDV-Systeme zu stellen, etwa durch technische und informationelle Redundanz [79]).

3. Darstellung möglicher Maßnahmen

3.1. Fehler [80])

3.1.1. Erfassen (Erstellen eines Eingabebeleges) und Eingeben

Es gibt folgende Sicherungsverfahren (nicht vollständig):

Protokollierung der Codierung in Klarschrift,
zweimaliges Codieren (Prüflochen oder automatischer Vergleich),
Formatkontrollen,
Plausibilitätskontrollen,
prüfbare Zahlen.

Es handelt sich also um organisatorisch-personelle und programmierte Sicherungen. Wesentliches Merkmal der meisten Kontrollen ist die Erhöhung der Redundanz.

3.1.2. Übertragung

Fehlermeldung,
Fehlerkorrektur (durch Rückfrage und Wiederholung),
selbstkorrigierende Codes.

3.1.3. Verarbeitung

programmierte Kontrollen,
Protokolle,
Unterbrechungsroutinen (Wiederanlaufpunkte),
Tests: DVA (+ Wartung),
Programm,
Personal.

3.1.4. Ausgabe

Hier gilt sinngemäß das für 3.1.1. Gesagte.

3.1.5. Das System bedingende Faktoren

Notstromaggregate,
Unterbrechungsfreie Stromversorgung,
zusätzliche Klimaanlagen,
Alarmanlagen,
Personal.

3.2 Katastrophen

katastrophensichere Archivierung
Originalbelege,
Eingabebelege,

---

[72]) Steinbuch (3), 844
[73]) Siemens AG (2)
[74]) Miller, 1207
[75]) Kraushaar/Vollmeyer, 27
[76]) Miller, 1214; Westin (2), 27; Giloi, 9
[77]) Miller, 1214
[78]) so etwa auch Giloi, 10
[79]) Brennan, 9; Schneider (1), 60
[80]) Kraushaar/Vollmeyer, 27 ff.

Duplikate,
Speicherauszüge,
Generationsbänder,

katastrophensichere Anlageinstallation
Bunker u. ä.

3.3. Unberechtigter Umgang

Input-Kontrollen,
Speicher-Kontrollen [81]),
Output-Kontrollen [82]),
Datenorganisation entsprechend der sensitivity [83]),
Terminalidentifikation,
Benutzeridentifikation, bzw. -autorisation.

Im folgenden wird versucht, die hierarchische Struktur eines Berechtigungskonzepts darzustellen.

Terminal
Benutzer
berechtigt oder autorisiert, privilegiert
DVA
Programm
Programmteil
Datei
Feld (Datum)
Grund- oder
Folgedatum, bzw. sensitivity
speichern
abfragen
aggregiert
verknüpft
ändern
löschen
Ausgabe aller Werte
(Hintergrundinformation).

Kontrolle des Dialogs,
der Prozeduren (speichern, ausgeben usw.),
der Benutzer,
der Daten;

Protokollierung der Korrespondenz.

3.4. Versicherung

Nachdem kein System absolut sicher sein kann [84]), ist immer mit Fehlern und Mißbrauch sowie Katastrophen zu rechnen. Ein Stromausfall kann zwar durch geeignete Maßnahmen ausgeglichen werden [85]), aber die möglichen Maßnahmen können nicht jede Fehlermöglichkeit ausschließen, z. B. den ungeregelten Ausschluß von Terminals [84]) oder den Verlust von Daten in den Puffern [84]), und dabei ist der Stromausfall eine nicht außergewöhnliche Möglichkeit. Ebenso steht es mit den Mißbrauchsmöglichkeiten, wie oben erwähnt. Als Ergebnis ist die Notwendigkeit entsprechender Versicherungen festzustellen [86]). So kann zwar der Fehler nicht vermieden oder beseitigt, aber der Schaden ersetzt werden.

3.5 Mögliche Maßnahmen

Die folgende Aufzählung ist nicht abschließend und sollte nach Stand der Technik ergänzt werden.

Speicherschutz

parity bit
(Prüfziffern), Selbstprüfzahlen, Mischsummenprüfung (von Zahlen, die in der Regel nicht addiert werden: Erkennung, Verlust)

Erkennung, Blocküberlauf

Formatkontrolle

Plausibilitätskontrolle

Ausschlußprüfung
Bereichsabfrage (sind die Ordnungsbegriffe im Programm vorgesehen?)
Vorzeichenprüfung
Grenzprüfung

Selbstprüfzahl Kennummer: Kontrollziffer, die in arithm. Verhältnis zur Kennziffer steht

Folgekontrolle bei aufsteigenden Ordnungsbegriffen

Interne Kontrollen: Prüfschaltungen
sich selbst kontroll. Stromkreise
programmierte Prüfabläufe

korrigierbare Codes (= Informationsredundanz) = Oberbegriff?

Blocksicherung

Summenkontrolle, -fortschreibung, logische Kontrolle

technische (hardware) Redundanz (zusätzl. Schaltungen)

Speicherabzug, Speicherauszug

Wiederanlaufpunkte (Checkpoint — Restart — Routine) an bestimmten Punkten wird Inhalt der Speicher sichergestellt (nach ungeregeltem Zusammenbruch kann die Wiederaufnahme des Programms von dieser Marke an einsetzen, eine Wiederholung des ganzen Programms entfällt; technische Fehler, Stromausfall, u. ä.

Klimaanlage Zuverlässigkeit

---

[81]) Westin, 27: physische Sicherungen, Überwachung des Personals; Überprüfung des password-Konzepts
[82]) Miller, 1214: wenn überhaupt, dann vollständige Ausgabe
[83]) Control Data Corporation, 88-3: sensitivity level für Dateien; Control Data Corporation, 8-4: kneed-to-know flags für einzelne Daten kumulativ mit sensitivity
[84]) Westin (2), 27; Miller, 1212
[85]) unterbrechungsfreie Stromversorgung (USV)
[86]) Müller, 710: Feuerbetriebsunterbrechungsvers. (712), Schwachstromversicherung (712)

Stromausfall — Notstromaggregat, USV, V-Batterie; Puffer; Terminals; Zeit muß bis zum geregelten Archivieren des Verarbeitungsstandes (Warteschlangen, Übertragungsroutinen) reichen (ca. 7 Minuten); timesharing *Echtzeit*

Schreibring

Archivierung von Originalbelegen, Datenträgern der Eingabe, Duplikaten, Generationsbändern, Ergebnissen/Dateiauszügen;

sicher vor Feuer,
Wasser,
Temperatur,
Diebstahl;

an einem anderen Ort
zur Kontrolle
zur Rekonstruktion

Verwendungskartei

Programmbibliothek

Tests mit anderem Personal
auch der Sicherungsroutinen
mit Prüfprogrammen (zentrale Methoden- und Programmprüfung, Originalität, Richtigkeit)

closed shop Betrieb

Schlüssel für Räume
Archivschränke
Terminals

Straffe Arbeitsteilung bei Personal
bei Änderungen/Umstellungen

bei Arbeiten mit Platte Bänder mitlaufen lassen

Datenorganisation — indirekte Adressierung
Codieren für Übertragung
Verschlüsseln
Verdichten
Zerhacken bei Übertragung

Berechtigungsprüfung, Unterdrücken von Routinen (u. a. Ausgabe, aber auch Eingabe bzw. Änderung)

Password-Datei

sensitivity level für Datei

flag für Datum/Feld

Terminalberechtigung

Programmberechtigung
Eingabe,
Ausgabe,
Änderung,
Assoziation,
Aggregation,
Endergebnis,

Benützercode
Ausweisabtaster

Personal — Zugang,
Auswahl,
Einsatz (Arbeitsteilung, Original)

Protokollierung — wer,
wann,
mit welcher Prozedur,
welche Daten.

Versicherung

4. Ergebnis

Es existieren zahlreiche Datensicherungsmaßnahmen, die geeignet sind, zusammen mit den Datenschutzvorkehrungen die Belange des Bürgers ausreichend zu gewährleisten. Wegen der hohen Kosten müssen sie im DSchG ausdrücklich vorgeschrieben werden. Hierzu genügt eine Ermächtigungsnorm, die — abgestuft nach Bedeutung des jeweiligen IS — den jeweiligen „technischen" Stand der Datensicherung unter Berücksichtigung der zumutbaren Kosten verlangt, im übrigen aber eine — alle 3 Jahre neu zu erlassende — Rechtsverordnung vorsieht, die die Maßnahmen jeweils zum letzten Stand anpaßt.

Teil C

Besonderer Teil des Individualdatenschutzes Öffentliche Informationsverarbeitung

C. Besonderer Teil des Individualdatenschutzes
— Öffentliche Informationsverarbeitung —

1. Vorbemerkung

1.1. Schutzgegenstand

Ein Gesetz, das den Datenschutz in der öffentlichen Verwaltung (neben der Regelung der privaten Informationsverarbeitung) zum Gegenstand hat, bedarf insofern neuer Überlegungen als damit die Rolle von Informationen im Rahmen der öffentlichen Verwaltung zu bewerten ist. Dies wurde bisher nur sehr bruchstückhaft und auf Teilbereichen der Verwaltung geleistet. Im Gutachten soll deshalb versucht werden, den Faktor Information von grundsätzlichen rechtlichen und informationstheoretischen Ansatzpunkten her zu untersuchen und über die Verarbeitung von Informationen in der öffentlichen Verwaltung grundlegende Aussagen zu machen. Diese Aussagen sind nötig, da durch sie die verfassungsrechtlichen Möglichkeiten eines Datenschutzgesetzes erst abgesteckt werden. Öffentliche Informationsverarbeitung bezeichne hierbei die Informationsverarbeitung durch öffentliche Stellen, d. h. durch die öffentliche Verwaltung [1]).

Zunächst hat sich der Gesetzgeber jedoch zu überlegen, *wer* denn eigentlich durch das geplante Gesetz geschützt werden soll.

Datenschutz schützt den *Bürger*. Der Bürger tritt auf als Einzel- und als organisierte Person, d. h. als Mitglied von Gruppierungen. Er verwirklicht sich nicht nur im privaten außerstaatlichen Bereich, er wirkt vielmehr in den staatlichen Bereich hinein und bedarf, um seine Vorstellungen durchsetzen zu können, der Unterstützung der organisierten Gruppierungen der Gesellschaft.

Datenschutz umfaßt demnach nicht nur den Bürger als Einzelperson, sondern auch als organisierte Person, und damit die Organisation, die *Gruppierung* selbst. Datenschutz erschöpft sich also nicht in der Erörterung der „privacy"-Problematik, wie man gemeint hat, er geht noch erheblich darüber hinaus. Dabei ist es jedoch außerordentlich schwierig, die Schutzwürdigkeit von Gruppierungen jeder Art rechtlich zu beurteilen. Hierfür sind grundlegende rechtspolitische Überlegungen notwendig, die im Rahmen dieses Gutachtens in extenso nicht angestellt werden können; es können deshalb nur Lösungsvorschläge in hypothetischer Form aufgezeigt werden.

Rechtlich tiefer begründete Ausführungen können demnach nur insoweit gemacht werden, als sie den Bürger als Einzelperson betreffen.

[1]) im oben definierten weiten Sinn
[2]) dies wird allgemein anerkannt; für die Rechtsprechung vgl. BVerfGE 2, 280; 3, 24, 135, 337; 4, 18; 15, 201
[3]) Hesse (2), 10
[4]) Hesse (2), 11

1.2. Ziel und Gang der Untersuchung

Das Verfahren, das im folgenden eingeschlagen wird, orientiert sich an der Funktion, die das Verfassungsrecht nach den neueren Lehrmeinungen einnimmt: Zwar hat der Gesetzgeber bei der Gestaltung eines neuen Gesetzes einen „weiten Ermessensspielraum" [2]). Er ist in seinem Ermessen aber nicht völlig frei. Durch die Verfassung ist es ihm einerseits untersagt, verfassungswidrige Gesetze zu erlassen. Auf der anderen Seite stellt aber „die normative Verfassung die Voraussetzungen der Schaffung, Geltung und Durchsetzung der Normen der übrigen Rechtsordnung" her und bestimmt deren Inhalt weitgehend [3]): Die „Grundzüge aufgegebener rechtlicher Gesamtordnung werden durch die normative Verfassung verbindlich festgelegt" [4]). Ein zu erstellendes Gesetz muß sich daher in die vom GG errichtete Ordnungsvorstellung einfügen.

Das bedeutet für das Verfahren der Gesetzesfindung, daß nach der Umgrenzung der festzustellenden Materie (des zu regelnden Sachverhaltes) nach den grundgesetzlichen Ordnungskriterien Ausschau gehalten werden muß. Erst dann kann — innerhalb des immer noch bestehenden gesetzgeberischen Ermessensspielraumes — die gewünschte Regelung entworfen werden. Wegen der anerkanntermaßen bestehenden Antinomität einiger Bestimmungen des GGs hat dann noch eine Rückkontrolle zu erfolgen, bei der die Vereinbarkeit mit der Gesamtheit der verfassungsrechtlichen Grundnormen geprüft wird.

Dieses Verfahren unterscheidet sich grundsätzlich von dem zentralen Verfahren der Rechtsanwendung, der Subsumtion. Während bei der Subsumtion ein Sachverhalt daraufhin überprüft wird, ob er dem durch eine Rechtsnorm gewünschten Sachverhalt entspricht, werden hier die Verfassungsnormen zur Beantwortung der Frage herangezogen, welche Sachverhalte überhaupt durch Rechtsätze als gewünscht oder unerwünscht normiert werden sollen.

Für die folgende Untersuchung bedeutet das eine grundsätzliche Zweigliederung: Zunächst werden die relevanten verfassungsrechtlichen Kriterien *(Prüfungsmaßstab)* gesucht, anschließend werden diese Kriterien mit den zu regelnden Sachverhalten konfrontiert *(Prüfungsgegenstand)*.

Für den Prüfungsgegenstand, der hier zu betrachten ist, wurde oben bereits festgestellt, daß die Informationsverarbeitung sich nicht allgemein für eine rechtliche Erörterung eignet, daß sie vielmehr in einzelne Phasen mit unterschiedlicher rechtlicher Relevanz (Topoi) aufgegliedert werden muß. Die Untersuchung wird daher diese einzelnen Phasen nacheinander zugrunde legen.

2. Prüfungsmaßstab des Grundgesetzes

Der Datenschutz i. e. S. (Individualdatenschutz) beruht auf der Verfassung der BRD; näherhin im wesentlichen auf zwei Säulen:

— dem Rechtsstaatsprinzip, hier vor allem dem Grundsatz der Gewaltenteilung und der Gesetzmäßigkeit der Verwaltung, das dem Bürger und den geschützten gesellschaftlichen Gruppierungen (Artikel 19 III/IV GG) ein verfassungsmäßiges subjektives Recht darauf einräumt, daß öffentliche Informationsverarbeitung nicht in seine/ihre Rechte eingreift;

— dem Grundrechtskatalog, hier vor allem den Persönlichkeitsrechten der Artikel 2, 5 GG, die dem Bürger und seinen Gruppierungen u. U. sogar ein Grundrecht auf Information einräumen.

Aus diesen beiden „Säulen" leiten sich die Grundsätze des Datenschutzrechts des Bundes ab.

Da die „erste Säule", der Grundsatz der Gewaltenteilung und der Gesetzmäßigkeit der Verwaltung, sowohl im Rahmen von Artikel 2 GG wie der einzelnen Topoi zu erörtern ist, verbleibt hier die Präzisierung besonders des Artikels 2 Abs. 1 GG im Hinblick auf die Erfordernisse der Informationsverarbeitung.

Vorweg sind jedoch auch die übrigen einschlägigen Grundrechte auf ihre Eignung als Prüfungsmaßstab kurz zu untersuchen.

2.1. Untersuchung der speziellen Grundrechte auf ihre Eignung als Prüfungsmaßstab

Für die Auswahl der in Betracht kommenden Grundrechte ist entscheidend, ob und gegebenenfalls inwieweit sie ihre jeweilige Aussage auf Individualinformationen erstrecken. Da dies expressis verbis kaum der Fall ist, ist zu dieser Feststellung eine eigene Untersuchung nötig. Hier öffnet sich ein weites Feld neuer wissenschaftlicher Betätigung, das im Rahmen dieses Gutachtens nicht abgedeckt werden kann. Es steht zu vermuten, daß dazu für jedes Grundrecht eine neue inhaltliche Theorie entwickelt werden muß. Im Gutachten kann das nur für Artikel 2 Abs. 1 geleistet werden [5]).

2.1.1. Artikel 4 Abs. 1 — Informationsermittlung

Diese Bestimmung enthält unter anderem auch die Freiheit des religiösen Bekenntnisses. Darunter wird die Kundgabe des Glaubens und des Gewissens sowie die Kundgabe damit zusammenhängender persönlicher Entscheidungen verstanden [6]). Derjenige, der sich über seine Glaubensüberzeugung äußert, gibt damit Informationen nach außen, die ihn als Träger dieser Überzeugungen eindeutig bestimmen: er gibt Individualinformationen ab. Der Staat darf diese Abgabe weder beschränken, noch umgekehrt ihre Abgabe fordern. Letzteres wäre eine Informationsermittlung (Beschaffung), bezogen auf eine spezielle Art von Individualinformationen. Diese Frage ist bereits normativ geregelt: Artikel 136 Abs. 3 WV, der über Artikel 140 GG aktuelles Verfassungsrecht darstellt, ist eine Ausgestaltung der in Artikel 4 Abs. 1 enthaltenen Bekenntnisfreiheit [7]). Danach ist es staatlichen Stellen verboten, Informationen der religiösen Überzeugung zu ermitteln (Artikel 136 Abs. 3 Satz 1 WV); es ist ihnen aber erlaubt, die Frage nach der Zugehörigkeit zu einer Religionsgesellschaft zu stellen, wenn „davon Rechte und Pflichten abhängen oder eine gesetzlich angeordnete statistische Erhebung dies erfordert" (Artikel 136 Abs. 3 Satz 2).

Die Bekenntnisfreiheit des Artikels 4 Abs. 1 stellt sich also in der Ausprägung, die sie durch Artikel 140 i. V. m. Artikel 136 Abs. 3 WV erfahren hat, als ein Grundrecht dar, das sich auf die Informationsermittlung bezieht.

2.1.2. Artikel 5 Abs. 1 — Informationsweitergabe

Artikel 5 Abs. 1 Satz 1 statuiert das Recht des einzelnen, seine Meinung frei zu äußern, zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Hinter dieser Regelung steht die Auffassung, daß die Meinungsfreiheit (als zusammenfassende Bezeichnung der in Artikel 5 Abs. 1 genannten Spielarten) „für eine freiheitlich demokratische Staatsordnung schlechthin konstituierend" ist [8]). Artikel 5 Abs. 1 ist die Grundsatznorm unseres Verfassungsrechts [9]), sie wird sogar als institutionelle Garantie einer sog. „öffentlichen Meinung" verstanden [10]).

Artikel 5 Abs. 1 ist insoweit bemerkenswert, als hier Information als Grundlage des staatlichen Lebens anerkannt wird [11]); sie ermöglicht es dem Bürger erst, seine Rolle im öffentlichen Bereich adäquat zu spielen [12]).

Die Meinungsfreiheit lebt also vom Austausch von Informationen [13]) jeder Art; der Bürger gibt und nimmt Sach- und Personeninformationen. Beide Informationsarten sind also im Rahmen des Artikels 5 Abs. 1 relevant; in unserem Zusammenhang sind jedoch nur Individualinformationen interessant [14]). Unter dem Aspekt der Informationsverarbeitung ist festzustellen: Es handelt sich in jedem Fall um *Informationsweitergabe* (Äußern und Verbreiten durch den einzelnen; Unterrichten ist Weitergabe an einzelne). Es ist dabei dem Staat geboten, sich „aller Einwirkungen auf die freie geistige Kommunikation der Individuen zu enthalten (Achtungspflicht) und Einwirkungen Dritter so gut wie möglich abzuwehren (Schutzpflicht)" [15]).

Die in Artikel 5 Abs. 1 Satz 2 fixierte Pressefreiheit garantiert alle mit der Presse zusammenhängenden

---

[5]) Die nach Kenntnis der Verfasser einzige wichtigere wissenschaftliche Untersuchung ist die von Windsheimer, die „Information" als Interpretationsgrundlage für die subj. Rechte des Artikels 5 Abs. 1 GG

[6]) Hamann - Lenz, Artikel 4 N. B 3; BVerwGE 7, 195

[7]) Hamann - Lenz, a. a. O.

[8]) BVerfGE 7, 208; 12, 125

[9]) Hamann - Lenz, Artikel 5 N. A 2

[10]) Grundlegend Ridder, (2), 243 ff.; Herzog in Maunz - Dürig - Herzog, Artikel 5 N. 11 bis 14

[11]) Steinbuch (1), 15

[12]) siehe dazu Maunz - Dürig - Herzog, Artikel 5 N. 82

[13]) Dieser Ausdruck ist hier untechnisch gebraucht

[14]) Zur Bedeutung von Sachinformationen im Rahmen von Artikel 5 Abs. 1, s. u.

[15]) Windsheimer, 33

Tätigkeiten [16]). Pressefreiheit ist damit institutionalisierte *Informationsweitergabe.*

2.1.3. Artikel 6 Abs. 1 — Gruppeninformation, Informationsweitergabe

Artikel 6 Abs. 1 garantiert den besonderen Schutz von Ehe und Familie durch die staatliche Ordnung. Ehe und Familie bilden eine „Gruppierung" im Sinne dieses Gutachtens. Die Mitglieder dieser Gruppe genießen im Schoße der Familie einen Freiheitsraum wie es ihn sonst nicht gibt: Mann, Frau und Kinder können innerhalb der Familie einen „Rollenwechsel" vornehmen, sich vom öffentlichen Leben zurückziehen: Sie können Informationen über sich an die anderen Familienmitglieder geben, ohne darauf achten zu müssen, wie diese Informationen in der Öffentlichkeit wirken, und dadurch die „ganz persönliche Selbstdarstellung im Familienkreis [17]) leisten.

Wenn es nun über moderne Informationssysteme gelingt, diesen Intimbereich zu zerstören, indem das Verhalten des einzelnen in der Familie transparent und damit der Öffentlichkeit zugänglich gemacht wird, dann ist die Ehe in ihrem informationellen Kernbereich angetastet (und zugleich der Autonomiebereich des Artikel 2 Abs. 1 GG verletzt).

Artikel 6 Abs. 1 schützt demnach als „Kommunikationsfreiheit" die freie *„Informationsabgabe"*. Darin besteht die prinzipielle Bedeutung dieses Artikels für das Informationsrecht. Das informationelle Personenbild, das der einzelne mit Hilfe seiner Informationen an die Familienangehörigen abgibt, und das ihn in seinem Privatverhalten modelliert, ist insoweit mit umfaßt und geschützt.

2.1.4. Artikel 8 — Informationsermittlung

Im Rahmen der Versammlungsfreiheit kann Information in mindestens zweifacher Hinsicht relevant werden: sowohl die Tatsache der Teilnahme an einer Versammlung durch eine Person oder Gruppe als auch deren Äußerungen während der Versammlung sind Individualinformationen. Beschafft sich der Staat diese Informationen (dabei handelt es sich um *Informationsermittlung),* so greift er unter Umständen in den grundrechtlich geschützten Bereich ein [18]). Ein Eingriff liegt jedoch nicht darin, daß der Veranstalter nach § 2 I Versammlungsgesetz seinen Namen angeben muß; diese Bestimmung versteht sich lediglich als eine inhaltliche Ausgestaltung von Artikel 8 [19]).

2.1.5. Artikel 10 — Informationsaustausch, Informationsweitergabe

Briefverkehr, der Verkehr mit Postsendungen aller Art und telefonische und telegraphische Verbindungen sind unter dem Gesichtspunkt der Informationsverarbeitung als *Weitergabe* von Individualinformationen (z. B. Privatmann A an Privatmann B; Privatmann A an die Behörde C) oder als *Austausch* von Individualinformationen (z. B. Behörde C an Behörde D) anzusehen. Die Aussage von Artikel 10 Abs. 1 statuiert also die grundsätzliche Freiheit dieser beiden Verarbeitungsphasen von staatlichen Eingriffen. In Absatz 2 sind die Einschränkungsmöglichkeiten für den Staat abschließend geregelt. Für ein weitergehendes Datenschutzgesetz ist insoweit kein Raum mehr. Artikel 10 ist damit eine der wenigen bereits bestehenden Normen, in denen der Sachverhalt in der Verarbeitung von Individualinformationen besteht und durch rechtliche Vorschriften erfaßt wird.

2.1.6. Ergebnis: Nur begrenzte Eignung der speziellen Grundrechte

Die speziellen Grundrechte können nur insoweit als Prüfungsmaßstäbe herangezogen werden, als sie ihre jeweilige Aussage auf Individualinformationen erstrecken. Im übrigen ist das Auffanggrundrecht des Artikels 2 Abs. 1 zu prüfen.

2.2. Artikel 2 Abs. 1 als möglicher Prüfungsmaßstab

Die einzelnen speziellen Grundrechte erfassen jeweils nur einen Teil der Persönlichkeit. So erfaßt Artikel 4 Abs. 1 den einzelnen nur als Träger einer Glaubensüberzeugung, Artikel 8 als Teilnehmer von Versammlungen, Artikel 5 Abs. 1 Satz 1 nur als Subjekt einer Meinung. Die historische Entwicklung des Grundrechtskatalogs hat es mit sich gebracht, daß hauptsächlich die Rechte des einzelnen, deren Ausübung durch den Staat in der Vergangenheit am meisten gefährdet war, verfassungsrechtlich normiert wurden. Es steht jedoch außer Zweifel, daß darüber hinaus auch andere Lebensbereiche der Persönlichkeit gegenüber dem Staat schutzwürdig sind. Dies wird rechtlich gewährleistet durch die Interpretation des Artikels 2 Abs. 1 als Auffanggrundrecht [20]).

Ein solcher, von den speziellen Grundrechten nur teilweise erfaßter Lebensbereich der Persönlichkeit ist das Wissen um sie, um ihren Namen, ihre Wohnung, ihre Gewohnheiten, ihre Familienverhältnisse, ihren Besitz, kurz: ihre Individualinformationen. Dieses Wissen wird dann grundrechtlich relevant, wenn der Staat diese Informationen ermittelt und über sie verfügen kann.

Soweit also nicht spezielle Grundrechte eingreifen (was in der überwiegenden Zahl der Fälle nicht der Fall sein wird), ist für die Verarbeitung der übrigen Teile der Individualinformationen Artikel 2 Abs. 1 als Prüfungsmaßstab in Betracht zu ziehen.

2.2.1. Untersuchung von Artikel 2 Abs. 1 GG auf seine Eignung als Prüfungsmaßstab

Die Voraussetzung dafür, daß Artikel 2 Abs. 1 als Prüfungsmaßstab verwendet werden kann, besteht darin, daß dieses Grundrecht den einzelnen hinsichtlich der Informationen über seinen Lebensbereich schützt, wenn diese Informationen durch die Verwaltung ermittelt werden und ihr danach zur weiteren Verarbeitung zur Verfügung stehen. Mit ande-

---

[16]) Maunz - Dürig - Herzog, Artikel 5 N. 135; weitere Nachweise bei Windsheimer, 107 ff.
[17]) Luhmann (5), 103 ff.
[18]) Maunz - Dürig - Herzog, Artikel 8 N. 68
[19]) Maunz - Dürig - Herzog, Artikel 1 N. 95
[20]) BVerfGE 9, 343; 7, 386; Maunz - Dürig - Herzog, Artikel 2 N. 8 ff.; Hamann - Lenz, Artikel 2 N. A 3 b

ren Worten: *Schützt Artikel 2 Abs. 1 die Individualinformation vor unerlaubter Verarbeitung durch die Verwaltung?*

Diese Frage muß im folgenden untersucht werden.

Die Beantwortung dieser Frage hängt davon ab, ob die Verarbeitung von Individualinformationen sich auf die freie Entfaltung der Persönlichkeit im Sinne von Artikel 2 Abs. 1 auswirkt. Dies hängt wiederum davon ab, ob eine Auslegung des Begriffs der „freien Entfaltung der Persönlichkeit" es zuläßt, daß die Individualinformation diesem Begriff zuzuordnen ist.

2.2.2. Die freie Entfaltung der Persönlichkeit in Artikel 2 Abs. 1 (Auslegung)

2.2.2.1. Darstellung der herrschenden Lehre

Freie Entfaltung der Persönlichkeit wird von der h. L. in Literatur und Rechtsprechung als *„allgemeine Handlungsfreiheit"* interpretiert [21]). Dies ist historisch zu erklären: Einer der Vorschläge zur Fassung von Artikel 2 Abs. 1 hatte nämlich gelautet: „Jedermann hat die Freiheit, zu tun und zu lassen, was die Rechte anderer nicht verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt" [22]). Die heute geltende Fassung bedeutet demgegenüber lediglich eine sprachtechnische, aber keine inhaltliche Änderung [23]). Demnach wird Handlung mit Tätigkeit identifiziert: „Entfalten heißt tätig werden" [24]). Der einzelne „soll alles tun dürfen, was er will" [25]). Unter Tätigkeit wird also lediglich eine zeitlich begrenzte Auswirkung auf die Umwelt verstanden, vielleicht beschreibbar als Bewegung nach außen. *Hat also die Verwaltung Individualinformationen zur Verfügung, so wird durch diese Tatsache allein diese Handlungsfreiheit nicht eingeschränkt;* die Beeinträchtigung tritt erst dann ein, wenn die Tätigkeit selbst beschnitten wird [26]).

Der Besitz von Individualinformationen ermöglicht es aber der Verwaltung, den Betroffenen entweder gar nicht erst zum Handeln kommen zu lassen, oder seinen Handlungsspielraum von vornherein entscheidend einzuschränken. Die Verfügungsmöglichkeit über Individualinformationen ist somit potentielle Einschränkung der Persönlichkeitsentfaltung, und damit für Artikel 2 Abs. 1 relevant.

In der h. L. wird dies nirgends gesehen oder geschweige denn vertreten. Ihre Theorie ist somit für die Prüfung, ob und inwieweit die Verarbeitung von Individualinformationen die Persönlichkeitsentfaltung beeinträchtigt, in hohem Maße unbrauchbar.

Folgerungen für die anstehende Frage:

Für die Entscheidung der Frage, ob Artikel 2 Abs. 1 ein geeigneter Prüfungsmaßstab ist, ergeben sich jetzt zwei Möglichkeiten:

— Folgt man der h. L., so entfällt Artikel 2 Abs. 1 als Prüfungsmaßstab, da die Individualinformation nicht dem Begriff der freien Entfaltung der Persönlichkeit zuzuordnen ist.

Für ein Datenschutzgesetz würde das bedeuten: Will man diesem Gesetz eine Verfassungsgrundlage in einem Grundrecht verschaffen, so muß ein neues Grundrecht auf Individualinformation konstituiert werden. Oder aber man verzichtet auf eine verfassungsrechtliche Fundierung und erstellt ein Datenschutzgesetz ohne verfassungsrechtliche Relevanz.

— Folgt man nicht der h. L., so ist Artikel 2 Abs. 1 als Prüfungsmaßstab nur dann zu halten, wenn die freie Entfaltung der Persönlichkeit neu interpretiert wird. *Das bedeutet die Entwicklung einer neuen Theorie zu Artikel 2 Abs. 1, die es erlaubt, Individualinformationen der freien Entfaltung der Persönlichkeit zuzuordnen.*

2.2.2.2. Entscheidung für eine neue Theorie

Die Verfasser haben sich für die zweite Möglichkeit entschieden. Sie begründen dies folgendermaßen:

— Die Schaffung eines neuen Grundrechtes auf Individualinformation erfordert die qualifizierte Mehrheit des Artikels 79 Abs. 4 in Bundestag und Bundesrat. Dies setzt möglicherweise einen langwierigen Meinungsbildungsprozeß innerhalb der Regierungsparteien voraus. Dadurch könnte der Erlaß eines Datenschutzgesetzes in unzumutbarer Weise verzögert werden, da unterdessen die EDV in Bund und Ländern in immer steigendem Maße eingeführt wird. Dadurch erhöhen sich die Gefahren für den Bürger.

— Die Einführung des neuen Grundrechts wäre sachlich erst dann gerechtfertigt, wenn feststeht, daß das geltende Verfassungsrecht selbst nach einer Neuinterpretation von Artikel 2 Abs. 1 keine befriedigende Lösung der aufgeworfenen Probleme ermöglicht. Die Bildung einer neuen Theorie muß also mindestens versucht werden.

— Ein Datenschutzgesetz ohne verfassungsrechtliches Fundament wäre ein dogmatisch zweifelhafter Ausweg. Denn für die rechtlichen Beziehungen zwischen Bürger und Staat sind die Grundrechte schlechthin konstitutiv. Ein Datenschutzgesetz, das über diese Beziehungen Aussagen trifft, würde diesen Grundgedanken der Verfassung einfach negieren.

— Es gibt einige Stimmen in der Literatur, die die Interpretation durch die h. L. als allgemeine Handlungsfreiheit kritisieren. Sie deuten die Notwendigkeit einer Uminterpretation bereits an. *Brinkmann* sagt allgemein, daß Handeln als Umschreibung der Persönlichkeitsentfaltung zu eng sei [27]).

Stein konstituiert aus der *Freiheit* der Persönlichkeitsentfaltung ein Autonomierecht. Es soll das

---

[21]) BVerfGE 6, 36; Wernicke, Artikel 2 N. II 1 a; Maunz - Dürig - Herzog, Artikel 2 N. 11; Hamann - Lenz, Artikel 2 N. B 3 a; siehe auch Stein, 198

[22]) Vorschlag des Allgemeinen Redaktionsausschusses vom 13. Dezember 1948, vgl. Jahrbuch des öffentl. Rechts, Neue Fassung, 1, 1 ff.; 54 f.

[23]) Stein, 198

[24]) Hamann - Lenz, a. a. O.

[25]) Wernicke, a. a. O.

[26]) Bezeichnenderweise verzichten Maunz - Dürig - Herzog, a. a. O. auf jede allgemeine Erläuterung der allgemeinen Handlungsfreiheit

[27]) Brinkmann, Artikel 2 N. I 1 b 2

Recht umschließen, über das Ob und Wie der Selbstentfaltung zu bestimmen [28]). Das nackte Entfaltungsrecht würde gegen eine staatliche Verplanung nichts helfen; der Staat würde dadurch nicht an der Bevormundung des einzelnen gehindert. *Evers* unternimmt einen bemerkenswerten Versuch: Er geht ab von der vordergründigen Bestimmung der allgemeinen Handlungsfreiheit als der Freiheit, tun und lassen zu können, was man will, und weitet den Handlungsbegriff auch auf die Begleitumstände aus, unter denen die Handlung sich vollzieht: „Die Worte zu dem Freund können die gleichen sein wie vor einer Volksversammlung. Man wird nicht auf den Gedanken kommen, beide Fälle als gleich zu bewertende Handlung anzusehen. Handeln kann nur sinnvoll gedacht werden ... im Hinblick oder mit Rücksicht auf die Folgen. Es wird ein anderes Handeln, wenn sich Folgen daran knüpfen, die der Handelnde vermeiden will" [29]). Setzt man nun als Folge einer Handlung in der Umwelt das Zurückbleiben von Informationen über den Handelnden, so unterfallen diese nach Evers dem Handlungsbegriff und damit dem Artikel 2 Abs. 1.

Damit hat Evers einer neuen Theorie die Richtung gewiesen: Er hat erkannt, daß sich die Persönlichkeitsentfaltung nicht erschöpft in einer Handlung, verstanden als zeitlich begrenztes Tätigwerden in der Umwelt. Vielmehr hinterläßt eine Handlung nach ihrer zeitlichen Beendigung noch Spuren in der Umwelt, etwa Informationen über den Handelnden, die wiederum mit der Persönlichkeitsentfaltung in Beziehung gebracht werden können [30]). Von dieser Erkenntnis hat eine neue Theorie auszugehen.

2.2.3. Versuch der Entwicklung einer neuen Theorie

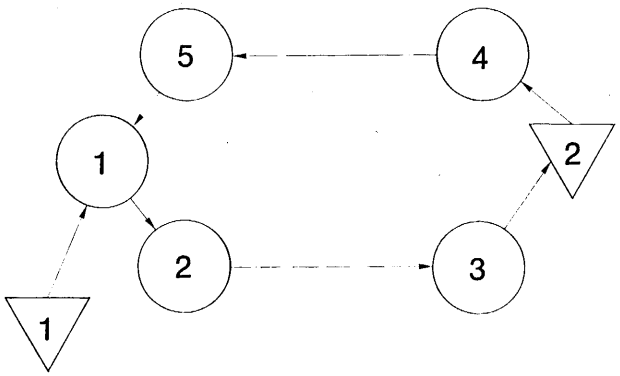
2.2.3.1. Methodische Schwierigkeiten

Es ist bereits geraume Zeit her, daß Evers diese Gedanken zum ersten Mal äußerte [31]). Seine Erkenntnis hat dennoch nicht zu einer neuen Theoriebildung zu Artikel 2 Abs. 1 geführt. Dies hat vermutlich folgenden Grund: Es gelang ihm nicht, eine plausible Erklärung dafür zu finden, daß die Folgen einer Handlung Einfluß auf die Persönlichkeitsentwicklung des Handelnden haben. Genau an diesem Punkt liegt das Problem einer neuen Theorie: *Über die Beziehungen zwischen dem Handelnden, der Handlung und den Folgen der Handlung läßt sich mit juristischen Methoden nichts aussagen.* Vielmehr handelt es sich um ein Problem, das von Psychologie und Soziologie erfaßt wird; *demzufolge läßt sich nur mit Methoden, die in diesen Bereichen angewandt werden, etwas Schlüssiges über die genannten Beziehungen aussagen.*

Von dieser methodischen Grundtatsache hat eine neue Theorie auszugehen.

2.2.3.2. Ansatz einer kybernetischen Erklärung

Es soll versucht werden, mit Hilfe eines einfachen kybernetischen Handlungsmodells die Zusammenhänge zu erklären, die zwischen den Folgen einer Handlung (etwa das Zurücklassen von Informationen über den Handelnden in der Umwelt) und der Entfaltung der Persönlichkeit des Handelnden bestehen. Dieses Modell hat auch bereits in die Kriminologie Eingang gefunden [32]). Es soll hier stark vereinfacht wiedergegeben werden [33]).



1 = Synthese
2 = Motiv und Selektion
3 = Aktion
4 = resultative Bewertung
5 = internes Modell

◁1 = Umwelteinfluß
◁2 = Reaktion der sozialen Umwelt

Erläuterung des Modells

Nach diesem Modell vollzieht sich der Handlungsablauf folgendermaßen: In Stufe ① vollzieht sich eine Synthese zwischen den Umwelteinflüssen, die auf den potentiell Handelnden einwirken ◁1 , und seinem internen Modell ⑤ . Darunter versteht man ein „Abbild der Außenwelt in der Struktur der Persönlichkeit" [34]), also die Vorstellungen, die sich der Handelnde von seiner Umwelt macht. Aus der Synthese entsteht die Motivbildung, die die Selektion der Möglichkeit zur Motivbefriedigung einschließen soll ② . Die ausgewählte Möglichkeit wird zur Aktion ③ , die in der Außenwelt wirksam wird. Diese Aktion wird von der Umwelt beurteilt, die Umwelt reagiert also ◁2 . Diese Reaktion nimmt der Handelnde wieder auf und bewertet sie für sich ④ . Diese Bewertung fließt wieder in das interne Modell ⑤ zurück. Das hier bereits vorhandene Abbild der Umwelt wird durch diese, auf der Reaktion der Umwelt aufbauende Bewertung, ständig bestätigt oder verbessert („Durch Erfahrung wird man klug!").

---

[28]) Stein, 201
[29]) Evers, 39
[30]) Diese Erkenntnis hat Luhmann (5), 53 ff. in seiner Deutung des Persönlichkeitsrechts als Recht der Selbstdarstellung durch Informationsaustausch rechtssoziologisch weitergeführt.
[31]) Sein Buch „Privatsphäre und Ämter für Verfassungsschutz" erschien bereits 1960.
[32]) vgl. Steinmüller (2), 96; G. Herzog, 781 ff.
[33]) Die Vereinfachung gegenüber der Darstellung bei Herzog erklärt sich aus dem hier verfolgten Zweck der Abbildung.
[34]) Herzog, 783

Für unsere Zwecke kommt es hauptsächlich auf die letzten Stadien des Handlungsablaufs an:

Bezeichnend ist zunächst, daß die Handlung mit der Aktion ③ nicht beendet ist; vielmehr zeigt schon allein die weitere Fortführung des Modells, daß noch weitere Auswirkungen für den Handelnden relevant sind. Da ist zunächst das Wirksamwerden der Handlung in der sozialen Umwelt; entscheidend ist aber, daß diese Umwelt reagiert und daß diese Reaktion auf den Handelnden zurückfließt. Damit ist genau das erklärt, was Evers gemeint hat:

Die Folgen einer Handlung wirken auf den Handelnden zurück, weil sie als die Reaktion der Umwelt das Bindeglied zwischen der Aktion und ihrer Beurteilung durch den Handelnden darstellen. Das Modell zeigt außerdem die Intensität der Rückwirkung. Der Handelnde bewertet nicht nur die Reaktion der Umwelt für sich, er läßt diese Bewertung in sein internes Modell einfließen; dies befähigt ihn zur Verbesserung seiner Vorstellungen über die Umwelt und gibt ihm damit die Möglichkeit, künftige Handlungen diesen neuen Erkenntnissen gemäß auszugestalten. „Der Handelnde eignet sich eine optimale Strategie der Auseinandersetzung mit der sozialen Umwelt an. Die Ergebnisse aus den resultativen Bewertungen werden gespeichert und bestimmen als Erfahrungen die Strategie der zukünftigen Handlungen" [35]). Diese Selbstoptimierung des Handelnden dient der Entfaltung seiner Persönlichkeit. Damit ist eine auf psychologischer Grundlage entwickelte kybernetische Erklärung für die gestellte Frage aufgezeigt.

Das Modell ist für unsere Zwecke jedoch nur brauchbar, wenn sich mit seiner Hilfe Aussagen über den Zusammenhang von Individualinformationen und Persönlichkeitsentfaltung machen lassen. Dies geschieht folgendermaßen: Durch die Aktion nimmt die Umwelt von dem Handelnden und der Handlung Kenntnis, sie nimmt Individualinformationen auf. Diese Kenntnis befähigt sie zu einer Reaktion, die der Handelnde wieder aufgreift. *Es ist also für eine Person nicht gleichgültig, was über sie in der Umwelt gewußt wird, denn dieses Wissen, das aus Individualinformationen besteht, fließt in veränderter Form als Reaktion der Umwelt in diese Person zurück und beeinflußt so ihre Entfaltung* [36]).

2.2.3.3. Ansatz einer soziologischen Erklärung

Den Zusammenhang zwischen Aktion und Umwelt, der bereits Gegenstand des geschilderten kybernetischen Denkansatzes war, ist auch mit soziologischen Kategorien faßbar. Von den verschiedenen soziologischen Begriffen, die sich mit dieser Seite der Persönlichkeit beschäftigen [37]), soll hier beispielhaft lediglich der der „sozialkulturellen Persönlichkeit" herausgegriffen werden. Er bezeichnet folgenden Tatbestand: „Das Individuum wird zur Person und zur Persönlichkeit, wenn andere ihm soziale Identität zuschreiben und auf es reagieren" [38]). Genauso wie die Gesellschaft in keiner Weise getrennt von den Individuen existieren kann, die sie aufbauen, kann auch das konkrete menschliche Individuum, wie wir es kennen, nicht allein in individuelle Vorstellungen aufgelöst werden; vielmehr gibt es eine „soziale Komponente seiner Persönlichkeit" [39]). Die Umweltkomponente wird also sehr stark betont. Sie ist die soziale Umwelt, d. h. die Gesellschaft und ihre Mitglieder. Nur durch ihre Reaktion auf den einzelnen bildet, d. h. entfaltet sich die Persönlichkeit des einzelnen: „Ein Grundproblem (der sozio-kulturellen Persönlichkeitsbildung) betrifft das Maß der Unterstützung, die die soziale Organisation der Gestaltungsstruktur gewährt, in der sich die Persönlichkeit bildet und die Frage, ob sie nicht geradezu die relative Entwicklung der organisch determinierten Persönlichkeitsdimensionen bestimmen" [40]). In aller Vorsicht [41]) kann also gefolgert werden: Die Persönlichkeitsbildung hängt von der Reaktion der Umwelt ab. Diese Reaktion setzt voraus, daß sie Individualinformationen über den einzelnen besitzt, die die Art der Reaktion beeinflussen.

2.2.3.4. Rechtliche Folgerung

Mit Hilfe kybernetischer und soziologischer Methoden läßt sich erklären, in welcher Weise die Folgen einer Handlung auf die Persönlichkeitsentfaltung des Handelnden zurückwirken. Darüber, wie diese Ergebnisse rechtlich umgemünzt werden, ist hier noch nichts ausgesagt. Dies ist Gegenstand der nun folgenden Untersuchung.

— Da die Persönlichkeitsentfaltung von Artikel 2 Abs. 1 geschützt wird und die Folgen einer Handlung auf die Persönlichkeitsentfaltung zurückwirken, wird der Handelnde auch hinsichtlich der *Handlungsfolgen* durch Artikel 2 Abs. 1 geschützt.

— Da der Staat gemäß Artikel 2 Abs. 1 nichts tun darf, was die Persönlichkeitsentfaltung unzulässig einschränkt, darf er dies auch nicht auf dem Umweg über die Folgen einer Handlung betreiben.

— Für den Handelnden bedeutet das: Er muß ein *Bestimmungsrecht über die Folgen seiner Handlung* in der Umwelt behalten. Zur Freiheit der Entfaltung der Persönlichkeit „ist das Recht zu zählen, den Umfang, in dem die Umwelt von Denken und Handeln einer Person Kenntnis nehmen soll, selbst zu bestimmen" [42]).

Kenntnis nimmt die Umwelt aber durch die Individualinformationen, die ihr vom einzelnen mitgeteilt werden. Noch allgemeiner: Für Dritte stellt sich jede Person durch Mitteilung einer Klasse geordneter Informationen dar.

Diese Selbstdarstellung — das informationelle Personenmodell — fällt zusammen mit dem Schutzbereich des Artikels 2 Abs. 1.

---

[35]) Herzog, a. a. O.
[36]) Hierzu Luhmann (5), ebd.
[37]) z. B. Enkulturation, Internalisierung, Sozialisation
[38]) Turner, 1032
[39]) Parsons, zit. nach König, 243
[40]) Turner, a. a. O.
[41]) Die Verfasser sind sich der Lückenhaftigkeit dieses Ansatzes bewußt.
[42]) Evers, 40; Stein, 201

Nun ist die Wirklichkeit noch etwas komplizierter:

An sich bestimmt jedermann ausschließlich selbst darüber, ob und welche Informationen er zur Selbstdarstellung an die Umwelt abgibt.

Aber genauso gilt, daß jedermann stets mehr Informationen an die Umwelt gelangen läßt, als zu dieser Selbstdarstellung erforderlich wäre.

Er tut sogar eine Menge Dinge ausschließlich deswegen, damit die Umwelt Informationen über ihn erhält, die ein bestimmtes Personenmodell erzeugen sollen.

Das regelungsbedürftige Problem besteht nun darin, daß in dieses Selbstbestimmungsrecht aus Artikel 2 Abs. 1 die moderne Informationsverarbeitung mittels Informationssystem massiv eingreifen kann und dadurch das „Informationsgleichgewicht" [43]) empfindlich zuungunsten des Staatsbürgers — und ebenso der Gruppierungen — stärkt. Denn durch die Transparenz des Personenmodells (= der Individualinformationen im Informationssystem) wird der Verhaltensspielraum des einzelnen eingeschränkt.

Bemerkenswert ist, daß diese potentiellen Auswirkungen moderner Informationssysteme auf den einzenlen stattfinden können, *ohne* daß auch nur im geringsten die Verwaltung oder einer ihrer Beamten entfernt totalitäre Absichten hätte!

Das System als solches entfaltet diese Wirkungen (werden sie nicht durch geeignete Maßnahmen verhindert), die der Beobachter von außen nicht von den Auswirkungen totalitärer Systeme unterscheiden kann.

GG Artikel 2 Abs. 1 garantiert demgegenüber das Selbstbestimmungsrecht des Bürgers über sein informationelles Personenmodell.

Dieses Ergebnis läßt sich auch durch eine dogmatische Überlegung stützen: *durch eine Auslegung des Begriffs der Persönlichkeitsentfaltung mit Hilfe des Artikels 1 Abs. 1.*

Dafür muß vorausgeschickt werden, daß Artikel 1 hier nicht als Grundrecht, sondern als übergeordnetes Verfassungsprinzip verstanden wird, das „Maßstab für alle einzelnen Grundrechtsbestimmungen und deren Auslegung" sein muß [44]). Die Menschenwürde des einzelnen ist verletzt, wenn er zum Objekt staatlichen Handelns gemacht wird [45]). Der einzelne wird aber dann nicht zum Objekt, wenn ihm Räume für eigene Entscheidungen vorbehalten bleiben, wenn sein Selbstbestimmungsrecht nicht beseitigt wird. Er muß die Entscheidung darüber tragen können, ob und wie er sich entfalten will [46]).

Es liegt nun folgende Frage nahe: Warum wird hier mühsam mit außerjuristischen Methoden ein Ergebnis gefunden, das sich ebenso gut auf dogmatischem Wege hätte finden lassen? Dazu ist zu sagen, daß die Verfasser der Auslegung von Artikel 2 Abs. 1 durch Artikel 1 nur Unterstützungswert zugestehen; sie ist nach unserer Auffassung nicht in der Lage, eine neue Theorie zu Artikel 2 Abs. 1 zu tragen.

Somit ergibt sich ein Formulierungsvorschlag für eine Theorie über den Begriff der Persönlichkeitsentfaltung: Freie Entfaltung der Persönlichkeit beinhaltet das Selbstbestimmungsrecht des einzelnen darüber, ob er handeln soll und welche Folgen er seiner Handlung zumißt.

Das bedeutet für Artikel 2 Abs. 1 als Prüfungsmaßstab:

Die Folgen der Handlung eines einzelnen sind das Zurücklassen von Individualinformationen in der Umwelt. Der *einzelne hat also ein Selbstbestimmungsrecht, welche Individualinformationen er unter welchen Umständen an wen abgibt.*

Die Verarbeitung von Individualinformationen durch die Verwaltung muß sich also daran messen lassen, ob und inwieweit sie das Selbstbestimmungsrecht und damit das Recht auf freie Persönlichkeitsentfaltung verletzt. Artikel 2 Abs. 1 ist somit ein tauglicher Prüfungsmaßstab [47]).

Das gleiche gilt für das Selbstbestimmungsrecht geschützter *Gruppierungen* [48]).

Ergebnis: Individual- und Gruppeninformationen sind vom Schutzbereich des Persönlichkeitsrechts aus Artikel 2 Abs. 1 GG mit umfaßt.

(Alternative: Artikel 2 ist entsprechend vom Verfassungsgesetzgeber zu erweitern — die Verfasser neigen eher ersterer Lösung zu).

2.2.4. Schranken des Informationsschutzes aus Artikel 2 Abs. 1

Individualinformationen sind vom Schutzbereich des Artikels 2 Abs. 1 GG mitumfaßt — in welchem Rahmen?

Beschränkungen ergeben sich aus zwei Richtungen: Von den Informationen und von den Schranken des Artikels 2 Abs. 1 selbst:

2.2.4.1. Schranken aus den Informationen selbst

Nur Individual- (und Gruppen-)Informationen sind vom Schutzbereich des Artikels 2 Abs. 1 GG umfaßt.

Hier muß ins Gedächtnis gerufen werden, daß die Menge der Individualinformationen im konkreten Fall sehr umfangreich sein kann — etwa bei einer Person des öffentlichen Interseses. Denn sie umfaßt alle im konkreten Informationssystem des Staates enthaltenen Informationen, die nach der konkreten Organisation dieses Systems zu einem „Personenmodell" zusammengefaßt werden kann, also vor allem alle personenbezogenen Informationen. Es gilt sogar der Satz: je mehr solcher Informationen auf eine Person (bzw. Gruppe) bezogen werden können, um so vollständiger ist das Personenmodell in den Händen der Verwaltung, um so größer die Beeinflußbarkeit, also die Gefährdung der Selbstbestim-

---

[43]) Begriff von Simitis (2), 677 aus dem Verhältnis Exekutive - Legislative

[44]) So Wernicke, Artikel 1 N. II 2 e; ebenso v. Mangold - Klein, Artikel 1 N. III 1 c 2; Stein, 219, Evers, a. a. O.

[45]) Maunz - Dürig - Herzog, Artikel 1 N. 24 f.

[46]) Maunz - Dürig - Herzog, Artikel 2 N. 42; Stein, 201; Nipperdey (3), 77

[47]) im Ergebnis ebenso Evers, a. a. O.

[48]) Hamann - Lenz, Artikel 19 N. 11

mung; um so stärker muß der Schutz aus Artikel 2 GG eingreifen können.

Freilich kann diesen Schutz nicht das GG allein gewähren; vielmehr bedarf es der Datenschutzgesetzgebung des Bundes und der Länder.

Ergebnis: Nur — aber alle — Individualinformationen sind von Artikel 2 geschützt im Rahmen der Schranken dieses Artikels.

2.2.4.2. Schranken aus dem Grundrecht

Der Informationsschutz aus Artikel 2 Abs. 1 ist jedoch dreifach eingeschränkt: Rechte anderer, verfassungsmäßige Ordnung, Sittengesetz. Aus dieser Schrankentrias kommt für unseren Zusammenhang nur der „verfassungsmäßigen Ordnung" durchschlagende Bedeutung zu: „Rechte anderer" betrifft nur das Verhältnis unter Privaten, die Einhaltung des Sittengesetzes in der Verwaltungstätigkeit versteht sich von selbst. Der Begriff der verfassungsmäßigen Ordnung ist heftig umstritten: Das BVerfG versteht darunter „die Gesamtheit der Normen, die formell und materiell der Verfassung gemäß sind", [49]) eine Meinung in der Literatur begreift darunter nur die tragenden Grundsätze der Verfassung [50]). Angesichts dieser Lage erscheint es zweckmäßig, den Begriff der verfassungsmäßigen Ordnung festzulegen und seine Bestandteile zu erörtern.

Entscheidung für die Begriffsbestimmung des BVerfG

Aufgrund seiner Entscheidung zur „allgemeinen Handlungsfreiheit" hat das BVerfG den Begriff der verfassungsmäßigen Ordnung als „verfassungsmäßige Rechtsordnung" interpretiert [51]). Diese Entscheidung ist häufig angegriffen worden; für eine Erörterung der Argumente ist hier nicht der Ort. Es darf davon ausgegangen werden, daß die Meinung des BVerfG sich praktisch durchgesetzt hat [52]). Für ein Datenschutzgesetz ist dies der ausschlaggebende Gesichtspunkt.

Danach würde die Verarbeitung von Individualinformationen dann der verfassungsmäßigen Ordnung entsprechen, wenn sie einerseits den die Würde des Menschen beinhaltenden Wesenskern des Grundrechts nicht antastet (Artikel 19 Abs. 2, Artikel 1 Abs. 3, Artikel 2 Abs. 1) und andererseits vornehmlich der Gewaltenteilung, dem Rechtsstaatsprinzip und dem Sozialstaatsprinzip nicht zuwiderläuft [53]).

Zunächst ist der *Wesensgehalt des Artikels 2 Abs. 1* im Hinblick auf den Individualinformationsschutz näher zu umreißen.

Der Einwand, der der Entscheidung des BVerfG immer wieder entgegengehalten wird, lautet: Das Grundrecht des Artikels 2 Abs. 1 laufe leer, wenn es unter einen allgemeinen Gesetzesvorbehalt gestellt werde [54]). Um diesem Einwand zu begegnen, hat das Gericht in ständiger Rechtsprechung einen Wesenskern des Artikels 2 Abs. 1 herausgebildet, der jeglichem staatlichen Eingriff entzogen sei. Es hat diesen Bereich „Intimsphäre" [55]) oder den Bereich der Eigenständigkeit und Selbstverantwortlichkeit genannt [56]).

Die Intimsphäre ende regelmäßig dort, wo Handlungen in den Bereich eines anderen Menschen hinüberwirken und ein gewisser „Sozialbezug" der Handlung innewohne [57]).

Dieses Recht habe „seine Grundlage in dem durch Artikel 2 Abs. 1 verbürgten Recht auf freie Entfaltung der Persönlichkeit. Bei der Bestimmung von Inhalt und Reichweite dieses Grundrechts ist zu beachten, daß nach der Grundnorm des Artikels 1 Abs. 1 die Würde des Menschen unantastbar ist und von aller staatlichen Gewalt geachtet und geschützt werden muß. Überdies darf nach Artikel 19 Abs. 2 auch das Grundrecht aus Artikel 2 Abs. 1 nicht in seinem Wesensgehalt angetastet werden" [58]).

Für den hier in Rede stehenden Bereich der Individualinformation hilft diese Begriffsbestimmung nicht recht weiter: Einerseits wird auf Handlungen Bezug genommen, die in unserem Zusammenhang unbrauchbar sind, andererseits wird das Problem der Umschreibung der Intimsphäre auf die Beschreibung von Menschenwürde und Wesensgehalt verlagert, beides Begriffe, die an Verschwommenheit dem der Intimsphäre nicht nachstehen.

Etwas griffiger erscheint die Formel des BVerfG von der *Eigenständigkeit und der Selbstverantwortlichkeit der Person.* Das BVerfG verwendet sie zwar ausdrücklich nur im Zusammenhang mit selbständigen Unternehmern. Doch könnte eine Ausweitung auf alle Personen nützlich sein. Denn „im Gegensatz zur Intimsphäre beziehen sie sich auf den sozialen Bereich, auf das Miteinander mit anderen und das Eingeordnetsein des einzelnen in größere Zusammenhänge. In der modernen, wirtschaftlich und sozial eng verflochtenen Gesellschaft ist ein völlig unabhängiges Leben einzelner ... nicht mehr möglich" [59]). Deshalb gilt es, in dieser Verflechtung Entscheidungsfreiheit zu wahren und eine Entscheidungsmöglichkeit im sozialen Bereich nicht zu behindern. Man könnte sagen: Der Wesensgehalt des Artikels 2 Abs. 1 liegt im Erhalten autonomer Entscheidungsräume; er ist angetastet bei Heteronomie des einzelnen. Auch Forsthoff [60]) stimmt dem wohl zu, wenn er sagt, daß eine Intimsphäre nur da einen Sinn hat, wo über die Gesamtperson eine Aussage zu treffen ist.

Für die Verarbeitung von Individualinformation bedeutet das: Die Fremdbestimmung ist erreicht, wenn auf Grund der in der Verwaltung vorhandenen Individualinformationen ein umfassendes Persönlichkeitsbild erstellbar ist, ein „Personenmodell", das manipulativen Zugriff erlaubt. Schon jetzt kann gesagt werden, daß dieser Gesichtspunkt bei der In-

---

[49]) BVerfGE 6, 32
[50]) z. B. Hesse, 140
[51]) BVerfGE, 37
[52]) Hamann - Lenz, Artikel 2 N. 6
[53]) BVerfGE 4, 41; 17, 313; 10, 363; 14, 306
[54]) Hesse, 160 ff.
[55]) BVerfGE 6, 432
[56]) BVerfGE 6, 32 ff.
[57]) BVerfGE 6, 432
[58]) BVerfG in NJW 70, 555; Maunz - Dürig - Herzog, Artikel 2 N. 31
[59]) Stein, 200
[60]) Forsthoff (4), 49

formationsermittlung und dem Informationsaustausch eine wichtige Rolle spielen wird.

Da hier der Meinung des BVerfG und Steins gefolgt werden soll (wohl die h. M.), wird nur der Vollständigkeit halber, *die abweichende Ansicht des BGH* erwähnt, der die Schranke des Artikels 19 Abs. 2 aus dem Grundsatz der Verhältnismäßigkeit herleitet [61]). Hier ist nicht der Platz, sich diskussionsweise mit dieser Meinung auseinanderzusetzen [62]).

Es kann *zusammenfassend* gesagt werden: Nur der Kernbereich von Eigenständigkeit und Selbstverantwortlichkeit der Person darf „in keinem Fall" angetastet werden; das verbleibende Feld des Artikels 2 Abs. 1 dagegen stehe — zumindest auch — unter dem Grundsatz der Verhältnismäßigkeit [63]). Daraus ergibt sich, daß bei diesem Bestandteil der „verfassungsmäßigen Ordnung" nur geprüft werden kann, ob ein staatlicher Eingriff den Wesensgehalt antastet und deshalb unzulässig ist. Für den Bereich außerhalb des Wesenskerns kann nichts ausgesagt werden. Hierfür müssen die anderen Bestandteile der „verfassungsmäßigen Ordnung" herangezogen werden: Sozialstaatsprinzip, Gewaltenteilung und Rechtstaatsprinzip.

2.2.4.3. Insbesondere: Grundprinzipien der staatlichen Ordnung

a) Gewaltenteilung (Artikel 20 Abs. 2)

Die Gewaltenteilung hat zwei Aspekte: Sie ist Organisationsmaxime des Staatsaufbaues und Kontrollmaxime der Staatsgewalten. Die letztere Funktion wird vom BVerfG folgendermaßen verstanden: Der Sinn der Gewaltenteilung liege nicht darin, „daß die Funktionen der Staatsgewalt getrennt werden, sondern daß die Organe der Legislative, Exekutive und Justiz sich gegenseitig kontrollieren und begrenzen, damit die Staatsmacht gemäßigt und die Freiheit des einzelnen geschützt wird" [64]). Gewaltenteilung dient also — zumindest auch — der Abwehr des Staates. Allein unter dieser Prämisse konnte das BVerfG den Begriff der „verfassungsmäßigen Ordnung" in Artikel 2 Abs. 1 als allgemeinen Gesetzesvorbehalt fassen [65]); andernfalls wäre dabei jede dem Artikel 1 Abs. 3 entsprechende eigene Bindungswirkung des Artikels 2 Abs. 1 weitgehend illusorisch gewesen.

---

[61]) BGHZ in VerwRspr 8, 98
[62]) zum Problemstand siehe Huber (2), 140 ff.; Gallwas, 81 ff.
[63]) BVerfG in NJW 70, 555
[64]) BVerfGE 9, 279
[65]) BVerfGE 6, 32
[66]) Hahn, 447 — a. M. Hamann - Lenz. Einf. D 1 B. 6, Zuständigkeitsverteilung als besonderes Prinzip neben der Gewaltenteilung im Rahmen des Rechtsstaatsprinzips.
[67]) Peters (2), 102 f. zurückgehend auf frühere Ansätze bei Forsthoff.
[68]) Peters (3), 192
[69]) z. B. Creifedls
[70]) Wolff (2), 14
[71]) siehe dazu Rasch, 29
[72]) Wolff (2), 13

Zuständigkeitsverteilung als Ausformung des Gewaltenteilungsprinzips

Wenn aber — wie oben zitiert — das BVerfG den Sinn der Gewaltenteilung in seiner Kontrollfunktion für die Staatsgewalt sieht, gleichzeitig aber eine scharfe Trennung der Funktionen der Staatsgewalt ablehnt, so fragt man sich, wie anders denn die Gewaltenteilung funktionieren müsse, um ihrer Kontrollaufgabe gerecht zu werden. Diese Frage muß geklärt sein, wenn das Gewaltenteilungsprinzip praktikabler Bestandteil des Prüfungsmaßstabs sein soll. Von dieser Frage ausgehend, wird es verständlich, wenn Stimmen in der Literatur die Gewaltenteilung bereits auf niedrigerer Stufe beginnen lassen. In unserem Zusammenhang sei damit eine *Aufteilung der Staatsgewalt innerhalb der Verwaltung gemeint.* „In diesem Sinne wächst das Prinzip über den Rahmen einer Dreiteilung im Verhältnis horizontaler, gleichgeordneter staatlicher Machtträger hinaus und begreift als Aussage über Mittel und Erscheinungsform der Gewaltentrennung auch ... die innere Gliederung inhaltlich einheitlicher Funktionen ... [66])". Es führt das System einer Vielzahl von Verwaltungsbehörden mit mehr oder weniger festumrissenen, jedenfalls gegeneinander abgegrenzten sachlichen *Zuständigkeiten* ... zu einer Aufteilung der Staatsgewalt innerhalb des Verwaltungsbereichs, wie sie zu Montesquieus Zeiten noch unbekannt war und daher damals als Schutzmittel für die Freiheit und Sicherheit des Bürgers außer Betracht bleiben mußte. Heute liegt hierin eine Art von Gewaltentrennung, die darüber hinaus noch bewirkt, daß der Bürger im Hinblick auf die Fachkenntnis der sachlich zuständigen Behörde besser geschützt ist als bei weitreichenden Zuständigkeiten ein und derselben Verwaltungsbehörde ... [67]). Angesichts der zu einer wirksamen Kontrolle der Exekutive unfähigen Organisationsstruktur der Parlamente, gewinnen Verwaltungsorganisation und Zuständigkeitsregelungen als Mittel einer „In-Sich-Kontrolle" der Verwaltung noch eine über den Schutz des Bürgers hinausgehende Bedeutung: sie ermöglichen eine *Transparenz* der Verwaltung [68]). Verwaltungsorganisation und Zuständigkeitsregelungen sind also in zweifacher Hinsicht bedeutsam.

An dieser Stelle erscheint es angebracht, den Begriff der *Zuständigkeit* zu erläutern. Er ist nämlich nicht — wie viele meinen [69]) — mit dem Begriff der Kompetenz identisch. Vielmehr enthält jeder dieser Begriffe eine eigene Aussage:

‚Im bezug auf die (Grenzen der) *Befugnis und Verbindlichkeit zur Wahrnehmung von Geschäften* durch ein Subjekt wird jedoch überwiegend von dessen „Zuständigkeit", im Hinblick auf den *Inhalt der wahrzunehmenden Verpflichtungen und Berechtigungen* und deren Gegenständen, die Geschäfte, meist von „Kompetenz" gesprochen' [70]). *Kompetenz ist der Gegenstand der Zuständigkeit;* Zuständigkeitsnormen sind formelle Organisationsnormen, die sich aus Aufgabennormen und Ermächtigungsnormen zusammensetzen [71]). Zuständigkeitsnormen regeln nur die formelle Verpflichtung zur Wahrnehmung einer Aufgabe [72]). Für die weitere Erörterung bedeutet das: Die Zuständigkeit als formelles

Organisationsmittel ist somit ein Bestandteil des Gewaltenteilungsprinzips, das durch Organisation den Schutz des Bürgers und die In-Sich-Kontrolle der Verwaltung bewirken will. Die Kompetenz ist hier nicht weiter zu erörtern.

Zuständigkeit und Information

Die hier vorgenommene Ausformung des Gewaltenteilungsprinzips innerhalb der Verwaltung hat für die in unserem Zusammenhang anstehende Prüfung aber nur dann Bedeutung, wenn es gelingt nachzuweisen, daß zwischen Zuständigkeit und Informationen ein Zusammenhang besteht, der es erlaubt, *Zuständigkeitsgrenzen durch Informationsverarbeitung zu verletzen.*

Dazu ein kurzer Blick auf die Arbeit einer Behörde: Sie arbeitet, um die ihr zugewiesenen Aufgaben zu erfüllen. Dies erfolgt in vielen einzelnen, rechtlich selbständigen Ergebnissen wie dem Erstellen von Verwaltungsakten und Leistungsbescheiden. Jedes von der Behörde erstellte Ergebnis ist eine in eine bestimmte Form des Verwaltungsrechts gekleidete Entscheidung. Jede Entscheidung beruht auf Informationen [73]). Diese Informationen sind Bestandteile der der Entscheidung vorangehenden Willensbildung. Der Willensbildungsprozeß spielt sich ab innerhalb des Systems, das durch Zuständigkeitsverteilung und Koordination der Zuständigkeiten organisatorisch gebildet wird [74]). Damit treten Information und Zuständigkeit über den Willensbildungsprozeß miteinander in Beziehung: *die Zuständigkeit begrenzt Menge und Art der zur Willensbildung heranzuziehenden Informationen.*

Sie bewirkt, daß jede Behörde fortlaufend alle Informationen erhält, die sie braucht, um zweckorientiert handeln zu können [75]).

Dies scheint im Widerspruch zu einer Beobachtung Ellweins zu stehen [76]):

Für den Willensbildungsprozeß bedürfe es Anregungen von außen und Anweisungen von innen; auf beides reagiere die Verwaltung. Zugleich ergebe sich aus dem System der Zuständigkeiten eine ständige Beobachtung des Bereichs, für den die jeweiligen Zuständigkeiten bestehen. Aufgrund dieser Beobachtungen speise sich die Verwaltung selbst mit Materialien und Informationen, mit deren Hilfe sie stets neu überlegt, ob sie tätig werden kann. Insoweit bestimme sie ihr Tun selbst. Die Zuständigkeiten reagierten also nicht nur auf Gesetzesbefehl oder Anruf des Bürgers, sondern durch ständige Beobachtung des Bereiches, für den Zuständigkeiten bestehen, nehmen sie selbst aktiv an der immerwährenden Formulierung der „faktischen Zuständigkeiten" teil. Die „faktische Zuständigkeit" bestimmt sich also offenbar danach, inwieweit die Verwaltung auch außerhalb ihrer rechtlich fixierten Zuständigkeiten tätig werden kann. Dies ist jedoch eine Frage der Aufgabe, also der Kompetenz. So ergibt sich hinsichtlich der rechtlich fixierten Zuständigkeit die Folge, daß sie hinter dem einer Behörde zugewiesenen Aufgabenbereich zurückbleibt [77]).

Dieses Ergebnis ist jedoch unstimmig: Eine Aufgabenzuweisung ohne eine dementsprechende kongruente Zuständigkeitsregelung ist wirkungslos, materielle ohne formelle Organisation läuft leer. In Erkenntnis dieser Tatsache wird kompetenzgemäßes Handeln der handelnden Behörde auch dann zugerechnet, wenn die Zuständigkeit fehlt oder nicht beachtet wurde [78]). Es ist davon auszugehen, daß Zuständigkeit ohne Kompetenz ebensowenig möglich ist wie Kompetenz ohne Zuständigkeit [79]). Daraus folgt, daß Zuständigkeit nicht nur durch formell organisatorische Regelungen [80]), sondern auch durch Kompetenzverleihung „faktisch" zugewiesen wird. Eine Verwaltungsstelle ist dann zur Erfüllung einer Aufgabe zuständig, wenn sie durch formelle oder materielle Organisationsregelungen dazu berechtigt ist. Wird Zuständigkeit so verstanden, dann bildet sie die *Obergrenze des Informationsinteresses.*

Für unseren Zusammenhang bedeutet das:

Die Informationsverarbeitung von Individualinformationen verstößt dann gegen das Gewaltenteilungsprinzip und damit gegen Artikel 2 Abs. 1, wenn dabei Zuständigkeitsgrenzen im oben definierten Sinne verletzt werden. Die Möglichkeit einer Verletzung ist besonders bei der Informationsermittlung und dem Informationsaustausch zu prüfen.

b) Das Rechtsstaatsprinzip

Zunächst verlangt das Rechtsstaatsprinzip — namentlich, wenn es in Verbindung mit den allgemeinen Freiheitsvermutungen zugunsten des Bürgers gesehen wird, wie sie in Artikel 2 Abs. 1 zum Ausdruck kommt —, daß der einzelne *von unnötigen Eingriffen der öffentlichen Gewalt bewahrt* bleibt [81]). Dies wird hauptsächlich bei der *Informationsweitergabe* an Dritte und der *Informationsveränderung* eine Rolle spielen.

Das Rechtsstaatsprinzip beinhaltet weiterhin den *Grundsatz der Gesetzmäßigkeit der Verwaltung.* Er zielt darauf ab, die Eingriffe der öffentlichen Gewalt möglichst berechenbar zu machen [82]). Zu diesem Zweck beinhaltet er für alle Beeinträchtigungen von Artikel 2 Abs. 1 ein subjektives Recht auf Gesetzmäßigkeit des Eingriffs [83]). Daher ergibt sich für die Verwaltung die Notwendigkeit, bei der Verarbeitung von Individualinformationen dann gesetzlich legitimiert zu sein, wenn dabei der Schutzbereich des Artikels 2 Abs. 1 berührt wird [84]).

Damit ist noch einmal deutlich klargestellt, daß Information nicht dem rechtsfreien Raum angehört, sondern — wenigstens, soweit sie als Individualinformation im Verwaltungsverfahren Grundrechtsschutz genießt — aus dem Verfassungsgebot des

---

[73]) Ellwein (3), 175
[74]) Ellwein (2), 104
[75]) Mayntz, 95
[76]) Ellwein (2), 104 f.
[77]) Becker, 189
[78]) Wolff (2), 14 f.
[79]) Wolf a. a. O.
[80]) z. B. § 139 b I GewO
[81]) BVerfGE 17, 313 f.
[82]) BVerfGE 8, 325
[83]) Maunz - Dürig - Herzog, Artikel 2 N. 26; Evers, 33
[84]) Evers, 52

Artikels 20 Abs. 3 heraus Gegenstand einer gesetzlichen Regelung sein muß.

Der Grundsatz der Gesetzmäßigkeit der Verwaltung fordert schließlich eine *begrenzte und näher bestimmte Ermächtigung der Exekutive* zu Vornahme belastender Verwaltungsakte [85]). Dies kann dann für die Prüfung relevant werden, wenn sich herausstellen sollte, daß innerhalb der Informationsverarbeitung Verwaltungsakte vorliegen.

2.3. Gruppendatenschutz

Neben dem Individualdatenschutz steht der Schutz der Gruppierungen des sozialen Lebens vor unerwünschter Ioformationsverarbeitung öffentlicher Stellen.

Bisher ging diese Untersuchung — vielleicht etwas undifferenziert — davon aus, daß Gruppendatenschutz dem Individualdatenschutz ebenso gleichzusetzen sei, wie oben Individualinformationen den Gruppeninformationen. Besteht diese Annahme zu recht?

Auch hier ist vom Grundsatz auszugehen — nicht ohne zu betonen, daß mit den folgenden Hinweisen die Problematik nicht entfernt auszuschöpfen ist. Vielmehr ist eine eigene Untersuchung erforderlich.

Wie gezeigt, ist der einzelne durch Artikel 2 Abs. 1 GG in seiner Handlungsfreiheit grundrechtlich geschützt. Dabei bezieht sich diese Handlungsfreiheit auch auf den Schutz seiner Individualinformationen.

Die Handlungsfreiheit des einzelnen umfaßt auch die Freiheit, sich in Gemeinschaft zu entfalten (vgl. Artikel 9 GG). Dabei wäre es falsch, dieses Handeln in Gemeinschaft als eine „bloß addierte Summe isolierter Einzelhandlungen" [86]) aufzufassen: Denn Ganzheiten sind ein aliud im Verhältnis zur Summe ihrer Teile [87]). Dieses Mehr ist nun nicht ohne weiteres im Schutz der Handlungsfreiheit des einzelnen inbegriffen. Auf der anderen Seite „soll jenes — gewissermaßen überschießende — durchaus personale Kräfte- und Wirkungspotential nicht grundrechtlich verlorengehen, das dadurch „mehr" entsteht, daß Einzelmenschen im Verband agieren" [88]).

Daraus ergibt sich, daß die allgemeine Handlungsfreiheit des einzelnen einerseits und das Recht des einzelnen, sich in Gemeinschaft zu entfalten andererseits (vgl. die entsprechenden Assoziationsgrundrechte: Artikel 9 Abs. 1, 19 Abs. 3, 21 GG) konsequenterweise dazu führen müssen, daß auch das Handeln der Gruppe selbst grundrechtlichem Schutz unterliegt [89]). Dies wird bestätigt durch Artikel 19 Abs. 3 GG, der bezüglich der juristischen Personen den Grundrechtsschutz klarstellt [90]).

Dabei besteht Einigkeit, daß sich der Schutz des Artikels 19 Abs. 3 wegen Artikel 9 Abs. 1 auch auf nichtrechtsfähige Vereine, offene Handelsgesellschaften, Kommanditgesellschaften usw. erstreckt [91]). Weiterhin besteht Einigkeit, daß Artikel 19 Abs. 3 in negativer Hinsicht keinen Ausschließlichkeitsanspruch dahin erhebt, daß überhaupt nur natürliche Personen und Rechtsgruppen mit allgemeiner Rechtsfähigkeit Träger von Grundrechten sein könnten [92]). Artikel 19 Abs. 3 blockiert insoweit nicht „die eigenständige Interpretation sonstiger Assoziationsgrundrechte" [93]). Es kommt auf die Schutzbedürftigkeit, nicht Rechtsfähigkeit der Gruppierung privaten Rechts an [94]).

Danach ist die hier zu entscheidende Frage, inwieweit auch Informationen, die Gruppen betreffen, grundrechtlich geschützt sind, wie folgt zu beurteilen:

1. Informationen, die im Zusammenhang mit einer Gruppe stehen, aber nur Aussagen über die einzelnen Mitglieder machen, fallen ohne weiteres unter den durch Artikel 2 Abs. 1 GG geschützten Bereich der Handlungsfreiheit.
2. Das gleiche gilt für Informationen, die über Handlungen des einzelnen *in der* Gruppe Auskunft geben, die also seine „Persönlichkeitsentfaltung in Gemeinschaft" [95]) betreffen.
3. Informationen, die das „Mehr" an „Kräfte- und Wirkunspotential" [96]), also das Handeln *der* Gruppe betreffen, wären immer dann ungeschützt, wenn von der Information der Rückschluß auf die einzelnen Mitglieder nicht möglich ist. Dies hätte zur Konsequenz, daß der Grundrechtsschutz des einzelnen Gruppenmitglieds durch Ausweichen auf nicht geschützte Informationen unterlaufen werden könnte.

   Einziger Ausweg ist, in Anlehnung an den Gedanken des Artikels 19 Abs. 3 Handlungen der Gruppen bezüglich ihrer Informationen den Handlungen von Einzelpersonen gleichzusetzen. Dies geschehe im Bundesdatenschutzgesetz.

   Im folgenden soll also der Begriff „Individualinformationen" auch die Informationen, die Gruppen im obigen Sinn betreffen, umfassen.

3. Prüfungsgegenstand: Die Phasen der Informationsverarbeitung (IV)

Im Vorangegangenen wurden die Grundlagen der Untersuchung gelegt [97]):

Der zu regelnde *Sachverhalt* ist die öffentliche Informationsverarbeitung [98]) in ihren einzelnen Schritten.

Regelungsziel ist der Schutz des Bürgers bzw. gefährdeter gesellschaftlicher Gruppen vor rechtspoli-

---

[85]) BVerfGE 8, 325
[86]) Maunz - Dürig - Herzog, Artikel 19 Abs. 3 N. 3
[87]) Maunz - Dürig - Herzog, a. a. O.
[88]) Maunz - Dürig - Herzog
[89]) vgl. dazu Maunz - Dürig - Herzog, Artikel 19 Abs. 3 N. 55
[90]) zu diesem Argument vgl. Maunz - Dürig - Herzog, Artikel 19 Abs. 3 N. 2
[91]) Maunz - Dürig - Herzog, Artikel 19 Abs. 3 N. 57
[92]) Maunz - Dürig - Herzog, Artikel 19 Abs. 3 N. 55
[93]) Maunz - Dürig - Herzog, Artikel 19 Abs. 3 N. 56
[94]) vgl. Hamann - Lenz, Artikel 19 Anm. 10 f.
[95]) Maunz - Dürig - Herzog, Artikel 19 N. 2
[96]) Maunz - Dürig - Herzog, Artikel 19 Abs. 3 N. 3
[97]) vgl. oben 1.2.
[98]) vgl. oben B. II.

tisch unerwünschter Informationsverarbeitung gem. den „zwei Säulen" des Datenschutzrechts, die die Verfassung errichtet hat:

— das Rechts- und Sozialstaatsprinzip

— der Grundrechtskatalog des GG [99])

Prüfungsmaßstab, an dem öffentliche Informationsverarbeitung zu messen ist, so ergab sich oben 2., ist das *informationelle Selbstbestimmungsrecht über das eigene Person- bzw. Gruppenbild* („Personenmodell").

Im einzelnen handelt es sich um folgende Schritte (Phasen) der Informationsverarbeitung (sie bilden die „Topoi"):

1. Topos: Ermittlung von Informationen
2. Topos: Erfassung von Informationen
3. Topos: Speicherung von Informationen
4. Topos: Veränderung von Informationen
5. Topos: Austausch von Informationen
6. Topos: Weitergabe von Informationen
7. Topos: Verbund von Informationen
8. Topos: Löschung von Informationen

[99]) vgl. oben B. III.

Im folgenden wird zunächst nachgewiesen, daß die *Ermittlung* (1. Topos) von Individualinformationen nur insoweit zulässig ist, als sie nicht den Wesenskern des Artikels 2 Abs. 1 GG antastet. Dieser Wesenskern ist dann beeinträchtigt, wenn sich mit Hilfe der Informationen unter Überschreitung der Zuständigkeit ein umfassendes Persönlichkeitsbild („Personenmodell") herstellen läßt. In einem neuen theoretischen Ansatz wird sodann gezeigt, daß zwischen Informationsermittlung und dem schließlichen Verwaltungsergebnis ein enger rechtlicher Zusammenhang besteht. Zu diesem Zweck werden die Begriffe „Minimal- und Unterstützungsinformationen" eingeführt. Danach verstößt die Ermittlung von Individualinformationen nur dann nicht gegen Artikel 2 Abs. 1 GG, wenn es sich, bezogen auf das Verwaltungsergebnis, um Minimal- und Unterstützungsinformationen handelt und die Ermittlung der Unterstützungsinformationen verhältnismäßig ist.

I. Topos Informationsermittlung

1. Definition

Informationsermittlung wurde oben definiert als Beschaffung (Aufsuchen) und Auswahl von Informationen. Dabei setzt die Auswahl von Informationen durch die Verwaltung voraus, daß diese bereits über die auszuwählenden Informationen verfügt. Zeitlich vorgeordnet ist dem der Vorgang der Beschaffung. Erfaßt man rechtlich schon die Beschaffung hinsichtlich der Art und Menge der zu beschaffenden Informationen, so ist der Vorgang der Auswahl selbst nicht mehr regelungsbedürftig; sie würde sich nur als Auswahl von rechtmäßig beschafften Informationen darstellen. Ansatzpunkt für eine rechtliche Betrachtung ist deshalb allein die Beschaffung. Sie ist der Prüfungsgegenstand.

Die Beschaffung ist dabei in dreifacher Weise denkbar: Durch Befragen des Betroffenen, durch Befragen Dritter, durch eigene Beurteilung von Personen oder Sachverhalten.

> Beispielsweise kann die Polizei im Zuge eines Ermittlungsverfahrens gegen X diesen persönlich fragen, wo er am Freitag gewesen sei; sie kann aber auch den Komplizen Y fragen, ob er wisse, wo X am Freitag gewesen sei; endlich kann sie aus Fußspuren entnehmen, daß X am Freitag an einem bestimmten Ort gewesen war.

Zur leichteren Verständlichkeit ein kurzer Wegweiser durch diesen Topos: Zunächst wird festgestellt, wann eine Ermittlung von Individualinformationen eine Beschränkung von Artikel 2 Abs. 1 beinhalten kann. Für diese Fälle wird dann anhand der „verfassungsmäßigen Ordnung" und dem Wesensgehalt des Artikels 2 Abs. 1 untersucht, welche Regelungsgesichtspunkte für ein Datenschutzgesetz sich daraus ergeben. Auf die Erörterung der Besonderheiten der Informationsermittlung bei (integrierter) Datenverarbeitung folgt die Zusammenfassung der Ergebnisse.

2. Schutzbereich des Artikels 2 Abs. 1 GG

Ermittlung von Individualinformationen durch öffentliche Stellen kann dann eine Beschränkung des Rechtes auf freie Persönlichkeitsentfaltung nach Artikel 2 Abs. 1 sein, wenn der Schutzbereich dieses Rechtes auf Selbstbestimmung über Individualinformationen eingeengt wird, d. h., die zu ermittelnden Individualinformationen zum Personenmodell zählen.

2.1. Auseinandersetzung mit Evers

Die einzige, sich mit der Ermittlung von Individualinformationen beschäftigende Veröffentlichung von Evers [1]) geht zwar grundsätzlich davon aus, daß die Ermittlung von Individualinformationen das Grundrecht einschränkt, billigt der Ermittlung aber zugleich keine große Bedeutung zu. Evers behauptet, es gäbe in bezug auf Eingriffe einen weiten Bereich des Artikels 2 Abs. 1, in dem dieser keinen Schutz entfalte [2]).

[1]) Privatsphäre und Ämter für Verfassungsschutz
[2]) s. 2.1.4.

Dies sei der Fall, wenn der Staat

a) auf allgemein zugängliche Informationen zugreife,
b) in Ausfüllung seiner generellen staatlichen Ordnungsfunktion handle,
c) seine Nachforschungen von geringem Umfang und geringer Intensität seien,
d) zufällig oder/und unbewußt tätig werde.

2.1.1. Zugriff auf allgemein zugängliche Daten

Allgemein zugänglich sei öffentlich:

„Die Privatsphäre endet jedenfalls, sobald einer unbeschränkten Öffentlichkeit die Kenntnisnahme möglich ist" [2]). Evers schränkt diesen Satz dann selbst ein; selbst bei beschränkter Öffentlichkeit (etwa in einer Gastwirtschaft) könne doch schon der private Bereich erfaßt sein. Die Abgrenzungskriterien für eine Unterscheidung von beschränkter und unbeschränkter Öffentlichkeit werden nicht genannt. Sind sie subjektiver Natur, wird die Abgrenzung also aus der Sicht des Betroffenen vorgenommen, so unterfallen sie der Relativität des persönlichen Urteils; sind sie objektiv festzulegen, so scheinen jedenfalls Informationen in öffentlichen Druckerzeugnissen, Rundfunk und Fernsehen dieser unbeschränkten Öffentlichkeit zu unterliegen. Letzteres ist — wenigstens im Einzelfall — vertretbar: Das Recht aus Artikel 2 Abs. 1 kann nicht beschränkt sein, wenn aus tatsächlichen Gründen (z. B. eigene Veröffentlichung) der einzelne sich seines Selbstbestimmungsrechts hinsichtlich beliebiger konkreter Empfänger begeben hat; gerade das ist aber der Fall bei möglicher Kenntnisnahme durch eine unbeschränkte Öffentlichkeit.

Da es sich um Umstände handelt, die einen jeden Einzelfall spezifisch kennzeichnen, ist es naturgemäß schwer, allgemeingültiges auszusagen. Dennoch sind annäherungsweise einige Fallgruppen aufzuzählen, in denen einer unbeschränkten Öffentlichkeit eine Kenntnisnahme möglich ist, und für die darum kein Individualschutz besteht. Sie bedürfen enumerativer Aufzählung [3]).

Zunächst handelt es sich dabei um solche Individualinformationen, die in *Telefonbüchern* und *Adreßwerken* enthalten sind. Weiß jemand den Nachnamen einer Person und will dazu Vornamen und Wohnsitz wissen, so ist ihm das in jedem Postamt für den ganzen Bereich der Bundesrepublik Deutschland möglich. Weiß er, in welcher Stadt der Betreffende wohnt, so ist ihm das sogar in jeder Telefonzelle dieser Stadt möglich. Auch die Angaben, die das PK enthält, gehören hierher.

Während Name und Adresse so in jedem Falle „bloßgestellt" werden, verhält sich das mit dem Beruf anders. Er kommt nur ins Telefonbuch, wenn der Betreffende das will. Die Berufsangabe gehört deswegen zu dem Fall, in dem jemand sich selbst seines Selbstbestimmungsrechts hinsichtlich beliebiger Empfänger begibt.

Weiterhin handelt es sich dabei um Informationen, die in *öffentlichen Registern* enthalten sind, und die jeder ohne besonderen Grund einsehen kann. Ein Beispiel ist das Handelsregister: Jeder Bürger kann feststellen, ob sein Nachbar X geschäftsführendes Vorstandsmitglied einer Firma ist und ob sein persönlicher Feind Y ein Handelsgewerbe eröffnet hat. Anders verhält es sich jedoch bei den Registern, deren Einsicht den Nachweis eines rechtlichen Interesses erfordert. So sind die im Grundbuch enthaltenen Individualinformationen nur bei Nachweis eines rechtlichen Interesses einsehbar. Da hier nur eine beschränkte Öffentlichkeit (nämlich nur die Träger eines berechtigten Interesses) Kenntnis nehmen können, handelt es sich hier nicht um eine unbeschränkte Öffentlichkeit.

Zuletzt sind noch die Fälle aufzuzählen, in denen sich der Betroffene seines *Selbstbestimmungsrechtes* hinsichtlich beliebiger Empfänger begeben hat. Dies trifft zu bei den Autoren von Büchern, die im allgemeinen Buchhandel erscheinen, bei Nachschlagewerken, in denen Angaben über den Lebenslauf einer Person mit deren Einverständnis abgedruckt werden, mit Einschränkungen auch bei Personen, die im öffentlichen Leben stehen und deren Äußerungen, Verhaltensweisen oder Leistungen in der Presse veröffentlicht werden. Letzteres gilt hauptsächlich hinsichtlich der Informationen, die mit der öffentlichen Stellung des Betreffenden im direkten Zusammenhang stehen.

In diesem Rahmen also besteht kein Individualdatenschutz; der Schutzbereich des Artikels 2 GG erstreckt sich hierauf nicht.

Im übrigen aber ist das Kriterium der allgemeinen Zugänglichkeit zu unscharf: Man vergleiche nur etwa die frühere Diskussion um das „öffentliche" Ärgernis. Letztlich wird hier das unbrauchbare, weil relativistische Argument der „Privatheit" (bzw. Öffentlichkeit) der „Privatsphäre" wiederzubeleben versucht.

2.1.2. Ausfüllung der staatlichen Ordnungsfunktion

Der Staat müsse „um seiner Ordnungsfunktion nachkommen zu können, von jedermann einige *elementare Dinge* wissen. Im Verhältnis zum Staat besteht für diesen Ausschnitt überhaupt kein Schutz des Für-Sich-Bereichs, weil die *Rechtsordnung* ihn versagt" [4]).

Diese Begründung muß in Zweifel gezogen werden. Wenn es zutrifft, daß der Faktor Information bisher kaum in das Blickfeld rechtlicher Erörterungen gerückt ist [5]), dann kann die bestehende Rechtslage noch keinen Aufschluß über Schutz oder Schutzlosigkeit von Individualinformationen bieten. Das Gebiet ist einfach nicht erfaßt. Der Hinweis auf die staatliche Ordnungsfunktion könnte jedoch als ein überwiegendes Interesse des Staates über das des Bürgers verstanden werden. Doch damit würde Evers nach seiner Systematik in den relativ geschützten Bereich des Artikels 2 Abs. 1 GG fallen, was hier aber offensichtlich nicht beabsichtigt ist. So bleibt letztlich die Unklarheit dessen, was gemeint ist: sie führt zur weitgehenden *Unbrauchbarkeit dieses Arguments.*

[2]) s. 2.1.4.
[3]) etwa nach dem Muster des EntwBMeldeG § 19
[4]) Evers, a. a. O.
[5]) Kamlah, 18 f.

Inhaltlich stimmen die elementaren Dinge, die der Staat wissen muß, überein mit den Informationen, die im amerikanischen Recht als unerheblich für eine Verletzung des Persönlichkeitsbereichs angesehen werden [6]). Da diese Vorstellung jedoch von einem unterhalb der „Privatsphäre" liegenden Bereich ausgeht, die „Privatsphäre" aber relativ ist, somit auch dieser unterhalb ihrer liegende Bereich kaum zu fixieren ist, kann auch diese Begründung die These von Evers nicht tragen.

Artikel 2 Abs. 1 entfaltet somit grundsätzlich seinen Schutz auch über die elementaren Dinge, die der Staat zur Erfüllung seiner Ordnungsfunktion von jedem einzelnen wissen muß.

2.1.3. Intensität und Umfang staatlicher Nachforschungen

Evers meint, Artikel 2 Abs. 1 schütze nur gegen ein staatliches Befassen von gewisser Intensität und gewissem Umfang. Flüchtige, in der Natur des menschlichen Zusammenlebens liegende Kenntnisnahme und bloße Belästigung sollen ausgeschlossen bleiben. Als Beispiel bringt er statistische Erhebungen, da durch den Zweck der Zählung das Private von seinen Trägern abstrahiert werde [7]).

Wiederum ist dieses Abstellen auf den Zweck nicht recht faßbar: Entweder geht man davon aus, der Zweck schränkt den Schutzbereich des Artikels 2 Abs. 1 ein — dann haben wir es mit Interessenabwägung zu tun — oder der Zweck stellt einen Rechtfertigungsgrund für einen Eingriff dar. Beides scheint von Evers nicht intendiert zu sein. Begründet man seine These damit, daß nach der Löschung der Urinformationen ein Rückschluß auf eine Einzelperson nicht mehr möglich und somit der Persönlichkeitsbereich (das Personenmodell) nicht tangiert wird, so ist auch dies einzuschränken.

Erstens muß erst einmal die Information ermittelt, erfaßt, gespeichert und verarbeitet (nämlich zur statistischen Information verarbeitet) werden, ehe sie gelöscht werden kann. Es handelt sich also bei der „Ermittlung" statistischer Informationen um kein Ermittlungsproblem, sondern um ein Verarbeitungs- und Löschungsproblem.

Zweitens lassen auch statistische Informationen Rückschlüsse auf Einzelpersonen zu, wenn sie durch dem Benutzer verfügbare Zusatzinformationen aufschlüsselbar sind, wie oben begründet wurde.

Drittens können auch rein statistische Informationen selbst den Wesensgehalt des Artikels 2 verletzen („90 % der Anwesenden sind Ehebrecher").

Viertens ist keineswegs erwiesen, ob mit den verfeinerten Methoden der Statistik nicht auch ohne Zusatzinformationen statistische Informationen den Durchgriff auf Einzelpersonen erlauben.

Die drei letzten Gründe mögen die Ursache dafür sein, daß statistische Informationen über den den Bürger betreffenden Bereich nicht an Steuerbehörden weitergegeben werden dürfen [8]).

Demnach ist der Persönlichkeitsbereich auch dann tangiert, wenn Nachforschungen von geringer Intensität und geringem Umfang angestellt werden; Artikel 2 Abs. 1 schützt auch gegen derartiges staatliches Tätigwerden.

2.1.4. Zufälliges staatliches Tätigwerden

Die bisher behandelten Fälle von Ermittlungen gingen davon aus, daß die Verwaltung bewußt und gewollt Individualinformationen beschafft. Es ist aber auch denkbar, daß ihr Individualinformationen zur Kenntnis gelangen, ohne daß sie dies gewollt hat, namentlich infolge unbeabsichtigter Nebenwirkungen [9]).

Beispielsweise stellt die Polizei bei der Verfolgung eines Straftäters fest, daß dessen Freund X ein Dieb ist. Trotzdem waren gegen X keine Maßnahmen gerichtet.

Oder: Auf seinem Patrouillengang liest der Polizist Y gewohnheitsmäßig die Nummern der Autos, die am Straßenrand abgestellt sind.

Oder: Eine geschwätzige Tante erzählt einem Verwaltungsbeamten anläßlich einer kleinen Auskunft ihre Lebensgeschichte. Es fragt sich nun, ob eine derartige zufällige Kenntnisnahme einen selbständigen Eingriff in den durch Artikel 2 Abs. 1 geschützten Rechtskreis bedeutet. *Eingriff ist jedoch nur das, was eingreifen soll, nicht, was zufällig geschieht* [10]). Somit ist eine Ermittlung nur dann rechtlich relevant, wenn sie eingreifen will, also bewußt und gewollt vorgenommen wird. Die oben genannten Beispiele stellen also keine Ermittlung im rechtlichen Sinne dar. Zwar geben manche Autoren in solchen Fällen Ansprüche, die direkt aus dem — angeblich nicht verletzten — Grundrecht abgeleitet werden (Beseitigungs-, Unterlassungs-, Entschädigungsansprüche). Eine Normierung dieser Ansprüche kann jedoch in einem Datenschutzgesetz unterbleiben; da es sich um Einzelfälle handelt, kann die Entscheidung über solche Ansprüche — wie bisher auch — in die Hände der Rechtsprechung gelegt werden [11]). Die Erörterung dieser (fälschlich?) sog. „faktischen Grundrechtsbeschränkungen" [12]) scheidet damit aus der weiteren Betrachtung aus.

2.1.5. Ergebnis

Nicht zutreffend ist die Ansicht von Evers, daß eine Verletzung von Artikel 2 Abs. 1 nicht vorliege, wenn der Staat Individualinformationen bei der Ausfüllung seiner generellen Ordnungsfunktion ermittle; unrichtig ist auch seine Meinung, daß Nachforschungen von geringem Umfang oder geringer Intensität keine Einschränkung von Artikel 2 Abs. 1 bewirken könnten, da Artikel 2 Abs. 1 grundsätzlich jede Individualinformation schütze, gleich, ob sie mit Nachdruck in Erfahrung gebracht werde oder nicht.

Richtig ist dagegen, daß die Ermittlung allgemein zugänglicher Individualinformationen den Artikel 2

---

[6]) Kamlah (1), 160 ff.
[7]) Evers, a. a. O.
[8]) Krauthausen, 729
[9]) Gallwas, 13 f., 16, 18
[10]) Evers, 46
[11]) Forsthoff (1), 315; BGHZ 12, 57; Gallwas, 127 bis 137
[12]) Gallwas a. a. O.

Abs. 1 nicht verletzt, jedoch nur in enumerativ begrenzten Fällen. Richtig ist weiterhin, daß Artikel 2 Abs. 1 auch nicht durch unbewußte oder zufällige Kenntnisnahme einer Individualinformation verletzt wird.

Damit folgt:

— Jede bewußte und gewollte Ermittlung von Individualinformationen ist eine Beschränkung von Artikel 2 Abs. 1, soweit die ermittelten Informationen nicht allgemein zugänglich sind.

— Gegen unbeabsichtigte Ermittlungen hat der Betroffene einen Unterlassungsanspruch, soweit dies eine rechtmäßige Ermittlung einer Behörde nicht unmöglich macht. Der Betroffene hat nach Abschluß der Ermittlungen in jedem Falle ein Löschungsrecht.

— Tritt durch eine unbeabsichtigte Ermittlung ein Schaden beim Betroffenen ein, so ist er dafür angemessen zu entschädigen.

3. Zulässigkeit einer Beschränkung des Schutzbereichs

Im folgenden [13]) wird untersucht, welche Möglichkeiten oder Beschränkungen sich für die Verwaltung aus der Tatsache ergeben, daß die Ermittlung den Schutzbereich des Artikels 2 Abs. 1 berührt.

Zunächst ist Prüfungsmaßstab der *Wesensgehalt* von Artikel 2 Abs. 1. Es wird nachgewiesen, daß dieser Wesensgehalt — und damit ein Bereich, der staatlicher Einwirkung strikt verschlossen bleiben muß — nicht betroffen ist, wenn die zu ermittelnden Individualinformationen

— zu keinem umfassenden Persönlichkeitsbild zusammengefaßt werden können,

— im Hinblick auf das zu erstellende Verwaltungsergebnis als Minimal- oder Unterstützungsinformationen anzusehen sind. Der Grund dafür ist, daß sich mit derartigen Informationen keine umfassenden Personenmodelle herstellen lassen.

Sodann sind Prüfungsmaßstab die sich aus der *„verfassungsmäßigen Ordnung"* ergebenden Grundsätze. Dabei handelt es sich hauptsächlich um das Gewaltenteilungs- und das Rechtsstaatsprinzip. Beide Prinzipien sind in Artikel 20 Abs. 3 GG niedergelegt. Über den vom BVerfG geprägten Begriff der „verfassungsmäßigen Ordnung" werden diese Grundentscheidungen jedoch mit dem Recht auf freie Entfaltung der Persönlichkeit in Verbindung gebracht. Als Folge davon hat das BVerfG seit der Entscheidung in BVerfGE 6, 38 in ununterbrochener Rechtsprechung Verfassungsbeschwerden als zulässig erklärt, die Verstöße gegen andere Normen der Verfassung als die Grundrechte zu Gegenstand haben [14]). Auf Grund dieser heute absolut herrschenden Ansicht ist es sowohl zweckmäßig als auch rechtlich einwandfrei, die Erörterung der Prinzipien des Artikels 20 Abs. 3 GG in die Behandlung des Artikels 2 Abs. 1 miteinzubeziehen.

Anhand der *Gewaltenteilung* wird zunächst festgestellt, daß ganz allgemein die Zuständigkeit einer Behörde ihrer Ermittlungstätigkeit rechtliche Grenzen setzt. Das gilt für die Ermittlung jeder Art von Information. Handelt es sich dagegen um eine Ermittlung von Individualinformationen, so ist diese Einhaltung der Zuständigkeitsgrenzen identisch mit der Beschränkung auf Minimal- oder Unterstützungsinformationen.

Im Rahmen des *Rechtsstaatsprinzips* wird die Rechtsnatur der Ermittlung untersucht. Als Ergebnis ist festzuhalten, daß die Ermittlung zwar einen Eingriff in den Schutzbereich des Artikels 2 Abs. 1 bedeutet, daß sie aber dennoch — wenn man nicht gegen die völlig herrschende Meinung operieren will — kein Verwaltungsakt ist. Sie bedarf in jedem Fall einer generellen formellen Rechtsgrundlage im Datenschutz- bzw. Verwaltungsverfahrensgesetz.

3.1. Wesensgehalt von Artikel 2 Abs. 1 GG

Forsthoff [15]) schreibt, daß der einzelne zur Verwaltung nur in bestimmten besonderen Stellungen oder Tätigkeiten (Staatsangehöriger, Gewerbetreibender) in Berührung tritt, was sich im *Verwaltungsergebnis* niederschlage, das nur eine Aussage über einen Teilbereich der Persönlichkeit erlaube. Insofern sei die Menschenwürde nicht verletzt.

Dies ist richtig; nur muß dies unter den heutigen Verhältnissen [16]) im Hinblick auf die Rolle der Information im Verwaltungshandeln neu durchdacht werden.

3.1.1. Kein umfassendes Persönlichkeitsbild

Entsprechend der oben gefundenen Formel vom informationellen Selbstbestimmungsrecht kann ein unzulässiger Eingriff in den Wesensgehalt des Artikels 2 Abs. 1 vorliegen, wenn die Ermittlung Informationen betrifft, die ein umfassendes Personenmodell herstellen lassen. Dies kann einmal geschehen durch Informationsaustausch und Informationsweitergabe und Sammlung (Integration) dieser In-

---

[13]) Unproblematisch und nur der Vollständigkeit halber zu erwähnen ist der Fall, daß die Behörde sich *weigert*, Individualinformationen *zu ermitteln*. Dies kann immer nur dann auftreten, wenn eine Person ein Tätigwerden der Verwaltung ihr gegenüber begehrt. Beispielsweise begehrt sie Sozialhilfe oder die Zulassung eines Kraftfahrzeugs. Dem einzelnen steht in solchen Fällen die Verpflichtungsklage nach § 42 VwGO zur Verfügung (evtl. auch die Untätigkeitsklage nach § 75 VwGO). Die Behörde wird dann nach § 113 IV VwGO zur Vornahme der begehrten Amtshandlung verurteilt. Dies muß, wenn der Anspruch des Gerichts von der Behörde in die Tat umgesetzt werden soll, auch beinhalten, daß die Behörde verpflichtet ist, die Individualinformationen zu ermitteln, die für den Erlaß der begehrten Amtshandlung notwendig sind (also die Minimal- und Unterstützungsinformationen, s. u. 3.2.).

[14]) vgl. auch BVerfGE 6, 433; 7, 199; 9, 11 ff.; 10, 99; 14, 30; 17, 313; Maunz - Dürig - Herzog, Artikel 2 N. 18; Hamann - Lenz, Artikel 2 N. 6; Stein, 202

[15]) Forsthoff (4), 48 f.

[16]) Forsthoff schrieb dies im Jahre 1954

formationen an einer Stelle, zum anderen durch die Ermittlung aller dazu erforderlichen Informationen durch eine einzige Verwaltungsstelle. Was aber ist ein umfassendes Persönlichkeitsbild?

Unter einem Personenmodell ist jede Menge von Individualinformationen zu verstehen, die eine bestimmte Person identifizieren. Auch das Personenkennzeichen ist bereits ein (rudimentäres) Personenmodell. Umfassend ist das Personenmodell nicht nur dann, wenn es die Vereinigung aller Individualinformationen innerhalb eines Informationssystems der öffentlichen Verwaltung enthält, sondern bereits dann, wenn es das künftige Verhalten der Person prognostizierbar macht oder den Rollenwechsel des einzelnen vom Berufs- in das Privatleben unmöglich macht. Wann ein solches umfassendes Personenmodell im Einzelfall vorliegt, kann überaus schwierig zu bestimmen sein und sollte der Rechtsprechung zur genaueren Bestimmung überlassen werden.

Wichtiger aber ist ein anderer Gesichtspunkt: Sofern es sich nicht um ein umfassendes Personenmodell handelt, gilt der Satz: Nicht das Personenmodell in der Hand der Verwaltung schadet, sondern seine bestimmungswidrige Verwendung. Zu beschränken ist darum nicht seine bloße Verwendung, sondern seine zweckwidrige Verwendung. Es darf also nicht zu anderen Verwaltungszielen gebraucht werden, als zu denen es von der abgebildeten Person weggegeben (oder rechtmäßig weggenommen) wurde. Jedes Verwaltungsergebnis nämlich kommt zustande aufgrund einer Informationsverarbeitung anhand eines informationellen Modells einer Person, wobei, wie gesagt, jeweils Teilmodelle der Person genügen.

Die hier angestellte Prüfung am Wesensgehalt des Artikels 2 Abs. 1 läßt demnach eine prinzipielle Aussage über den Umfang der Ermittlung zu: Die Ermittlung von Individualinformationen darf nicht zu einem Bild der Gesamtpersönlichkeit führen. Ein solches Bild ist dann nicht erstellbar, wenn die Verwaltung die von ihr ermittelten Informationen streng auf den Zweck der Ermittlung bezieht. Beantragt beispielsweise eine Person die Konzession zum Betrieb einer Gaststätte, so darf die Verwaltung nur Informationen ermitteln, die über die Zuverlässigkeit der betreffenden Person im Hinblick auf den Betrieb einer Gaststätte positiv oder negativ etwas aussagen. Oder wenn jemand die Zulassung eines Kraftfahrzeugs beantragt, so darf der TÜV (der ja im hier definierten Sinne eine öffentliche Stelle ist) nur Informationen ermitteln, die damit in Zusammenhang zu bringen sind. Er muß etwa feststellen, ob es sich um ein Fahrzeug handelt, das nicht wegen Verkehrsuntüchtigkeit zwangsweise stillgelegt wurde.

Die Beispiele zeigen, daß es darauf ankommt, was die Verwaltung konkret mit den ermittelten Informationen vorhat, auf den Zweck der Ermittlung. Dieser Zweck ist das *Verwaltungsergebnis.* Zum „Verwaltungshandeln" verhält sich das „Verwaltungsergebnis" folgendermaßen: Verwaltungshandlungen werden definiert als alle Handlungen von Amtswaltern der Verwaltung, die einem Träger öffentlicher Verwaltung zugerechnet werden. Sie können in einem Tun, Dulden oder Unterlassen bestehen und werden eingeteilt in tatsächliche Verwaltungshandlungen (sog. Verwaltungsrealakte) und Verwaltungsrechtshandlungen [17]). Verwaltungshandlungen ist also der Inbegriff dessen, was der Verwaltung möglich ist. Demgegenüber soll das Verwaltungsergebnis die konkret spezifizierte Verwaltungshandlung bezeichnen. Verwaltungsergebnis ist also der konkret spezifizierte Realakt (z. B. das Benennen einer Straße) oder die konkret spezifizierte Verwaltungsrechtshandlung (z. B. der Erlaß eines VA). Dies allein würde jedoch die Einführung dieses neuen Begriffs noch nicht rechtfertigen. Der entscheidende Unterschied zum Verwaltungshandeln besteht aber darin, daß das Wort „Ergebnis" zum Ausdruck bringen soll, daß hier etwas mehr oder weniger abschließendes *über eine Person* ausgesagt wird. *Verwaltungsergebnis will ausdrücken, daß eine Person in einer bestimmten Seite ihrer Persönlichkeit Gegenstand einer Verwaltungshandlung geworden ist.* Von diesem Verwaltungsergebnis hat nun Forsthoff nachgewiesen, daß sich die in ihm enthaltene Aussage über eine Person immer nur auf einen Teilbereich ihrer Persönlichkeit bezieht. „Der grundlegende Unterschied zwischen der gesellschaftlichen und der staatlichen Qualifikation einer Person besteht nämlich darin, daß jedermann der gesellschaftlichen Qualifikation mit dem Gesamt seiner Person ausgesetzt ist, während er mit der Verwaltung normalerweise nur sub specie einer besonderen Stellung oder Tätigkeit in Berührung tritt, so daß die Qualifikationsbeurteilung der Verwaltung nur *bestimmte* Fähigkeiten und Eigenschaften zum Gegenstand hat, nicht aber die Gesamtperson" [18]).

Er schreibt weiter, daß eine „Intimsphäre" nur da einen Sinn habe, wo die *Gesamtperson* dem Urteil Dritter ausgesetzt sei. Setzt man — in Anlehnung an das Mikrozensus-Urteil des BVerfG — hier die „Intimsphäre" mit dem Wesensbereich gleich, so besagt die Erkenntnis Forsthoffs, daß Verwaltungshandlungen solange nicht in den Wesensgehalt von Artikel 2 Abs. 1 eingreifen, als sie nur einen Sektor des gesamten Persönlichkeitsbereiches betreffen, also Verwaltungsergebnisse im oben umrissenen Sinn bleiben.

Diese Erkenntnis muß jetzt konkret auf die Ermittlung von Individualinformationen bezogen werden.

3.1.2. „Keine überflüssigen Ermittlungen!"

Das erste Ergebnis lautete: die öffentliche Informationsermittlung darf kein umfassendes Persönlichkeitsbild herstellen. Das zweite Postulat kann in dem Satz zusammengefaßt werden: „keine überflüssigen Ermittlungen!"

Zur Präzisierung dieses Postulates bedarf es freilich *einer neuen Theorie über Individualinformationen in der Verwaltung:* Wenn *Aussagen* einer Verwaltungsstelle über Teilbereiche der Persönlichkeit zu-

[17]) Wolff (1), 291 f.
[18]) Forsthoff, 48

lässig sind, so darf sie auch die hierfür benötigten *Informationen* ermitteln.

Zwischen Information und Ergebnis eines Verwaltungshandelns ist somit eine Beziehung konstruierbar, die aussagt, daß der Umfang der Beschaffung von Individualinformationen in irgendeiner Weise abhängt von dem Ergebnis, das die Verwaltung mit Hilfe dieser Daten erreichen will. Welche Informationen sind aber „nötig" für ein Verwaltungshandeln? Von daher gesehen, können die Informationen *hinsichtlich ihrer Erforderlichkeit für ein Verwaltungsergebnis* unterteilt werden:

3.1.2.1. Minimalinformationen

Einmal gibt es Informationen, die zur Erstellung eines bestimmten Ergebnisses *unbedingt erforderlich* sind; ohne sie ist die Erstellung des Ergebnisses unmöglich.

Fehlt eine derartige Information, so kann das Ergebnis nicht erzielt werden. Diese Informationen seien hier *Minimalinformationen* genannt.

Ist beispielsweise die Staatsangehörigkeit eines Bürgers nachzuprüfen, so sind Informationen über Name, Geburt, eine Legitimation oder eine Einbürgerung unbedingt zur Feststellung erforderlich [19]). Die Ermittlung dieser Informationen kann nicht gegen Artikel 2 Abs. 1 verstoßen, da sie in jedem Falle auf ein Ergebnis bezogen sind, das selbst wieder nur einen Teilbereich der Persönlichkeit des Betroffenen — seine Staatsangehörigkeit — erfaßt.

Freilich mag es zahlreiche Grenzfälle geben, in denen eine eindeutige Entscheidung nicht möglich ist; denn solche Informationen aus dem Grenzbereich sind dann aber jedenfalls zulässige Unterstützungsinformationen [20]).

3.1.2.2. Unterstützungsinformationen

Nun ist es aber unbestreitbar, daß die Verwaltung, wenn sie effizient arbeiten will, darauf angewiesen ist, sichere Informationen zur Grundlage ihrer Entscheidung zu machen. Die Minimalinformationen müssen der Wirklichkeit entsprechen, wenn das Verwaltungshandeln rechtlichen und tatsächlichen Bestand haben will. Das erfordert eine Überprüfungsmöglichkeit der Minimalinformationen. Diese kann nur erfolgen durch *Zusatzinformationen, die Rückschlüsse auf die Richtigkeit der Minimalinformationen zulassen;* diese Zusatzinformationen seien hier Unterstützungsinformationen genannt, um sie von den Zusatzinformationen zu statistischen Daten zu unterscheiden. Ermittelt die Verwaltung zur Feststellung der Staatsbürgereigenschaft einer Person zur Staatsangehörigkeit des Vaters [21]) noch die Aufenthaltsorte des Vaters im Verlauf seines Lebens, so ist für die Richtigkeit der Minimalinformation „Staatsangehörigkeit des Vaters" durch diese Unterstützungsinformationen ein höherer Wahrscheinlichkeitsgrad der Richtigkeit der Minimalinformation anzunehmen; denn es entspricht der normalen Lebenserfahrung, daß der langjährige Aufenthaltsort einer Person einen Schluß auf ihre Staatsangehörigkeit zuläßt.

Es fragt sich aber, ob solche Zusatzinformationen unbeschränkt ermittelt werden können. Mit Hilfe der bereits gewonnenen Erkenntnisse läßt sich sagen: Die Ermittlung von Zusatzinformationen individualisierenden Inhalts verstößt dann gegen den Wesensgehalt der Artikel 2 Abs. 1, wenn diese nicht in Beziehung zu dem zulässigen Ergebnis des Verwaltungshandelns zu setzen sind. Sie überschreiten dann den verfassungsrechtlich zulässigen Bereich einer Teilaussage über eine Person. Konkreter: *Ein Verstoß gegen Artikel 2 Abs. 1 liegt vor, wenn eine Zusatzinformation nicht als Unterstützungsinformation für eine Minimalinformation fungiert.*

Eine weitere Frage ist, ob der Kreis der Unterstützungsinformationen noch enger gezogen werden muß; m. a. W.: dürfen Unterstützungsinformationen unbeschränkt ermittelt werden? Denn prinzipiell bedarf jede Unterstützungsinformation zur Erhöhung ihrer Glaubwürdigkeit weiterer Unterstützungsinformationen, diese, zur Erhöhung ihrer Glaubwürdigkeit, weiterer Unterstützungsinformationen dritten Grades usw. ad infinitum.

Hier wird sich nicht Generelles sagen lassen: Einmal kann der Wahrscheinlichkeitsgrad der Richtigkeit einer Minimalinformation so gering sein, daß tatsächlich entweder mehrere Unterstützungsinformationen oder sogar für die letzteren selbst wieder Unterstützungsinformationen zweiten Grades erforderlich sind. Ein anderes Mal gibt es keinen Grund, an der Richtigkeit der einfachen Minimalinformation zu zweifeln, und die Ermittlung einer Unterstützungsinformation erübrigt sich. Man wird hier das allgemeine Prinzip der Verhältnismäßigkeit bemühen müssen, dessen Verstoß als grundrechtswidrig angesehen wird [22]). Als Gesichtspunkte, die bei der Beurteilung der Verhältnismäßigkeit zu berücksichtigen sind, können benannt werden:

— die Bedeutung des Verwaltungsergebnisses für den einzelnen (handelt es sich um eine einschneidende Maßnahme?),

— Bedeutung der einzelnen Minimalinformationen für das Ergebnis (ändert die Minimalinformation etwas am Ergebnis?),

— Glaubwürdigkeit des Betroffenen („ist der Betroffene wegen Meineids vorbestraft?").

Zusammenfassung

Eine Zulässigkeitsprüfung der Ermittlung von Individualinformationen am Wesensgehalt des Artikels 2 Abs. 1 GG ergibt, daß die Ermittlung dann zulässig ist, wenn es sich im Hinblick auf das Ergebnis des Verwaltungshandelns um Minimal- oder Unterstützungsinformationen handelt und die Ermittlung letzterer in bezug auf den Wahrscheinlichkeitsgrad der Richtigkeit der Minimalinformation verhältnismäßig ist.

---

[19]) §§ 4, 5, 8 RuStAG

[20]) s. dazu unten

[21]) § 4 RuStAG

[22]) BVerfGE 24, 404; nach allgemeiner Auffassung ist es das Verhältnismäßigkeitsprinzip, das in die Zweck-Mittel-Relation das Kriterium der Erforderlichkeit für alle Verwaltungshandlungen — also auch die Ermittlung — mit verfassungsrechtlicher Verbindlichkeit einführt (vgl. dazu besonders BVerfGE 20, 154 ff.)

3.2. Verfassungsmäßige Ordnung

Im folgenden werden nun das Gewaltenteilungsprinzip und das Rechtsstaatsprinzip als Prüfungsmaßstab herangezogen. Dabei kommt im Rahmen des Gewaltenteilungsprinzips die Zuständigkeitsverteilung unter den Behörden zur Sprache; dann wird anhand des Rechtsstaatsprinzips untersucht, welche Rechtsnatur der Ermittlung von Individualinformationen zuzuschreiben ist.

3.2.1. Gewaltenteilung und Zuständigkeitsverteilung

Die Richtigkeit der vordergründigen Aussage, keine Staatsgewalt dürfe bei der Informationsermittlung den Zuständigkeitsbereich einer anderen Gewalt verletzen, mag angesichts der thematischen Beschränkung auf die Verwaltung dahingestellt bleiben. Der Sinn der Gewaltenteilung liegt ja nicht — wie oben festgestellt — in der scharfen Trennung ihrer Funktionen [23]). Um so mehr interessiert hier der Aspekt der *Zuständigkeitsverteilung*. Sie ist hier verstanden als rechtlich fixierte Organisationsnorm und als „faktische Zuständigkeit" im Rahmen einer, über die Grenzen der formellen Organisation hinausreichenden, materiellen Aufgabenzuweisung. Hinsichtlich der Ermittlung von Individualinformationen läßt sich mit Hilfe der oben gewonnenen Erkenntnisse sagen: Da Informationen in den Willensbildungsprozeß der Verwaltung einfließen und der Willensbildungsprozeß sich im Rahmen der Zuständigkeiten abspielt, ist eine Ermittlung von Individualinformationen, die den Zuständigkeitsbereich überschreitet, ein Verstoß gegen das Gewaltenteilungsprinzip (Artikel 20 Abs. 3 GG) und damit gegen Artikel 2 Abs. 1 [24]). Dieses Ergebnis erscheint praktikabel. Es billigt der Verwaltung einerseits das Recht zu, Informationen in solchem Umfang zu ermitteln, wie dies für ein Funktionieren auch in unvorsehbaren Situationen nötig ist; andererseits grenzt es die Information nach Art und Menge gegen eine uferlose Ermittlung ab.

Zwischenergebnis

Aus der Prüfung am Wesensgehalt des Artikels 2 Abs. 1 und am Gewaltenteilungsprinzip ergibt sich:

Die Ermittlung von Individualinformationen ist nur zulässig, wenn die Verwaltung Informationen ermittelt, die im Hinblick auf das Verwaltungsergebnis als Minimal- oder Unterstützungsinformationen bezeichnet werden können. Die Ermittlung von Unterstützungsinformationen muß verhältnismäßig sein. Diese Zulässigkeitsbedingungen sind im Normalfall identisch mit dem Einhalten der Zuständigkeitsgrenzen durch die ermittelnde Behörde.

Auf diesem Wege ist es gelungen, ohne inhaltliche Fixierung eines in Artikel 2 Abs. 4 enthaltenen Persönlichkeitsrechts die Ermittlung von Individualinformationen über die Bestimmung der in der verfassungsmäßigen Ordnung liegenden Grenzen rechtlich in den Griff zu bekommen. Das Rechtsstaatsprinzip im übrigen ist dabei noch unberücksichtigt; es ist Gegenstand der folgenden Prüfung.

3.2.2. Rechtsstaatsprinzip

Im Rahmen der Prüfung am Rechtsstaatsprinzip werden die Gesichtspunkte „Freiheit vor unnötigen Eingriffen" und „Rechtsnatur der Ermittlung" zur Sprache kommen.

Freiheit vor unnötigen Eingriffen

Eingriffe in der Form der Ermittlung von Individualinformationen sind dann unnötig, wenn sie nicht an die verfassungsmäßige Ordnung gebunden sind, d. h., wenn sie den Wesensgehalt des Artikels 2 Abs. 1 (Verhältnismäßigkeit bei Unterstützungsinformationen) antasten oder den Zuständigkeitsbereich einer Behörde überspringen.

Diese Ausformung des Rechtsstaatsprinzips bringt also nichts Neues.

Gesetzmäßigkeit der Verwaltung

Wenn die Ermittlung von Individualinformationen einen Eingriff in das Grundrecht des Artikels 2 Abs. 1 darstellen kann, müssen diese Eingriffe auf einer gesetzlichen Grundlage beruhen. Insoweit ist also Kamlah im Ergebnis zuzustimmen [25]); zweifelhaft erscheint jedoch seine Ansicht bezüglich einer ungeschriebenen Kompetenz der Verwaltung zur Ermittlung eines Sachverhalts, wie sie § 161 StPO normiert [26]). Dies kann nur solange ein dürftiger Notbehelf sein, als ausdrückliche Eingriffsnormen für die Ermittlung von Individualinformationen auf bestimmten Gebieten noch fehlen — *wenn* sie überhaupt erforderlich sind.

Das wäre vor allem dann der Fall, wenn Informationsermittlung als VA zu qualifizieren wäre. Das ist nun zunächst zu prüfen.

3.3. Insbesondere: Die Verwaltungsaktqualität der Ermittlung

Individualinformationen können direkt vom Betroffenen, von Dritten oder aus den Umständen ermittelt werden. All diese verschiedenen Weisen der Ermittlung sind Gegenstand der folgenden Prüfung. Angesichts der Schwierigkeit, eine einigermaßen einheitliche Definition des Verwaltungsakts zu finden und zur Grundlage der Prüfung zu machen, soll hier eine Definition gewählt werden, die fußend auf § 26 MRVO in § 106 LVwG von Schleswig-Holstein und § 4 Berliner VwVG ihren Niederschlag gefunden hat, und deswegen für die Praxis weitgehend als verbindlich anzusehen ist:

Verwaltungsakt ist jede Verfügung, Entscheidung oder andere öffentlich-rechtliche Maßnahme, die eine Behörde zur Regelung eines Einzelfalles auf dem Gebiet des öffentlichen Rechts trifft und die auf unmittelbare Rechtswirkung nach außen gerichtet ist.

---

[23]) BVerfGE 9, 279

[24]) vgl. dazu auch die Fehlerhaftigkeit bzw. Nichtigkeit von VAen, die von einer unzuständigen Behörde erlassen worden sind.

[25]) Kamlah (3), 19

[26]) Kamlah (2), 363

3.3.1. „Regelung" eines Einzelfalls?

Problematisch ist in diesem Zusammenhang vor allem, ob die Informationsermittlung — gleich welcher Art — das Merkmal der Regelung erfüllt.

Nach allgemeiner Ansicht [27]) liegt eine Regelung dann vor, wenn die Maßnahme unmittelbare Rechtswirkung gegenüber einer Person hat. Dabei kann die Rechtswirkung darin bestehen, daß die Rechtsstellung einer Person verbessert, verschlechtert oder festgestellt wird. Man könnte nun folgendermaßen argumentieren: Die Verfügungsmöglichkeit des einzelnen über seine Individualinformationen gehört zu seinem durch Artikel 2 Abs. 4 GG geschützten Bereich. In jedem Fall wird zwischen Betroffenem und ermittelnder öffentlicher Stelle ein Rechtsverhältnis in der Weise festgelegt, daß durch diese und nur diese Informationen das Verhältnis zwischen Betroffenem und ermittelnder Stelle festgelegt wird. Schon die Tatsache, daß die Behörde Individualinformationen ermittelt, verschlechtert die in Artikel 2 Abs. 1 GG geschützte Rechtsposition, unabhängig davon, ob die Individualinformationen für ein rechtmäßiges Verwaltungsergebnis erforderlich sind oder nicht. Insofern begründet allein die Kenntnis der ermittelnden öffentlichen Stelle einen Eingriff. Auf die spätere — rechtmäßige oder rechtswidrige — Verwendung kommt es demgegenüber nicht entscheidend an. Dieser Eingriff unterliegt den Grundsätzen über Verwaltungsakte.

Für diese Auffassung finden sich bisher in Literatur und Rechtsprechung keine eindeutigen Belege. Zwar ist dem sog. Mikrozensus-Urteil des BVerfGs [28]) zu entnehmen, daß in Fällen, in denen dem Bürger eine *Rechtspflicht zur Herausgabe seiner Individualinformationen* auferlegt wird (vgl. das dort angefochtene Bundesstatistik-Gesetz), eine Regelung und damit ein Verwaltungsakt anzunehmen ist. Doch darf diese Entscheidung nicht dahin verallgemeinert werden, daß jede Ermittlung ein Verwaltungsakt ist. Soweit die Literatur überhaupt zu dem hier zu entscheidenden Problem Stellung nimmt, wird vielmehr angenommen, daß konkrete Tatsachenermittlungen nicht unter den Begriff Verwaltungsakt fallen [29]). Sie führen unmittelbar nur einen tatsächlichen Erfolg herbei, der die Bedingung für den künftigen rechtlichen Erfolg (nämlich den Erlaß eines Verwaltungsakts) erst herstellt [30]). Entscheidend an dieser Meinung ist, daß dem „Faktor Information" keine selbständige Bedeutung beigemessen wird. Das liegt daran, daß unser Verwaltungsrecht die je in den Kompetenzzuweisungen angegebenen Mittel vornehmlich auf das *Ergebnis*, nämlich Verwaltungsakt oder Leistungsbescheid, abstimmt. Der vorliegende Willensbildungsprozeß, der erst die Entscheidung ermöglicht, wird als Vorgang verwaltungsinterner Willensbildung aus dem Begriff des Verwaltungsaktes ausgeschieden. Eine Verbindung zwischen dem Verwaltungsergebnis, dem vorhergehenden Willensbildungsprozeß und den verwandten Informationen wird bisher noch nicht hergestellt.

Daß diese Auffassung heute nicht mehr haltbar ist, wurde oben bereits nachgewiesen. Freilich kann daraus andererseits auch nicht ohne weiteres die Konsequenz gezogen werden, daß *jede* Datenermittlung ein Verwaltungsakt sei. Schon die verfahrensmäßigen Besonderheiten bei Verwaltungsakten lassen ein derartiges Ergebnis als unpraktikabel erscheinen. Schließlich erscheint es fraglich, ob die Annahme der Verwaltungsaktqualität im Fall der Ermittlung bei Dritten so recht weiterhelfen kann. Wenn etwa der Dritte Individualinformationen an eine Behörde weitergibt, die er rein zufällig erfahren hat (z. B. der Dritte hat gesehen, daß der Betroffene jede Nacht eine andere Frau auf dem Zimmer hat), so darf er diese Kenntnisse ohne weiteres weitergeben, wenn er nur bei der Wahrheit bleibt. Jede andere Lösung müßte differenzieren je nach der Zweckbestimmung, die der Betroffene seinen nach außen dringenden Individualinformationen geben will. Eine solche Differenzierung muß — jedenfalls beim derzeitigen Stand der Diskussion — scheitern.

3.3.2. Ausweg

Nach allem bleibt festzuhalten: Die Informationsermittlung wird in vielen Fällen ein Verwaltungsakt sein, in anderen Fällen erscheint diese Annahme unpraktikabel und rechtlich bedenklich. Einer endgültigen Klärung dieses Problems durch Rechtspraxis und Rechtslehre kann durch dieses Gutachten nicht vorgegriffen werden, so reizvoll diese Aufgabe wäre. Andererseits kann die gegenwärtige Aufgabe des Gesetzgebers nicht von der zukünftigen Lösung eines rechtsdogmatischen Problems abhängig gemacht werden. Denn unabhängig davon, ob die Informationsermittlung als Verwaltungsakt angesehen werden kann oder nicht, ist soviel sicher: Der Bürger muß ein Recht haben, daß seine Individualinformationen in einer Weise ermittelt werden, die seine durch Artkeil 2 Abs. 1 geschützte Rechtssphäre nicht beeinträchtigen. Da zudem die Gefahr besteht, daß Individualinformationen, die einmal in den Bereich der Verwaltung gelangt sind, in einer nicht dem Willen des Betroffenen entsprechenden Weise verwandt werden, müssen schon in dieser Phase der Informationsverarbeitung verfahrensmäßige Besonderheiten den Interessen des Betroffenen Rechnung tragen [31]).

4. Datenschutzregelung

Die Achtung seiner Interessen kann der Bürger nur dann erreichen, wenn ihm Kontrollmaßnahmen zur Verfügung stehen, mit deren Hilfe die Rechtmäßigkeit einer Ermittlung überprüft werden kann. Als Kontrollmaßnahmen sind hier zunächst Ansprüche des Verwaltungsprozeßrechts, weiterhin aber auch in anderen Gesetzen enthaltene Möglichkeiten zur gerichtlichen Überprüfung zu verstehen. Um entscheiden zu können, ob diese Kontrollmöglichkeiten ausreichen, soll im folgenden die Rechtslage, wie sie

---

[27]) Wolff (1), 302 f.
[28]) BVerfGE 27, 1 ff.
[29]) etwa Wolff (1), 291
[30]) vgl. dazu Forsthoff (1), 191
[31]) zum Vorschlag eines subjektiv-öffentlichen Rechts auf ordnungsgemäße Informationsverarbeitung siehe unten

hinsichtlich einer Ermittlung besteht, dargelegt werden. Dabei wird zweckmäßigerweise davon ausgegangen, daß die Ermittlung grundsätzlich *kein* Verwaltungsakt ist. Die Darstellung der Rechtslage hat sich in die drei Fälle der Ermittlung zu gliedern: Ermittlung durch Befragen des Betroffenen, durch Befragen eines Dritten, durch Untersuchung bestimmter Umstände.

4.1. Ermittlung durch Befragen des Betroffenen

Nehmen wir einmal an, der Betroffene verweigert die Auskunft, dann ergibt sich folgendes:

Da es sich — wie vorausgesetzt — bei der Ermittlung, also der Anfrage, nicht um einen Verwaltungsakt handelt, kann der Betroffene auch nicht mittels Verwaltungszwangs zu einer Auskunft gebracht werden. Die Behörde kann jedoch den Befragten u. U., falls es sich um die Individualinformation „Personalien" handelt, wegen einer Übertretung nach § 360 Nr. 8 StGB anzeigen. Danach ist jeder Bürger verpflichtet, einer zuständigen Behörde seine Personalien bekanntzugeben. Dann aber ist das Erfragen der Personalien ein Verwaltungsakt. Kommt es dann unter den Voraussetzungen des § 153 Abs. 1 StPO (öffentliches Interesse an der Herbeiführung einer gerichtlichen Entscheidung; die Staatsanwaltschaft entscheidet darüber nach ihrem pflichtgemäßen Ermessen [32]) zum Prozeß, so wird zu prüfen sein, ob die ermittelnde Behörde „zuständig" war. Diese Prüfungsmöglichkeit trifft allerdings nur bei Personalien zu.

Ähnlich ist es, wenn in einem bestimmten Gesetz dem Bürger die Pflicht auferlegt wird, bestimmte Individualinformationen an eine ermittelnde Behörde abzugeben. Ein Beispiel ist § 10 Abs. 1 StatGes. Weigert sich der Bürger, so erläßt die ermittelnde Behörde einen Bußgeldbescheid wegen einer Ordnungswidrigkeit (§ 14 Abs. 1 StatGes i. V. m. § 35 Abs. 1 und Abs. 2 OWiG). Nach § 67 OWiG kann der Betroffene Einspruch einlegen; nach § 68 I OWiG entscheidet dann das Amtsgericht über die Rechtmäßigkeit des Bußgeldbescheides. Auch auf diesem Wege — dem eines speziellen Gesetzes — ist also eine gerichtliche Kontrolle möglich.

Beide aufgezeigten Wege werden jedoch von der Behörde entweder durch Strafanzeige oder Bußgeldbescheid initiiert. Die VwGO stellt dagegen dem Bürger Möglichkeiten zur Verfügung, selbständig von seiner Seite aus eine Kontrolle herbeizuführen.

Da die Ermittlung hier nicht als Verwaltungsakt angesehen wird, kommt nur eine allgemeine Leistungsklage in Betracht. Sie muß entsprechend den Bedürfnissen des Bürgers ausgestaltet werden; dazu gibt es folgende Möglichkeiten:

— *Unterlassungsanspruch* [33]):

Der befragte Betroffene hat die Möglichkeit, durch eine Unterlassungsklage die ermittelnde Behörde zu zwingen, ihre Fragen einzustellen. Jedoch hat die Sache einen Haken: Wird nämlich die Unterlassungsklage am Verwaltungsgericht rechtsanhängig, dann ist damit der Betroffene nicht davor geschützt, dennoch antworten zu müssen [34]). Bekanntlich hat die Erhebung einer Leistungsklage keinen Suspensiveffekt und so müßte der Betroffene warten, bis über seine Klage — vielleicht nach Jahren — endgültig rechtskräftig entschieden ist. Ausweg ist hier die Beantragung einer einstweiligen Verfügung nach § 123 VwGO. Nach dem Wortlaut des Absatzes 1 dieser Bestimmung kann das Gericht eine vorläufige Entscheidung bereits vor Klageerhebung erlassen. Die einstweilige Verfügung ist im Hinblick auf einen Unterlassungsanspruch ganz besonders von Bedeutung — und deswegen durchaus ein tauglicher Rechtsschutz —, wenn Eingriffe in Rechte des Antragstellers durch bloßes Verwaltungshandeln behauptet werden, ohne daß ein Verwaltungsakt vorliegt [35]). Auf diesem Wege können wenigstens Wiederholungen derselben Art von Ermittlungen verhindert werden [36]).

Das Gericht kann Unterlassungsklagen und darauf gestützten einstweiligen Anordnungen jedoch nur dann stattgeben, wenn der Befragte einen *Anspruch* auf Unterlassung geltend machen kann, d. h. der einzelne muß einen *Anspruch* darauf haben, daß die ermittelnde Behörde ihre Zuständigkeitsgrenzen einhält und nur Minimal- und Unterstützungsinformationen ermittelt. Dieser Anspruch ergibt sich direkt aus Artikel 2 Abs. 1; er ist subjektiv öffentlicher Art [37]).

Im Hinblick auf die Erfordernisse des Datenschutzes ist er wie folgt zu präzisieren und entweder in das Datenschutzgesetz oder — besser — in das Verwaltungsverfahrensgesetz einzufügen:

Es besteht ein subjektiv-öffentliches Recht darauf, daß im Hinblick auf das Verwaltungsergebnis (Verwaltungsakt) *nur* solche Individualinformationen ermittelt, erfaßt und verarbeitet werden, die sich als Minimal- und Unterstützungsinformationen im Rahmen der Zuständigkeit der erlassenden Behörde darstellen.

Mit Hilfe dieses Anspruchs kann der Bürger eine Unterlassungsklage mit Aussicht auf Erfolg geltend machen.

Ein zusätzlicher Schutz besteht noch darin, daß bei einer Anfechtung eines Verwaltungsergebnisses das Gericht inzidenter zu prüfen hat, ob die Verarbeitung derjenigen Informationen, die dem Verwaltungsergebnis zugrunde liegen, rechtmäßig war. Bei der Prüfung wird das Gericht zu berücksichtigen haben, daß im Laufe des Prozesses der Informationsverarbeitung immer weniger Informationen benötigt werden:

Es werden immer — und zulässigerweise — mehr Informationen ermittelt, als dann erfaßt, mehr Informationen erfaßt, als gespeichert, mehr In-

---

[32]) Dreher, vor § 360 N. 3

[33]) Der Unterlassungsanspruch kann eine Unterart der Leistungsklage sein — so Redecker - v. Oertzen § 42 N. 100.

[34]) oder er wird eben mit Sanktionen dazu gezwungen

[35]) Redecker - v. Oertzen § 123 N. 9

[36]) Münster OVGE 12, 162 ff.

[37]) Maunz - Dürig - Herzog, Artikel 2 N. 26

formationen gespeichert als verarbeitet werden. Dies entspricht dem normalen *Rechtsfindungsprozeß* des Juristen in der Verwaltung.

Der Unterlassungsanspruch reicht aber nicht aus: Ausgehend von der Prämisse des aus Artikel 2 Abs. 1 folgenden Selbstbestimmungsrechts muß der Bürger noch weitere Möglichkeiten haben; eine Kontrolle muß sich auch auf die Richtigkeit der gespeicherten — und vorher ermittelten — Individualinformation erstrecken.

— *Berichtigungsanspruch:*

Ein derartiger Anspruch ist in der Tat im öffentlichen Recht etwas Neues [38]). Er muß als eine Ausformung der allgemeinen Leistungsklage gedacht werden. Auch er muß mit einer einstweiligen Verfügung nach § 123 VwGO vorläufig durchsetzbar sein. Inhaltlich umfaßt er bei *zuwenig* ermittelter und gespeicherter Information ihre Ergänzung, bei *zuviel* ermittelter und gespeicherter Information die Streichung dieser Teile oder Informationen und bei entstellt gespeicherten Informationen ihre Entzerrung [39]). Dem Bürger ist damit ein brauchbares Instrument in die Hand gegeben, um sein Selbstbestimmungsrecht, auch bezogen auf den gespeicherten Inhalt von Individualinformationen, ausreichend zur Geltung zu bringen. Wohlgemerkt ist dieser Anspruch aber *nicht* zur Überprüfung der *Rechtmäßigkeit* der Ermittlung geeignet; er setzt lediglich das Selbstbestimmungsrecht des Bürgers auch nach der Ermittlung in die Tat um und mildert somit indirekt die von einer Ermittlung möglicherweise ausgehenden negativen Folgen. Endlich kommt es noch darauf an, die Folgen einer *rechtswidrigen* Ermittlung vollends beseitigen zu können.

— *Löschungsanspruch:*

Hat eine Behörde rechtswidrig — also beispielsweise außerhalb ihrer Zuständigkeit — Individualinformationen ermittelt, so werden diese Informationen gespeichert. Es ist nun das allergrößte Interesse des Befragten, diese Speicherung rückgängig zu machen, also die Informationen zu löschen. Die Löschungsklage ist dazu geeignet; sie wird bisher wohl überwiegend als Unterart der Leistungsklage verstanden [40]).

Die Klage ist begründet, wenn ein *Anspruch* des Betroffenen auf Löschung gegeben ist. Ebenso wie bei der Unterlassungsklage ergibt er sich aus dem subjektiv-öffentlichen Recht auf Einhaltung der Zuständigkeitsgrenzen und der Beschränkung auf Minimal- und Unterstützungsinformationen. Der Anspruch ist also begründet, wenn eine Behörde bei der Ermittlung dagegen verstoßen hat.

4.2. Ermittlung durch Befragen eines Dritten

Hier ändert sich die rechtliche Lage des Betroffenen in drei Punkten:

— Naturgemäß entfällt die Möglichkeit, über Sanktionen wie § 360 Nr. 8 StGB eine Überprüfung der Rechtmäßigkeit zu erreichen. Ist nämlich etwa der befragte Nachbar aussagewillig, so ist ein Schweigen des Betroffenen gegenstandslos. Umgekehrt ist allerdings die Behörde machtlos: Sagt der Nachbar nichts, so kann sie ihn rechtlich nicht zur Aussage zwingen.

— Sagt ein Dritter aus, so steht dem Betroffenen der *Unterlassungsanspruch* zu. Hier ist jedoch ganz vorsichtig vorzugehen, denn das aus Artikel 2 Abs. 1 folgende Selbstbestimmungsrecht kann sich wohl nicht darauf erstrecken, dem Nachbarn zu verbieten, etwas Wahres über den Betreffenden auszusagen. Wohl aber ist der subjektiv-öffentlich-rechtliche Anspruch auf Einhaltung der Zuständigkeitsgrenzen und auf die Beschränkung auf Minimal- und Unterstützungsinformationen unverändert aufrechtzuerhalten.

— Es ist möglich, wenn nicht sogar wahrscheinlich, daß der Betroffene von einer Befragung eines Dritten nichts weiß. Damit er dennoch seine Rechte durchsetzen kann, ist ihm ein *Auskunftsrecht* zu gewähren, das ihm den Inhalt der ermittelten Informationen und dem Zeitpunkt der Ermittlung offenlegt. Nur dies versetzt ihn in die Lage, von möglichen Rechtsverletzungen Kenntnis zu erlangen und gegen sie vorzugehen. Die Auskunft ist im Wege der *Leistungsklage* des Betroffenen durchzusetzen. Hinsichtlich des *Berichtigungs- und Löschungsanspruchs* ergibt sich nichts Neues.

  Bei der Ermittlung durch die Untersuchung bestimmter Umstände ergibt sich gegenüber dem zuletzt geschilderten Fall nichts Neues.

4.3.

Zusammenfassend kann gesagt werden, daß die Rechte des einzelnen bei der Ermittlung ausreichend gewahrt werden, wenn man einerseits die Verwaltung gesetzlichen Schranken bei der Ermittlung unterwirft und andererseits der Bürger die Einhaltung dieser Vorschriften nachprüfen und gerichtlich erzwingen kann, sowie einen Berichtigungs- und einen Löschungsanspruch erhält.

Eine Klassifizierung der Ermittlung als Verwaltungsakt würde vielleicht einen leichter durchschaubaren, kaum aber einen weitergehenden oder praktikableren Schutz bieten; auch deswegen ist es vertretbar, auf diese Klassifikation generell zu verzichten.

---

[38]) Vgl. dagegen im Privatrecht § 894 BGB; das öffentliche Recht kennt Berichtigungsansprüche im wesentlichen nur im Rahmen des Folgenbeseitigungsanspruchs.

[39]) hierzu vgl. die parallelen Erläuterungen unter E.IV.2.

[40]) Redecker - v. Oertzen, § 42 N. 97; Ule, 113; unentschieden BVerwGE 26, 169

5. Bedeutung der Ermittlung von Individualinformationen in einer integrierten Verwaltung

5.1. Allgemeines

Entscheidendes Kriterium der integrierten Verwaltung ist, daß zwischen den räumlich und eventuell organisatorisch getrennten Verwaltungsstellen technische Verbindungen (meist Datenfernverarbeitungslinien) bestehen, die einen *ungehinderten Austausch von Informationen* zwischen diesen Stellen ermöglichen. Dadurch kommt dem einmaligen Akt der Ermittlung erhöhte Bedeutung zu; denn nur das, was im integrierten System an Information vorliegt, kann ausgetauscht werden. Überspitzt ausgedrückt: Ermittlung ist potentieller Austausch. Deshalb ist es rechtspolitisch wünschenswert, bereits die Beschaffung von Informationen einer rechtlichen Regelung zu unterwerfen, also den Schutz vorzuverlegen: Nicht nur das Ergebnis bedarf der Kontrolle, sondern ebenso der dahin führende Weg. Befinden sich die ermittelten Individualinformationen dann innerhalb des Systems, so unterliegt der Austausch den dafür einschlägigen Regelungen. So ergibt sich, daß die hier gefundenen Regelungen für die Ermittlung auch bei integrierten Systemen ihren Wert behalten und grundlegend sogar rechtspolitisch an Bedeutung gewinnen. Vor allem ist das oben postulierte subjektiv-öffentliche Recht auf ordnungsgemäße Informationsermittlung grundlegend.

5.2. Problem der Sicherheitsverwaltung

Es gibt Behörden, deren legitimes Funktionieren davon abhängig ist, daß der Betroffene die Ermittlung ihn betreffender Informationen nicht erfährt. Es handelt sich um die Polizei bei der Verbrechensbekämpfung, um ärztliche IS, um Verfassungsschutz und Spionageabwehr u. ä. Von diesen Behörden hat lediglich die Polizei in § 161 StPO eine rechtliche Grundlage zur Informationsermittlung.

Würde man nun — entgegen der bisherigen Praxis — evtl. eine Bekanntgabe der Ermittlung fordern, so wäre die Effizienz der genannten Behörde wohl unzumutbar eingeschränkt. Von dieser Grundlage geht wenigstens das sog. „Abhörurteil" des BVerfG zu Artikel 10 Abs. 2 GG aus. Es ist hier nicht der Ort, die Problematik erschöpfend zu behandeln.

Der Lösung des Problems dienen folgende Grundsätze:

1. Es ist zu unterscheiden zwischen Behörden, deren Verwaltungsergebnis in einem Verwaltungsakt besteht, und anderen (z. B. BND).
2. Für erstere (z. B. Polizei) gilt nichts Besonderes: auch hier ist das Verwaltungsergebnis im Rahmen der gesetzlich vorgesehenen Verfahren auf Einhaltung der Zuständigkeit und der Ermittlungsbeschränkung auf Minimal- und Unterstützungsinformationen vom Gericht zu überprüfen.
3. Bei sonstigen Behörden (z. B. BND), die also nachher keinen Verwaltungsakt erlassen, ist der Informationsschutz auf andere Weise zu gewährleisten:

   Oberster Grundsatz ist, daß die Informationssysteme der Behörden von den allgemeinen staatlichen Informationssystemen völlig organisatorisch, technisch und juristisch getrennt aufgebaut und durchgeführt werden müssen. Keine Kopplung zwischen diesen speziellen und den allgemeinen öffentlichen Informationssystemen! Sie sind grundsätzlich auf eigene Informationsermittlung usw. beschränkt. Ein Zugriff auf die allgemeinen öffentlichen Informationssysteme steht ihnen nur insoweit zu, als er jedermann zusteht.

4. Jede darüber hinausgehende, also behördenfreundlichere Regelung ist wegen der unabsehbaren Folgen für den Individualdatenschutz abzulehnen.

6. Zusammenfassung

Im Vorangegangenen wurde geprüft, ob und inwieweit die Ermittlung von Individualinformationen durch die Verwaltung das Grundrecht aus Artikel 2 Abs. 1 einschränkt und unter welchen Voraussetzungen diese Einschränkungen zulässig sind. Aus den Ergebnissen dieser Prüfungen lassen sich folgende *Vorschläge* für den Gesetzgeber eines Datenschutzgesetzes ableiten:

— Alle Verwaltungsbehörden sind berechtigt, Individualinformationen zu ermitteln.

— Die Ermittlung ist jedoch in jedem Fall nur zulässig, wenn

  1. die ermittelnde Behörde ihren Zuständigkeitsbereich nicht überschreitet (eine Behörde ist zuständig im Sinne dieses Gesetzes, wenn sie durch formellen oder materiellen Organisationsakt [Aufgabenzuweisung] zur Erfüllung von Verwaltungsaufgaben berechtigt ist) *und*
  2. die zu ermittelnde Individualinformation im Hinblick auf das Ergebnis des Verwaltungshandelns als Minimal- oder Unterstützungsinformation anzusehen ist. Minimalinformationen sind Informationen, die zur Erstellung des Ergebnisses erforderlich sind. Unterstützungsinformationen sind Informationen, die Rückschlüsse auf die Richtigkeit der Minimalinformationen zulassen. Die Ermittlung von Unterstützungsinformationen ist nur zulässig, wenn sie im Hinblick auf den Wahrscheinlichkeitsgrad der Richtigkeit einer Minimalinformation verhältnismäßig ist.

Entsteht durch die Ermittlung ein Schaden, so hat der Geschädigte Anspruch auf Entschädigung. Darüber hinaus kann er Unterlassung weiterer Ermittlung, Beseitigung der ermittelten und Löschung der unberechtigt erhaltenen Informationen verlangen.

II. Topos Informationserfassung

1. Definition

Informationserfassung ist die Transformation von Informationen in Daten, namentlich — bei EDV — in maschinell verarbeitbare Daten.

Wenn beispielsweise eine Locherin einen Namen in eine Lochkarte stanzt, die dann der EDVA eingegeben wird, handelt es sich um Informationserfassung.

2. Schutzbereich

Die Informationserfassung als Übersetzen von Informationen in Daten kann dann eine Beschränkung von Artikel 2 Abs. 1 GG sein, wenn der Vorgang der Erfassung allein, ohne Rücksicht auf die vorangegangene Ermittlung, die nachfolgende Weitergabe oder den anschließenden Austausch, eine Entfaltung der Persönlichkeit beschränkt, indem sie das informationelle Selbstbestimmungsrecht einengt. Systemtheoretisch ist die Erfassung ein Schritt zur Bildung eines Personenmodells.

2.1. Verletzung des Persönlichkeitsrechts durch Erfassen

Für eine Verletzung des Persönlichkeitsrechts durch die Erfassung von Individualinformationen spricht folgendes: Bisher war eine Erfassung in manuell geführten Karteikästen relativ ungefährlich. Die technische Schwierigkeit, alle diese Aufzeichnungen zusammenzuführen und auf diese Weise ein umfassendes Persönlichkeitsbild zu erhalten, waren zu groß. Jetzt hat sich die Lage grundlegend geändert: Durch eine technische Erfassung gerät eine Individualinformation in ein System, das durch Computer gesteuert wird. Damit sind Zugriffs- und Austauschfrequenz technisch unbegrenzt, Veränderungen und Löschungen zunächst unkontrollierbar.

Vor allem können durch die Erfassung virtuell unbegrenzt viele Daten über jede Person akkumuliert und jeweils auf dem neuesten Stand gehalten werden. Dadurch entsteht ein umfassendes und stets aktuelles Personen- und Gruppenmodell, das — vorbehaltlich des Datenschutzes — allen interessierten Stellen für individuelle und Planungsentscheidungen uneingeschränkt zur Verfügung steht. Es ermöglicht Urteile über die Persönlichkeit des Betroffenen von Stellen, mit deren Beurteilung er nicht rechnen konnte. Diese Urteile fließen in das Persönlichkeitsmodell des Betroffenen zurück und beeinflussen es ebenso wie das Verhalten des Originals selbst, das von den Beurteilungen Kenntnis erhält. Auch die Rechtsprechung zum allgemeinen Persönlichkeitsrecht liefert ein Argument [1]): Der Mensch habe die Bestimmungsbefugnis darüber, „ob seine Worte einzig seinem Gesprächspartner, einem bestimmten Kreis oder der Öffentlichkeit zugänglich sein sollen"; das folge aus dem Rechtsschutz für seinen Persönlichkeitsbereich. Das Urteil betraf eine heimliche Tonbandaufnahme, gilt aber für alle Erfassungsarten. Überträgt man dies auf die technische Erfassung durch die Verwaltung, so ergibt sich auch in dieser Hinsicht ein Selbstbestimmungsrecht des Betroffenen [2]).

2.2. Argumente dagegen

Gegen die Verletzung des Schutzbereichs spricht folgendes:

Die vorhergehenden Ansichten verlangen die Beschränkung der Informationserfassung wegen der gesteigerten Möglichkeiten des Austausches und der Weitergabe. Nicht die Erfassung als solche steht also in Rede, sondern die durch sie eröffneten zusätzlichen Mißbrauchsmöglichkeiten bei Veränderung, Austausch und Weitergabe. Diese sind jedoch als selbständige Phasen der Informationsverarbeitung einer eigenen rechtlichen Bewertung unterworfen, die Mißbräuche ausschließen soll.

2.3. Zwischenergebnis

Damit kann durch die Erfassung an sich das Grundrecht aus Artikel 2 Abs. 1 nicht selbständig verletzt werden. Entscheidend für eine Verletzung ist ja nicht, *wie* die Individualinformationen fixiert werden, sondern *wer* darüber verfügt und *wozu* sie verarbeitet werden, und das ist allein eine Frage von Veränderung, Austausch und Weitergabe. Auch ein eigenes Rechtsschutzbedürfnis des einzelnen besteht nicht, zumal in kritischen Fällen bereits die Ermittlung gerichtlich überprüfbar ist.

3. Insbesondere: ist die Informationserfassung Verwaltungsakt?

Informationserfassung ist die Übersetzung von Informationen in fixierte, insbesondere (für EDV) in maschinell lesbare Daten.

Entsprechend dem oben zur Ermittlung Gesagten kann auch hier nur fraglich sein, ob die Erfassung im Sinne der gegebenen Verwaltungsaktdefinition eine Regelung mit unmittelbarer Außenwirkung darstellt.

[1]) BGHZ 27, 287

[2]) siehe Seidel, in: NJW 70, 1582 f. Seidel betrachtet das Problem als Speicherungsproblem. Das ist sachlich falsch: Der Vorgang der Erfassung eröffnet die Mißbrauchsmöglichkeiten; die Speicherung als solche läßt demgegenüber keine neue Lage eintreten.

Die Erfassung stellt gegenüber der Ermittlung keine Verwaltungstätigkeit dar, die selbständig einen Eingriff in den durch Artikel 2 Abs. 1 GG geschützten Bereich beinhaltet. Sie bleibt insofern ein verwaltungsinterner Vorgang, der keine unmittelbaren Außenwirkungen gegenüber dem betroffenen Bürger zeitigt: Die Datenermittlung bereitet die eigentliche Entscheidung der Verwaltung, die erst aufgrund der Informationen ergeht, nur vor. Dieses Ergebnis entspricht der derzeit ganz h. M. in der Verwaltungsrechtslehre.

Wie bereits bei der Datenermittlung betont wurde, ist es fraglich, ob diese Auffassung angesichts der Erkenntnis, daß die Verfügungsmöglichkeit über Individualinformationen zu der durch Artikel 2 Abs. 1 GG geschützten Sphäre gehört, aufrechterhalten bleiben kann. Überwiegende Gründe sprechen dafür, doch kann es nicht Aufgabe dieses Gutachtens sein, Theorien zu entwickeln, die zwar zutreffend und wegweisend erscheinen, aber im derzeitigen Stand der Diskussionen keinerlei Aussicht auf praktische Verwirklichungen haben.

Aus allem folgt freilich nicht, daß diese Phase der Informationsverarbeitung weiterhin im rechtsfreien Raum verbleiben darf. Auch hier sind — unabhängig von der Verwaltungsaktdiskussion — Regeln aufzustellen, die den Besonderheiten des Faktors Information in einem modernen Verwaltungs*verfahren* Rechnung tragen [3]).

[3]) s. o. TOPOS I.3.3.

4. Rechtliche Regelung

Zur Gewährleistung des Datenschutzes bei dem technischen Vorgang der Transformation der ermittelten Informationen in Daten steht ein reiches Repertoire an Datensicherungsmaßnahmen zur Verfügung, das stets auf dem technisch und organisatorisch letzten Stand im Rahmen des finanziell Zumutbaren gehalten werden muß.

5. Ergebnis

Abschließend kann somit festgehalten werden:

— Die Erfassung von Individualinformationen stellt keine eigene Verletzung des Schutzbereichs von Artikel 2 Abs. 1 dar. Eine eigene rechtliche Regelung erübrigt sich deshalb.

— Mangels Eingriffsqualität kann die Erfassung auch nicht als Verwaltungsakt bezeichnet werden.

— Geeignete und zumutbare Datensicherungsmaßnahmen sind generell vorzuschreiben. Ihre Aufzählung im einzelnen geschehe durch Rechtsverordnung. Ihre Geltungsdauer sei wegen des raschen Wandels auf drei Jahre beschränkt.

III. Topos Informationsspeicherung

1. Definition

Informationsspeicherung ist Festhaltung der erfaßten Information zur weiteren Verwendung.

Wird beispielsweise eine Information auf Magnetband festgehalten, so steht sie damit einer weiteren Verwendung jederzeit zur Verfügung.

2. Bedeutung

Die Bedeutung der Speicherung ist dreifach:

— Gespeicherte Informationen tragen zur Beeinflussung des internen Modells einer Person bei. Sie sind potentiell geeignet, später wieder zur Kenntnis des Betroffenen zu gelangen und so als neues Urteil der Umwelt auf seine Selbstentfaltung zurückzuwirken.

— Sind Informationen gespeichert, so stehen sie jeder weiteren Verarbeitung, sowie jedem weiteren Austausch und jeder Weitergabe offen. Die Speicherung ist damit geeignet, die Gefährdung von Individualinformationen vor unkontrollierter Verarbeitung zu steigern.

— Die Speicherung bewirkt es, für eine Verarbeitung durch EDV den Faktor Zeit und Ort weitestgehend auszuschalten. In integrierten Systemen ist es durch Datenfernverarbeitung möglich, praktisch unabhängig vom Speicherort in kürzester Zeit jede beliebige Individualinformation zu beschaffen.

3. Schutzbereich

Gegenüber der Erfassung stellt die Speicherung zunächst nur ihre verarbeitungstechnische Konsequenz und keine neue rechtliche Situation dar. Für die Mißbrauchsmöglichkeit ist entscheidend, daß die Information überhaupt der Verarbeitung zugänglich gemacht wird. Auf sie kommt es an, nicht auf die Speicherung.

Darum kann entsprechend dem oben zur Erfassung Gesagten festgestellt werden, daß die Speicherung als bloßer verwaltungsinterner Vorgang nicht unter den Begriff des Verwaltungsaktes fällt. In jedem Fall wäre die Speicherung keine selbständige Verletzung des Schutzbereiches von Artikel 2 Abs. 1, die selbständige Verletzung müßte dann schon bei der Informationsermittlung vorgelegen haben.

Anders verhält es sich bei integrierter Informationsverarbeitung: Hier wird die Information durch Spei-

cherung in einen prinzipiell dem Informanten (dem Abgebildeten) nicht mehr überblickbaren Kontext eingeordnet. Dieser Kontext ist die Daten- und Programmstruktur des integrierten Systems. Es ermöglicht die Vielfachbenutzung der gleichen Individualinformation durch alle dem integrierten System angeschlossenen Teilnehmer — nur nicht dem Betroffenen. Jede Zuordnung einer erfaßten Individualinformation zu einem weiteren Benutzer (Teilnehmer) bedeutet jedoch ihre Veränderung (auf pragmatischer Ebene) und — gegebenenfalls — einen Informationsaustausch. *Rechtlich* unterfällt also die Speicherung von Individualinformationen bei integrierten Systemen dem IV. und V. Topos.

4. Ergebnis

Abschließend wird festgestellt:

Die Speicherung ist kein selbständig regelungsbedürftiger Sachverhalt.

IV. Topos Informationsveränderung

1. Definition

Informationsveränderung wurde oben folgendermaßen definiert:

Informationsveränderung ist

1. die inhaltliche [1]) Umgestaltung einer gespeicherten Information, wobei sie für den Benutzer identifizierbar bleibt, also als *diese* Information wiedererkannt werden kann.
2. Die Verknüpfung von Informationen und die sich daraus ergebende Gewinnung neuer Informationen.
3. Eine Änderung der Benutzerzuordnung.

Schon der erste Blick auf die Definition zeigt, daß wir es hier mit unterschiedlichen Sachverhalten zu tun haben, die sich einer einheitlichen rechtlichen Beurteilung — so wie es bei den anderen „TOPOI" möglich war — entziehen. Es erscheint deshalb angezeigt, den Topos in Fallgruppen zu untergliedern und die Fallgruppen getrennt voneinander einer rechtlichen Würdigung zu unterziehen.

Entsprechend der Dreiteilung der Definition empfiehlt es sich, in folgende Fallgruppen zu unterscheiden:

I. Fallgruppe

Inhaltliche Umgestaltung einer Information — semantische Ebene —: *„Informationsverfälschung"*

II. Fallgruppe

Die Verknüpfung von Informationen und die sich daraus ergebende Gewinnung neuer Informationen — syntaktische Ebene —: *„Informationsverknüpfung"*

[1]) Umgestaltungen auf rein syntaktischer Ebene ohne inhaltliche Veränderungen sind zwar durchaus denkbar und machen sogar den Kern der automatisierten IV aus, bleiben jedoch für rechtliche Gesichtspunkte unergiebig, da der Betroffene dadurch nicht belastet wird. So ist die Umstellung von in ASSEMBLER gespeicherten Informationen auf FORTRAN ein rechtlich irrelevanter Vorgang.

[2]) Löschung läge vor, wenn die Steuerbehörde bei ihrem Zugriff keinerlei Antwort erhielte.

III. Fallgruppe

Die Änderung der Benutzerzuordnung — pragmatische Ebene —: *„Benutzeränderung"*

2. Informationsverfälschung

Fallgruppe I

Zunächst ist zu unterscheiden, ob die Informationsveränderung vor oder nach der Erfassung/Speicherung geschieht:

1. *Falscherfassung*
2. *Falschspeicherung*
3. *Falschverarbeitung* (durch geändertes bzw. verfälschtes Programm)

Nur so ist es nämlich möglich, von der definierten Veränderung den Sachverhalt einer Umgestaltung zwischen Ermittlung, Speicherung und Verarbeitung zu unterscheiden. Die Unterscheidung ist deshalb notwendig, da eine unterschiedliche rechtliche Bewertung nicht von vornherein auszuschließen ist.

2.1. Abgrenzung zur Informationslöschung

Die Unterscheidung von der Informationslöschung ist klar: wo eine Information nicht mehr identifizierbar ist, ist die Information nicht verändert, sondern gelöscht.

Zur weiteren Verdeutlichung sollen folgende *Beispiele* der Informationsverfälschung gebildet werden:

1. Durch einen Programmierfehler wird an die Summe des Jahreseinkommens von X eine Null angehängt.

   Greift die Steuerbehörde auf die Information „Jahreseinkommen X" zu, so erhält sie die veränderte Summe [2]).
2. Im Strafregister wird die Gefängnisstrafe von X gelöscht; dabei bleibt der Name von Y im Register stehen: das Feld, in dem die Gefängnisstrafe eingetragen war, bleibt leer [3]). Greift eine Justizbehörde auf die Information „Vorstrafen des Y"

zu, so erfährt sie, daß der Name Y im Register enthalten ist und das Vorstrafenfeld frei ist. Die Information ist damit inhaltlich geändert. Vorher hieß sie: „Y hat eine Gefängnisvorstrafe", jetzt eine „... Vorstrafe" (unbekannter Art). Auch hier erfährt die Behörde also etwas über die Information nach ihrer Veränderung, ja selbst nach ihrer scheinbaren Löschung.

3. Ein Mitglied des Bedienungspersonals einer EDVA gibt der Anlage falsche Informationen ein, um ein Verwaltungsergebnis zu verfälschen.
4. Ein Programmierer verändert das Programm, um ein Verwaltungsergebnis zu verfälschen.

Derartige inhaltliche Umgestaltungen können durch Umwelteinflüsse oder durch Personen vorgenommen werden.

a) Die Verhinderung schädigender *Umwelteinflüsse* ist ein Problem der Datensicherung. Rechtliche Regelungen können sich allerdings nur an Personen richten, die die Umwelteinflüsse zu verantworten oder ihre Folgen nicht verhindert haben.

b) Die Umgestaltung durch *Personen* umfaßt jede schuldlose oder schuldhafte Veränderung von Zeichen, die einer Information zugehörig sind, durch Eingabe anderer Daten oder (veränderter oder neuer) Programme. Die fahrlässige Veränderung ist ein naheliegender Fall: Ein Programmierfehler kann eine gespeicherte Information verfälschen, ein Verwaltungsangestellter macht eine Eintragung auf einer Karteikarte irrtümlich unkenntlich.

Auch die Umgestaltung durch Personen ist zunächst ein Datensicherungsproblem, soweit es sich darum handelt, technische, personelle und organisatorische Maßnahmen zur Verhinderung der Umgestaltung durch Personen einzuführen. Die Einführung selbst geschieht wieder durch geeignete Rechtsnormen (siehe unter Datensicherung).

Trifft der Staat nicht die notwendigen Vorkehrungen, so muß er die nachteiligen Folgen für den Staatsbürger ausgleichen. Dies geschieht vor allem durch die Amtshaftung. Zunächst unterliegt der Staat als Verwaltungsträger der Haftung nach § 839 BGB i. V. m. Artikel 34 GG, die ihn im Haftungsfalle berechtigt, gegen den Beamten (im haftungsrechtlichen Sinn), der seine Amtspflicht verletzt hat, in Regreß zu gehen, wenn dem Beamten Vorsatz oder grobe Fahrlässigkeit zur Last fällt. Diese Folge ergibt sich bereits aus dem geltenden Recht und ist deshalb nicht noch einmal zu normieren.

Geschieht die Informationsverfälschung schuldlos, so versagt der Schutz des § 839 BGB. Hierfür muß ein Gefährdungshaftungstatbestand eingeführt werden — so die inzwischen herrschende Meinung [4]).

Als strafrechtliche Sanktionen — allerdings lediglich für den EDV-Bereich — könnte § 268 I StGB zur Anwendung kommen und so die Schaffung einer neuen Strafnorm überflüssig machen. Er lautet:

Wer zur Täuschung im Rechtsverkehr

1. eine unechte technische Aufzeichnung herstellt oder eine technische Aufzeichnung verfälscht oder
2. eine unechte oder verfälschte technische Aufzeichnung gebraucht,

wird mit Freiheitsstrafe bis zu fünf Jahren bestraft.

Dabei ist zunächst fraglich, ob die inhaltliche Umgestaltung einer Information im gespeicherten Zustand selbst oder nur das mit Hilfe der veränderten Information erstellte neue Ergebnis von § 268 StGB erfaßt wird. Die Beantwortung der Frage hängt davon ab, ob eine Information in gespeichertem Zustand eine „technische Aufzeichnung" im Sinne des § 268 StGB ist. Nach der in § 268 II enthaltenen Legaldefinition wäre dazu erforderlich, daß der Gegenstand der Aufzeichnung allgemein ist. § 268 II StGB lautet:

Technische Aufzeichnung ist eine Darstellung von Daten, Meß- oder Rechenwerten, Zuständen oder Geschehensabläufen, die durch ein technisches Gerät ganz oder zum Teil selbständig bewirkt wird, den Gegenstand der Aufzeichnung allgemein oder für Eingeweihte erkennen läßt und zum Beweis einer rechtserheblichen Tatsache bestimmt ist, gleichviel ob ihr die Bestimmung schon bei der Herstellung oder erst später gegeben wird. Daraus ergibt sich, daß die inhaltliche Umgestaltung einer gespeicherten Information keine Herstellung oder Fälschung technischer Aufzeichnungen ist [5]). Regelmäßig dürfte jedoch gelten, daß die Informationsänderung vom Vorsatztäter als Vorstufe verstanden wird, um einen der Wirklichkeit nicht entsprechenden Ausdruck zu erzielen, der dann als technische Aufzeichnung zu bezeichnen ist [6]). *Somit ist die inhaltliche Veränderung von gespeicherten Informationen bereits in fast allen Fällen ein Versuch des § 268 Abs. 1,* der dann im Falle eines mit dieser veränderten Information zustande gekommenen Ausdrucks vom vollendeten Delikt des § 268 Abs. 1 (Fälschung) konsumiert wird.

---

[3]) Löschung läge vor, wenn auch der Name des Y aus dem Strafregister gelöscht würde. Die Behörde hätte dann hinsichtlich der Vorstrafen des Y keinerlei Anhaltspunkte.

[4]) vgl. hierzu Berger und Dagtoglou

[5]) Die Literatur (vgl. anschließende Fußnote) stimmt dem im Ergebnis zu, hauptsächlich wohl deshalb, weil mangels Kenntnis der Verarbeitungsvorgänge das Problem nicht gesehen wurde.

[6]) so Dreher, § 268 Anm. 3 c, Lampe, 1066 ff. A. a. Kienapfel 165. Kernpunkt des Streites ist die Abgrenzung der Begriffe „technische Aufzeichnungen" und „Urkunde". Während Kienapfel darauf abstellt, ob das Produkt noch Urkundencharakter hat, ist nach der Meinung der übrigen Autoren die Selbsttätigkeit der maschinellen Herstellung entscheidend. Kienapfel kommt konsequenterweise hier zur Anwendung des § 267 bzw. § 348 StGB. Da eine Pönalisierung in jedem Falle vorliegt, braucht hier auf den Streit nicht weiter eingegangen zu werden.

Der Fall der *Programmänderung* fällt unter § 268 III: Es handelt sich um eine störende Einwirkung, wenn der ordnungsgemäße Gang der Anlage beeinflußt wird und es sich dabei um den maschinellen Vorgang handelt. Der Arbeitsgang der Maschine wird jedoch ausschließlich von Programmen bestimmt, so daß ihre Veränderung gleichbedeutend ist mit einer Beeinflussung des maschinellen Vorgangs.

Der Fall des *„Fütterns" mit falschen Informationen* ist dagegen mit dem der inhaltlichen Veränderung gleichzubehandeln: Gelangen die falschen Informationen in den Arbeitsspeicher (und sind deswegen potentiell zur Erstellung eines falschen Ergebnisses geeignet), so liegt Versuch des § 268 vor. Kommt es zum Ausdruck des falschen Ergebnisses, so liegt vollendete Tat nach § 268 vor [7] [8]).

Bei dieser Sachlage ist ein kriminalpolitisches Interesse an einer eigenen Pönalisierung der Informationsveränderung nicht mehr erkennbar. Die Schaffung einer eigenen Strafnorm ist somit überflüssig.

Entsprechend dem aus Artikel 2 Abs. 1 GG hergeleiteten Selbstbestimmungsrecht des einzelnen an seinen Informationen muß ihm im Falle einer inhaltlichen Veränderung ein *Berichtigungsanspruch* gegen die speichernde Behörde gegeben werden. Für manuelle Informationsverarbeitung gelten strafrechtlich die §§ 263, 267 bzw. 348 StGB; der Berichtigungsanspruch gilt auch hier unverändert.

3. Informationsverknüpfung

Fallgruppe II

3.1. Erläuterung

Die Fallgruppe „Informationsverknüpfung" umfaßt zwei Tatbestände:

1. die Informationsverknüpfung ohne Erstellung eines weiteren Ergebnisses über diese Verknüpfung hinaus (z. B. die Information „A ist vorbestraft" wird in den Informationszusammenhang der bisher über A gespeicherten Individualinformationen einsortiert),
2. den Vorgang der eigentlichen Datenverarbeitung zwecks Erzielung eines neuen Resultats.

Der erste Fall hat darum prinzipiell Bedeutung, weil er den Grundtatbestand der integrierten Datenverarbeitung darstellt: durch Informationsverknüpfungsvorgänge entstehen die ungeheuren Möglichkeiten, ebenso aber auch die entsprechenden Gefahren der EDV.

Gleichwohl ist rechtlich dieser Vorgang der „Informationseinordnung" der normalen Informationsverknüpfung zwecks Erzielung eines neuen Ergebnisses gleich zu behandeln und wird darum im folgenden nicht gesondert erörtert.

Hierher gehört auch der Fall, daß das Programm geändert wird oder ein unverändertes Programm mit falschen Informationen in Verbindung gebracht wird, die richtigen aber dabei unverändert weiterbestehen. Das ist z. B. der Fall, wenn anstelle des richtigen ein falsches Magnetband verarbeitet wird, das richtige aber unversehrt aufbewahrt bleibt. Mit Verknüpfung soll also nun vor allem der Vorgang der Datenverarbeitung i. e. S. gemeint sein: Das Zugreifen auf mindestens zwei gespeicherte Informationen, um mit ihnen eine logische Operation durchzuführen. EDV-technisch ist dies der Fall, wenn Informationen vom Arbeitsspeicher durch Programmbefehl ins Rechenwerk gelangen und dort verarbeitet werden. Zur Verdeutlichung zwei Beispiele:

— Die Steuerbehörde berechnet aus den Informationen „Xaver X" und „Jahreseinkommen 20 000 DM" und anderen Informationen die neue Information „Steuerlast des X". Die Verknüpfung geschieht durch ein Programm. Ein Programmbefehl könnte nun zur Folge haben, daß „Xaver X" nicht mit „Jahreseinkommen 20 000 DM", sondern mit „Jahreseinkommen 200 000 DM" verknüpft wird, wobei letzteres ursprünglich mit der Information „Franz Y" verknüpft war.

— Die Polizei ermittelt gegen X wegen Mordverdacht; dabei kommt heraus, daß X einen beschädigten Pkw fährt. Da der Polizei bekannt ist, daß ein Mann wegen Fahrerflucht gesucht wird, der einen beschädigten Pkw fährt, nimmt sie den Wagen des X zum Anlaß, nun gegen X wegen Fahrerflucht zu ermitteln. Während also zuerst die Verknüpfung Mordverdacht — beschädigter Pkw bestand, änderte sie sich in die neue Verknüpfung Fahrerflucht — beschädigter Pkw.

Gegenüber der Fallgruppe I ist zunächst hervorzuheben, daß die *Speicherung von Informationen nicht Voraussetzung* für ihre Verknüpfung ist. Zwar ist es technisch gesehen notwendig, vor einer Rechenoperation in einer EDVA den an der Operation beteiligten Informationen einen Speicherplatz zuzuweisen (so im ersten Beispiel), der Polizist jedoch, der einerseits vom beschädigten Pkw des X weiß und andererseits gerade mündlich von der Fahrerflucht erfährt, verknüpft die Informationen „beschädigter Pkw des X" und „Fahrerflucht" sozusagen geistig — also ohne sie sich zu notieren — und nimmt bei gegebenen Voraussetzungen X auf Grund der vorgenommenen Verknüpfung sofort fest.

3.2. Rechtliche Regelung

Verknüpfung ist also ein Problem jeglicher Art von Informationsverarbeitung. Schwierigkeiten macht aber die Herausarbeitung eines rechtlichen Aspekts. Die Fragestellung lautet: *Unter welchen Voraussetzungen sind Verknüpfungen von Individualinformationen rechtlich zulässig?* Oder, um an das letzte Beispiel anzuschließen: Ist für eine Verhaftung die vom Polizisten vorgenommene Verknüpfung rechtmäßig? Allgemeiner: *Welche Individualinformationen dürfen zur Bildung von Entscheidungen verknüpft werden?*

[7]) vgl. C. Schneider (1), 243; Mrachacz - Bauer, 27

[8]) Der sog. „Programmierbetrug" kommt schon so häufig vor, daß sich bereits eine eigene Berufssparte zur Überprüfung derartiger Handlungen herausgebildet hat; vgl. dazu Steinmüller (1), 113.

Hierzu wurde anläßlich der Umformung (von statistischen Einzelinformationen usw.) und zur Erstellung des Personenmodells (durch Verknüpfung von Individualinformationen) das Nötige ausgeführt: Die Verknüpfung unterliegt dem Schutzbereich des Artikels 2 Abs. 1 GG, sofern sie Individualinformationen *betrifft* und/*oder erzeugt*. Mit anderen Worten, sie sind zulässig im Rahmen der Zuständigkeit der jeweiligen Behörden, vorbehaltlich der Zulässigkeit eines Informationsaustausches.

Und jetzt ist ersichtlich, daß es — rechtlich — auf den Vorgang der Verknüpfung allein nicht ankommt, sondern das Problem grundsätzlicher gefaßt werden muß: Welche Individualinformationen darf eine Behörde verarbeiten, wenn sie Entscheidungen fällen will? *Hier ist der Sitz des rechtlichen Problems: Unter welchen Voraussetzungen ist ein Zugriff einer Behörde auf eine Individualinformation rechtmäßig?*

Durch die Verknüpfung entsteht das Persönlichkeitsbild, also das zu schützende Personenmodell. Zwar ist es bereits in den ermittelten und erfaßten Informationen sowie den Verarbeitungsprogrammen enthalten; es kommt also — scheinbar — nichts Neues hinzu, außer eben dieser aktuellen Inbeziehungsetzung der Informationen zueinander. Auch hier gilt der bisherige Grundsatz: Das Problem liegt bei der Ermittlung; was ermittelt ist, ist grundsätzlich der staatlichen Informationsverarbeitung zugeführt und muß entsprechend geschützt werden, auch im Stadium der Verknüpfung.

Damit reduziert sich aber das Problem der Zulässigkeit von Informationsverknüpfung auf die Frage der Zugriffsberechtigung, zuletzt der Informationsermittlung: Die Behörde darf nur die und alle die Informationen verknüpfen, die sie selbst rechtmäßig ermittelt hat.

Dabei treten drei Fälle auf:

1. Eine Behörde greift auf Informationen zu, die sie selbst ermittelt hat (= *„eigene Informationen"*).
2. Eine Behörde greift auf Informationen zu, die ein Dritter ermittelt hat, sei es eine andere Behörde oder ein Privater (*„fremde Informationen"*).
3. Integrierte Datenverarbeitung: Auch hier greift die verarbeitende Behörde entweder auf eigene oder fremde Informationen zu, die sie also selbst oder durch Dritte ermittelt hat.

Der zweite Fall ist bei Ermittlung durch eine Behörde ein Fall des Informationsaustausches und -verbundes und unterfällt damit den dafür unten vorgeschlagenen Regelungen.

Der dritte Fall der integrierten Informationsverarbeitung ist entweder wieder ein Fall des Informationsaustausches und Informationsverbundes, oder er ist ein Fall der Verarbeitung eigener Informationen.

So bleibt also als einziges hier zu behandelndes Rechtsproblem nur der erste Fall: Der Zugriff einer Behörde auf eigene Informationen.

3.2.1. Verarbeitung eigener Informationen

Betrachten wir dabei zunächst den Fall der gewöhnlichen Datenverarbeitung wie er der Berechnung der Lohnsteuer im 1. Beispiel zugrunde liegt: Um ein bestimmtes Verwaltungsergebnis zu erstellen, ermittelt eine Behörde Informationen, erfaßt und speichert sie und macht sie zur Grundlage ihrer Entscheidung. Die rechtliche Frage lautet jetzt: Ist der Zugriff auf eine bereits von der Behörde ermittelte Individualinformation eine zusätzliche Beschränkung von Artikel 2 Abs. 1, wenn er sich im Rahmen des bei der Ermittlung vorgestellten Verwaltungsergebnisses hält? Dies kann nicht der Fall sein, da es sich um einen rein internen Vorgang handelt.

Selbst wenn man einen Verwaltungsakt annähme — was abwegig ist — würde es einer Klage am Rechtsschutzbedürfnis fehlen. Denn akzeptiert man einerseits den im Gutachten gemachten Regelungsvorschlag zur Ermittlung von Individualinformationen, so ist eine gerichtliche Kontrolle der Informationen, auf die die Verwaltung zugreifen darf, z. T. bereits vor dem Zugriff angesiedelt. Sei es Verwaltungsakt oder schlichtes Verwaltungshandeln, es ist mit den Mitteln der VwGO gerichtlich nachprüfbar, wobei das Gericht nach § 86 VwGO die Pflicht hat, den Sachverhalt von Amts wegen zu erforschen; d. h., die Informationen auf ihre einwandfreie Verarbeitung hin zu untersuchen, die zur Grundlage der Entscheidung gemacht worden sind. Dabei wird genau zu prüfen sein, was hier in Rede steht: Darf die Behörde zur Begründung ihrer Entscheidung auf eine Information zugreifen? Unrichtigkeiten der Information gehen dabei zu Lasten der Behörde [9]).

Angesichts dieser zweifachen gerichtlichen Kontrollmöglichkeit ist ein ausreichender Schutz der Rechte des einzelnen gewährleistet. Der Zugriff einer Behörde auf von ihr selbst ermittelte Informationen bedarf keiner eigenen Regelung in einem Datenschutzgesetz.

3.2.2. Ergebnis

Darum gilt die Regel:

Jede Behörde darf stets auf die Informationen zugreifen, die sie rechtmäßig ermittelt hat [10]). Hat sie die Informationen von einer anderen Behörde erhalten, so ist die Regel folgendermaßen zu modifizieren:

Jede Behörde darf stets auf die Informationen zugreifen, die sie in rechtmäßigem Austausch erlangt hat. Dabei ist zu berücksichtigen, daß eine Doppelspeicherung der ausgetauschten Individualinformationen bei der verarbeitenden Behörde unzulässig ist.

Dies war zunächst für den Normalfall der Informationsverarbeitung gesagt, gilt aber auch für *andere Spielarten* dieses Vorgangs, z. B.:

— Eine Individualinformation, ermittelt im Hinblick auf ein Verwaltungsergebnis A, wird für ein Verwaltungsergebnis B verwendet (2. Beispiel).

Alle Spielarten sind datenschutzrechtlich durch die Kontrolle von Ermittlung bzw. Austausch, sowie der

[9]) BVerfG DVBl 60, 489
[10]) so zutreffend Kamlah (3), 22

Programme und der Kontrolle des Verwaltungsergebnisses ausreichend geregelt.

Hinzu kommt noch die erwähnte strafrechtliche Erfassung des EDV-Bereichs durch § 268 StGB.

3.3. Informationsverdichtung

Ein besonderer Fall der 2. Fallgruppe ist noch die *Informationsverdichtung.*

Informationsverdichtung kann definiert werden als die Zusammenfassung oder Auswahl vieler Einzeldaten nach vorgegebenen Gesichtspunkten.

Beispiele:

Das Bayerische Ministerium für Umweltschutz erstellt eine Statistik, welche Müllmengen für Haushalte bestimmter Größenordnung charakteristisch sind.

Oder: Dasselbe Ministerium verlangt von der Datenzentrale eine Liste derjenigen Grundbesitzer, die Eigentümer von Campingplätzen sind.

Beide Beispiele stehen für die möglichen Fallgruppen der verdichteten Informationen: Sie enthalten nur Sachangaben ohne bzw. mit Individualangaben ohne/mit Weitergabe dieser Informationen an Dritte.

Das Verdichtungsproblem läßt sich demnach auf die Unterscheidung von statistischen Informationen und Individualinformationen zurückführen. Enthalten die verdichteten Informationen Angaben, die einzeln bestimmte Personen betreffen, so ist ihre Weitergabe an andere Behörden ein *Informationsaustausch* und unterliegt den dafür vorgesehenen Regelungen. Handelt es sich dagegen um rein statistische Informationen, vermag sie eine Person also nicht als Individuum zu kennzeichnen, so sind diese Informationen potentieller Gegenstand des Datenschutzes insoweit, als dem Empfänger der statistischen Informationen die nötigen Zusatzinformationen zur Verfügung stehen, um die statistischen in Individualinformationen zu *überführen.*

4. Änderung der Benutzerzuordnung

Fallgruppe III

Im Unterschied zur zweiten Fallgruppe handelt es sich hier nicht darum, auf welche Informationen zugegriffen werden darf, sondern welcher Behörde eine Information zur Verfügung steht, d. h., wer auf eine Information zugreifen darf.

Hier sind drei Fälle denkbar:

— Die Ermittlungsbehörde ist auch Benutzer der ermittelten Informationen. Hier hat sich der Benutzer nicht geändert.

— Eine Behörde wird Benutzer, die die gewünschten Informationen nicht selbst ermittelt, sondern von einer anderen Behörde erhalten hat. In diesem Fall werden die Rechte des einzelnen durch die Regelungen über den *Informationsaustausch* gewahrt.

— Eine Behörde wird Benutzer, indem sie auf Informationen zugreift, die sie nicht ermittelt, sondern von Privaten erhalten hat. In diesem Fall werden die Rechte des einzelnen durch die Regelung über die Ermittlung durch Behörden einerseits und die Weitergabe durch Private andererseits geschützt.

Alle drei Fälle sind also in bestehende „Topoi" einzuordnen und dort zu erörtern.

Vorbemerkung zu den Topoi V bis VII — Informationsweitergabe

4.1. Fallgruppen

Auch die Informationsweitergabe zerfällt sachlich in mehrere Fallgruppen, die sich etwa wie folgt aufgliedern lassen:

1. Fallgruppe

Informationsveröffentlichung

Die Behörde A (Finanzamt) gibt die Individualinformation X („X hat 20 000 DM unterschlagen") frei, z. B. an die Öffentlichkeit (z. B. Presse).

2. Fallgruppe

Informationsaustausch und (öffentlicher) Informationsverbund

Behörde A gibt X an eine andere Behörde B (Staatsanwaltschaft)

oder: B verlangt X von A.

Hier ist je nach Stellung der Behörden zueinander zu unterscheiden:

Unterfall 1: Behörde B hat keinen Anspruch auf X.

Unterfall 2: Behörde B hatte X im Wege der Amtshilfe von der Behörde A verlangt.

Unterfall 3: Behörde B hat Auskunftsrecht auf das IS der Behörde A.

Unterfall 4: Behörde B hat Zugriffsrecht auf das IS der Behörde A.

Unterfall 5: Behörden B und A haben das gleiche IS („integrierte DV").

3. Fallgruppe

Informationsweitergabe an/von Private(n) und Verbund Staat-Wirtschaft

oder: Behörde A gibt (bzw. fordert) X an (bzw. von) Privatperson/Unternehmen C

oder: C verlangt X von A.

Hier bestehen grundsätzlich die gleichen Unterfälle.

Die Unterfälle von 2. bzw. 3. bezeichnen im wesentlichen verschieden starke Grade der Koppelung zwischen den Systemen A, B, C.

4.2. Grundproblem

Das *grundsätzliche Problem* des Informationsaustausches besteht darin, daß — pragmatische Ebene der Information — die Individual-(und Gruppen-)-information durch Wechsel des Benutzers einen anderen „Sinn" bekommt (vgl. die Beispiele zur Informationsveränderung und die Bedeutung des AIS).

Es ist eben nicht das gleiche, ob die — syntaktisch und semantisch identischen — Informationen „A ist Syphilitiker" bzw. „B ist Anhänger der KPD" sich in der Hand des Arztes, einer Polizeidienststelle oder des lieben Nachbarn befinden, vielleicht gar für alle Benutzer eines integrierten, Staat und Wirtschaft umfassenden Nationalen Informationssystems offenstehen, *oder* — und darauf kommt es an — ob nur jeder die *ihm zustehenden* Informationen erhält.

Der *grundsätzlich rechtlichen Lösung* dieses Grundproblems ist damit der Weg gewiesen: Jeder darf alle, aber nur die Informationen erhalten, die er zur Erfüllung seiner legitimen Aufgaben (für den Staat: im Rahmen seiner Zuständigkeiten) braucht.

Alles übrige ist im Grunde (technisch-finanziell-organisatorische) Durchführung dieses Prinzips.

Diese Durchführung ist *notwendig und möglich,* und zwar sowohl nach dem derzeitigen Stand, als auch nach den organisatorischen und rechtlichen Möglichkeiten des Staates.

4.3. Aufbau

Die drei wichtigsten Fallgruppen bilden — in etwas anderer Einteilung — wegen ihrer Bedeutung eigene Topoi; es sind dies

— Informationsaustausch (Topos 5),

— Informationsweitergabe an Dritte (Topos 6),

— Informationsverbund (Topos 7).

Die Informationsveröffentlichung ist rechtlich Topos 6 gleichzubehandeln (unten VI. 4.).

V. Topos Informationsaustausch

1. Definition und Bedeutung

1.1. Informationsaustausch

Informationsaustausch als Informationsweitergabe innerhalb der Verwaltung sei hier beschränkt auf die *Weitergabe von Individualinformationen innerhalb der öffentlichen Verwaltung.* „Weitergabe" impliziert, daß *eigene Daten* weitergegeben werden, daß also die empfangende Behörde die Daten nicht selbst ermittelt hat.

Mit dem Informationsaustausch ist wohl der neben der Ermittlung rechtlich *schwierigste Sachverhalt* in das Blickfeld der Erörterung gerückt. Er zeichnet sich durch zwei *Besonderheiten* aus:

— Die Häufigkeit des Informationsaustausches wächst mit der Zunahme der integrierten Datenverarbeitung nicht proportional, sondern exponentiell an. Damit wird der Austausch — im Gegensatz zur bisherigen rechtlichen Würdigung [1]) — Objekt verschärfter rechtlicher Auseinandersetzung sein.

— Informationsaustausch findet dann statt, wenn eine Behörde auf Informationen, die sie selbst nicht ermittelt hat, von einer anderen Behörde, die diese Informationen ermittelt hat, einholt. Sie tut das bisher meist mit einer Bitte um Auskunft. Dieser Vorgang wird bisher durch das Recht der Rechts- und Amtshilfe erfaßt [2]), das bereits in den §§ 4 bis 7 EVwVfG und §§ 32 bis 36 LVwG von Schleswig-Holstein normiert ist. Sind diese Vorschriften in der Lage, den Sachverhalt, wie er sich auch unter den Bedingungen der integrierten Datenverarbeitung darstellt, im Hinblick auf den Prüfungsmaßstab Artikel 2 Abs. 1 ausreichend zu erfassen, so ist Datenschutz beim Austausch von Individualinformationen ein Problem der Änderung des Amtshilfe- bzw. Rechtshilferechts. Die Untersuchung würde dann die Normen des EVwVfG zum Prüfungsgegenstand haben. Trifft dies zu? Von der Antwort auf diese Frage hängt der Fortgang der weiteren Prüfung ab.

1.2. Die Bedeutung des Informationsaustausches bei integrierter Datenverarbeitung

Es ist ein Merkmal herkömmlicher Verwaltungstätigkeit, daß jede öffentliche Stelle die Information, die sie zur Erfüllung ihrer Aufgaben braucht, *im wesentlichen selbst* ermittelt, selbst erfaßt, speichert und weiterverarbeitet [3]). So kommt es dazu, daß an vielen Stellen öffentlicher Verwaltung dieselben Informationen über eine Person vorhanden sind. Anders ausgedrückt: Im wesentlichen durchläuft jede Verwaltungsstelle den ganzen Prozeß der Informationsverarbeitung, unabhängig davon, ob die zu verarbeitenden Informationen bereits

[1]) Die letzte Monographie über die Amtshilfe erschien 1959!
[2]) Düwel, 92
[3]) Steinmüller (1), 73

anderen Verwaltungsstellen zur Verfügung stehen und der betreffenden Stelle zugänglich gemacht werden könnten. Eine Verwaltungsvereinfachung, die auf höhere Effizienz des Verwaltungshandelns abzielt, muß demnach an diesem Punkt ansetzen: Sie muß erreichen, daß die einzelnen Verarbeitungsphasen nicht alle gleich oft, sondern weniger häufig im Hinblick auf die Effizienz der gesamten Verwaltungstätigkeit durchlaufen werden [4]). Konkret heißt das: weniger Ermittlung und Erfassung, mehr Austausch [5]). Das technische Hilfsmittel, dieser Forderung zum Sieg zu verhelfen, heißt EDV. Nur damit ist es möglich, den Informationsfluß so zeitsparend auszugestalten, daß er arbeitstechnisch effizienter verläuft als eine neuerliche Ermittlung und Erfassung. Ist dieser Zustand erreicht, so handelt es sich um eine sog. integrierte Datenverarbeitung.

Sie soll hier entsprechend den eben gemachten Ausführungen folgendermaßen bestimmt werden: *Einmal am beliebigen Ort ermittelte Informationen werden einmal erfaßt und gespeichert und zu möglichst vielen Auswertungen am beliebigen Ort im System verarbeitet* [6]).

Diese mehrfachen Auswertungen sind aber nur möglich, wenn die einmal erfaßten Informationen innerhalb des Verwaltungsapparates *austauschbar* sind. Dagegen kommt es nicht darauf an, *wo* die Information gespeichert ist: Selbst bei dezentraler Speicherung ist unter der Bedingung der Datenfernverarbeitung volle Integration möglich. Dies kann soweit gehen, daß die Behörden keine eigenen Datenbestände mehr haben, sondern diese bei einer eigenen Datenbank zentralisiert oder bei einer fremden Behörde gespeichert sind. Ebenso brauchen sie keine eigene Datenverarbeitung: Auch sie kann zentralisiert und unabhängig von den einzelnen Behörden als Dienstleistungsbetrieb organisiert sein. Den angeschlossenen Behörden verbleibt dann noch die Ein- und Ausgabe. Dies könnte man als den *zentralisierten Typ der Integration* bezeichnen.

Zukunftsträchtig ist der *dezentrale Typ:* Die Integration kann auch dahin gehen, daß die virtuell zentrale Datenbank örtlich dezentral bei den einzelnen Behörden lokalisiert ist, alle dezentralen Teilbanken jedoch über Fernverarbeitung und gemeinsame Datenorganisation tatsächlich eine einzige Datenbank bilden. Dann kann jede Behörde mit jeder Behörde über Datenfernverarbeitung in Informationsaustausch treten, wobei der Austausch alle bei allen Behörden vorhandenen Daten erfaßt — sofern keine rechtlichen Schranken bestehen. Das aber ist das rechtliche Problem des Informationsaustausches unter den Bedingungen der integrierten Datenverarbeitung.

Beispielsweise werden bisher Grundstücksdaten (Eigentümer, Katasternummern) sowohl beim Grundbuchamt wie auch bei der Steuerbehörde wie auch bei den Kommunen (zum Zwecke der Erstellung von Bebauungsplänen) gespeichert. Bei integrierter Datenverarbeitung wird es nur noch eine Grundstücksdatenbank geben, die vielleicht Teil einer zentralen Datenbank sein wird. Hier werden alle Grundstücksdaten nur einmal erfaßt und gespeichert, und jede Behörde, die derartige Informationen zur Erfüllung ihrer Aufgaben benötigt, wird technisch in der Lage sein, diese Informationen aus der Grundstücksdatenbank abzurufen.

So kann zusammenfassend gesagt werden:

Die Verwaltung ist dabei, ihre Organisation fortlaufend im Hinblick auf die Einrichtung einer integrierten Datenverarbeitung zu verändern. Diesem Ziel dienen alle in der letzten Zeit erlassenen Organisationsgesetze über die EDV in den verschiedenen Bundesländern [7]). Die Folge dieser fortschreitenden Integration — gleich welchen (zentralisierten oder dezentralen) Typs — ist jedenfalls die rapide Zunahme von Austauschvorgängen und die Abnahme von Ermittlungen, Erfassungen und Mehrfachspeicherungen. Von dieser unterschiedlichen Gewichtung wird eine rechtliche Bewertung auszugehen haben.

2. Paßt das Amtshilferecht für den Informationsaustausch?

Die Normen des Amts- bzw. Rechtshilferechts können nur dann Prüfungsmaßstab für die Rechtmäßigkeit des Informationsaustausches sein, wenn sie angesichts der neuen Sachverhalte den Erfordernissen von Artikel 2 Abs. 1 Rechnung tragen können. Angesichts des Aufkommens der Meinung, daß Informationsaustausch keine Amtshilfe sei [8]), kann nicht schlankweg davon ausgegangen werden, daß es für den vorliegenden Sachverhalt einschlägig ist.

Unter Berücksichtigung der oben geschilderten Entwicklung muß deshalb festgestellt werden:

Das Recht der Amts- bzw. Rechtshilfe kann unter drei Voraussetzungen den Informationsaustausch befriedigend regeln (und damit Sitz dieser Datenschutzregelung sein), wenn

- auch bei perfekter Verwaltungsintegration noch *Behörden* im Rechtssinne [9]) weiterbestehen, weil sonst kein *Austausch* (zwischen Behörden) vorliegt,
- auch bei perfekter Verwaltungsintegration das Amtshilfe*verfahren* noch anwendbar bleibt,
- im Rahmen des Amtshilferechts den Erfordernissen des Artikels 2 Abs. 1 Rechnung getragen werden kann.

2.1. Weitergeltung des Behördenbegriffs

Behörde wurde oben definiert als jede organisatorisch *selbständige Stelle,* die materiell öffentlichrechtliche Verwaltungstätigkeit erfüllt. Es ist aber denkbar, daß sich durch die Einführung der integrierten Datenverarbeitung in die Verwaltung Ab-

[4]) Meincke, 29
[5]) Meincke a. a. O.; Mundhenke, 62
[6]) Mundhenke a. a. O.; vgl. auch Steinmüller (1), 70
[7]) vgl. Begründung zu Artikel 2 Bay EDVG; § 4 Hess EDVG; § 2 Gesetz über die Datenzentrale Schleswig-Holstein
[8]) Kamlah (3), 22
[9]) Wolff (2), 82

hängigkeitsverhältnisse der Behörden voneinander ergeben, die sowohl ihre organisatorische Selbständigkeit als auch ihre materiell-rechtlichen Befugnisse entscheidend beeinflussen, ja beenden können. Der Begriff der Behörde würde dann unbrauchbar sein, da er in der Wirklichkeit keine Entsprechung findet. Als weitere Folge würde sich ergeben, daß das Amtshilferecht, das den Austausch von Informationen unter Behörden regelt, mangels Existenz solcher Behörden unanwendbar geworden wäre.

Das Amtshilferecht kann nur dann Prüfungsmaßstab sein, wenn sein Grundsachverhalt — Informationsaustausch zwischen selbständigen Behörden — trotz Integration bestehenbleibt.

Die Beantwortung der damit gestellten Frage hängt davon ab, wie sich die integrierte Datenverarbeitung auf die Selbständigkeit der beteiligten Behörden auswirkt.

Integrierte Datenverarbeitung setzt eine integrierte Verwaltung voraus. Dabei sind verschiedene Arten der Integration möglich: die funktionelle und die institutionelle Integration [10]) können im extremen Fall dazu führen, daß eine bestimmte Behörde ihre organisatorische Selbständigkeit oder ihre wesentlichen Aufgaben verliert. Dann ist sie nicht mehr als Behörde anzusprechen, so daß insoweit die Voraussetzung des Amtshilferechts fehlt, und damit auch der Informationsaustausch zwischen mindestens zwei *Behörden* entfällt.

Im Normalfall dagegen bleibt die institutionelle und funktionelle Selbständigkeit der Behörden bestehen.

Ergebnis: Integrierte Datenverarbeitung läßt normalerweise die Behörden weiter bestehen; das Amtshilferecht bleibt anwendbar, falls die weiteren Voraussetzungen ebenfalls bestehenbleiben.

2.2. Anwendbarkeit des bisherigen Amtshilfeverfahrens?

Das Amtshilfeverfahren — soweit es in § 5 Abs. 1, 2, 3 EVwVfG niedergelegt ist — verlangt eine doppelte Prüfung: einmal muß die ersuchende Behörde prüfen, ob ihr Ersuchen rechtmäßig ist, zum anderen muß die ersuchte Behörde prüfen, ob sie dem Ersuchen stattgeben darf.

Beispielsweise kann die ersuchte Behörde nach § 5 Abs. 2 EVwVfG die Amtshilfe verweigern, wenn sie aus rechtlichen Gründen dazu nicht in der Lage ist (Ziffer 1). Dies setzt aber voraus, daß die ersuchte Behörde überhaupt Kenntnis vom Ersuchen erlangt.

In einem integrierten Verbundsystem geht der Austausch jedoch so vor sich, daß die Behörde, die bereits woanders ermittelte Informationen benötigt, über Datenfernverarbeitung die technische Möglichkeit hat, auf diese Informationen überall da zuzugreifen, wo sie sich innerhalb des Verbundsystems befinden. Sicherlich wird es dabei auch on-line-Zugriff geben, d. h. die Behörde kann ohne Zwischenstufen direkt in den Speicher bei einer anderen Behörde zugreifen. Die „ersuchte" Behörde merkt davon nichts; bei on-line-Zugriff erlangt höchstens das Maschinenpersonal Kenntnis von dem Vorgang. Das bedeutet, daß die Behörde mangels Kenntnis keine Zulässigkeitsprüfung darüber anstellen kann, ob sie die angeforderten Informationen herausgeben darf oder nicht.

Zwischenergebnis: Die Behörde ist mangels Kenntnis des Austauschvorgangs nicht in der Lage, die Rechtmäßigkeit des Ersuchens zu prüfen.

Auch der *Zeitfaktor* spielt eine Rolle: Die Einführung von EDVA hat nur dann Sinn, wenn die zeitliche Schnelligkeit der Anlage auch voll ausgenützt werden kann. Es wäre geradezu sinnwidrig, wenn einerseits teure elektronische Anlagen installiert würden, die gegenüber manueller Arbeit unvergleichlich schneller arbeiten, andererseits aber vor jedem Zugriff einer anderen Behörde eine langwierige Prüfung durch die ersuchte Behörde stattfinden müßte, die die Zulässigkeit des Ersuchens feststellt. Auf diese Weise würde eine integrierte Informationsverarbeitung ihres Hauptvorteils beraubt; ihre Einführung wäre wirtschaftlich nicht zu verantworten.

Zwischenergebnis: Selbst wenn die ersuchte Behörde Kenntnis vom Zugriff einer anderen Behörde erhält, hat sie keine Zeit, eine Zulässigkeitsprüfung anzustellen, geschweige denn einen unzulässigen Zugriff abzuwehren.

Ein förmliches Ersuchen wird es demnach nicht mehr geben; an seine Stelle tritt der Zugriff.

So ergibt sich also: Die bestehenden Amtshilfenormen sind auf Informationsaustausch in einer integrierten Verwaltung unabwendbar.

2.3. Amtshilferecht und Artikel 2 Abs. 1 GG

Ein erster Blick in § 5 EVwVfG belehrt uns schnell, daß als Zulässigkeitsvoraussetzungen für die Amtshilfe lediglich organisatorische und verwaltungstechnische Gesichtspunkte aufgezählt sind; dagegen fehlt die Berücksichtigung privater Interessen. Die Amtshilfe ist nicht darauf abgestellt, das Selbstbestimmungsrecht zu schützen. Auch wenn in der Begründung [11]) steht, daß die Ablehnung des Ersuchens aus rechtlichen Gründen zulässg sei und dabei das Steuergeheimnis erwähnt wird, so ist man sich doch nicht sicher, ob damit auf schutzwürdige Interessen des Bürgers angespielt wird. Denn immerhin liegt es bereits im staatlichen Interesse, die geoffenbarten Finanzverhältnisse des einzelnen geheimzuhalten, da die Finanzbehörden sonst noch mit weit unzutreffenderen Angaben bedient würden, als dies sowieso schon der Fall ist [12]). Insbesondere enthält § 5 keine Vorschrift, die bestimmt, daß Amtsgeheimnisse einem Amtshilfeersuchen entgegenstehen könnten.

Der Entwurf bewegt sich in dieser Hinsicht im Rahmen der h. L., die davon ausgeht, daß Privatinteressen — und hier eben das Interesse des einzelnen an seinen Individualinformationen —im Amtshilfe-

[10]) Steinmüller (1), 88 f.
[11]) Begründung zu § 5 II EVwVfG, 33
[12]) Düwel, 95; vgl. auch Kamlah, in: KEDV 14, 21

verkehr nicht berücksichtigt zu werden brauchen [13]). Sie stützen sich dabei auf den Wortlaut von § 61 Abs. 1 Satz 2 BBG und § 39 Abs. 1 Satz 2 BRRG, der den Beamten bei Mitteilungen im innerdienstlichen Verkehr von seiner Schweigepflicht entbindet. Die Genehmigung, die von Düwel [14]) und Forsthoff [15]) vertreten wird, geht demgegenüber davon aus, daß trotz des Grundsatzes der Einheit der Verwaltung die Staatsziele, die von der Verwaltung verfolgt würden, durchaus verschieden seien und kollidieren könnten (Bsp.: Interessenkollision zwischen Staatsanwaltschaft, die zwecks Strafverfolgung die Vermögensverhältnisse einer Person wissen möchte, und der Finanzbehörde, die aus eigenen Interessen diese Informationen geheimhalten möchte [16]). Um also den unterschiedlichen Staatszielen zum Sieg zu verhelfen, müßten Amtsgeheimnisse im Amtshilfeverkehr Wirkung entfalten; auch die Normen des Beamtenrechts wären dementsprechend einzuschränken.

Die ganze Diskussion zeigt das Unbehagen, das das geltende Amtshilferecht hervorruft: Mit Hilfe des Amtsgeheimnisses glaubt man, den Privatinteressen des einzelnen besser Rechnung zu tragen. Düwel [17]) beispielsweise will dem Grundrecht des Artikels 2 Abs. 1 GG über das Amtsgeheimnis im Amtshilfeverkehr Geltung verschaffen, und das BVerfG [18]) folgert sogar im Scheidungsaktenurteil aus Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 und Artikel 19 Abs. 2 GG eine Geheimhaltungspflicht.

Ungelöst bleibt aber trotz des richtigen Ansatzes der Mindermeinung die entscheidende Frage: Wann liegt ein Amtsgeheimnis vor? Nur wenn es ausdrücklich normiert ist? Das BVerfG hat dies wohl impliziert verneint, wenn es eine Geheimhaltungspflicht aus den Grundrechten allgemein herleitet. Es fragt sich eben nur, wann Artikel 2 Abs. 1 GG seine Geheimhaltungswirkung entfaltet und wann nicht. Damit sind wir wieder beim alten Problem der Abgrenzung der sog. Privatsphäre. Privatsphäre im Sinne eines definierbaren besonders schutzwürdigen „Intimbereichs" wurde von den Verfassern abgelehnt; deshalb ist auch die Diskussion um die Wirksamkeit des Amtsgeheimnisses, das sich nach einhelliger Meinung auf eine Privatsphäre bezieht [19]), für uns nur insoweit brauchbar, als sie die Tendenz aufweist, Artikel 2 Abs. 1 GG auch im Amtshilfeverkehr zur Geltung zu bringen.

Nachdem dies aber von den vorliegenden Normierungen in keiner Weise geleistet wird [20]), liegt der Schluß nahe, daß die Berücksichtigung des grundrechtlichen Individualschutzes (Artikel 2 Abs. 1 GG) im Amtshilfeverkehr einen *neuen Sachverhalt* darstellt, der — mangels Berücksichtigung — offenbar außerhalb der Amtshilfe anzusiedeln ist und gesonderter Regelung bedarf.

2.4. Ergebnis

Als Ergebnis kann festgestellt werden:

Eine Anwendbarkeit des Amtshilferechts (und damit auch der Rechtshilfenormen in §§ 156 bis 169 GVG) scheitert zwar nicht schon ohne weiteres am Wegfall des Behördenbegriffs, wohl aber an seiner Unfähigkeit, der Situation einer integrierten Verwaltung Rechnung zu tragen, und an der fehlenden Berücksichtigung des Artikels 2 Abs. 1 GG.

Daraus ergibt sich, daß der Austausch von Individualinformationen unter Behörden und zwischen Behörden und Gerichten vom Amts- bzw. Rechtshilferecht nicht erfaßt ist.

Dieses Ergebnis wird auch von der Literatur geteilt. So sagt Kamlah, daß die bisherige Auffassung besagte, daß ein behördeninterner Datenaustausch eine völlig rechtsfreie Sphäre sei. Dies sei als Amtshilfe bezeichnet worden. Die Entwürfe für die Verwaltungsverfahrensgesetze gingen bereits davon ab, ohne überhaupt an die Privatsphäre zu denken. Die vordringende Auffassung geht dahin, ein Datenaustausch sei keine Amtshilfe [21]).

Auch Podlech stimmt mit diesem Ergebnis anscheinend überein, wenn er für den Zugriff von Behörden auf Individualinformationen eine gesetzliche Ermächtigung fordert, ohne dabei das Amtshilferecht auch nur zu erwähnen [22]). Selbst das Scheidungsaktenurteil des BVerfG erwähnt die Amtshilfe nur ein einziges Mal in einem Nebensatz. Es legt das Schwergewicht auf die Feststellung eines Eingriffs und stellt für dessen Zulässigkeit keine Prinzipien des Amtshilferechts, sondern des Verfassungsrechts auf. Dies läßt darauf schließen, daß es Eingriff und Amtshilfe als verschiedene Dinge bewertet hat [23]).

Abschließend muß also festgestellt werden:

Das Recht der Amts- bzw. Rechtshilfe wird dem Informationsaustausch nicht gerecht. Insbesondere schützt es das aus Artikel 2 Abs. 1 GG folgende Selbstbestimmungsrecht des einzelnen nicht. Im folgenden müssen deshalb Möglichkeiten entwickelt werden, die den verfassungsrechtlichen Anforderungen des Artikels 2 Abs. 1 besser gerecht werden.

3. Zweckentfremdungsregel

Unter Berücksichtigung der oben gefundenen Ergebnisse kann behauptet werden: Wenn der einzelne selbst bestimmen kann, welche Individualinformationen er unter welchen Umständen an wen abgibt, so erstreckt sich das auch auf den Bereich zwischen Behörden und Gerichten.

---

[13]) BAG in NJW 60, 2118; BGHZ 34, 184; Wolff (2), 119; Peters (3), 60
[14]) Düwel, 95 ff.
[15]) Forsthoff (1), 98
[16]) Düwel a. a. O.
[17]) Düwel, 238
[18]) BVerfG in NJW 70, 555 f.
[19]) statt aller Düwel, 237 f.
[20]) auch im LVwG von Schleswig-Holstein findet sich nichts dergleichen
[21]) Kamlah (3), 18
[22]) Podlech, 475
[23]) BVerfG in NJW 70, 555

Hat er also eine Individualinformation für einen bestimmten Zweck an eine bestimmte Behörde preisgegeben, so ist es dieser nicht erlaubt, diese Information ohne Berücksichtigung des Selbstbestimmungsrechts weiterzugeben; umgekehrt darf eine andere Behörde nicht ohne weiteres auf diese Information zugreifen.

Dieses Postulat deckt sich mit der *„Zweckentfremdungsregel"*, nämlich dem Verbot, Individualinformationen, die für einen bestimmten Zweck ermittelt sind, einem anderen Zweck zuzuführen [24]).

Nach dem Scheidungsaktenurteil ist ein Handeln einer Behörde gegen diese Regel ein Grundrechtsverstoß [25]): Angesichts der Übersendung von gerichtlichen Scheidungsakten an den Untersuchungsführer eines Disziplinarverfahrens führt das Gericht aus, daß die in den Scheidungsakten enthaltenen Informationen von den Eheleuten nur im Hinblick auf den begrenzten Adressatenkreis — das Gericht und die Verfahrensbeteiligten — offengelegt wurden. Darum würden Ehescheidungsakten inhaltlich einer Geheimhaltung nach Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG unterliegen. Die Übersendung der Akten ohne vorherige Zustimmung der Eheleute an den Untersuchungsführer des Disziplinarverfahrens sprenge den begrenzten Adressatenkreis und verletzte die Geheimhaltungspflicht. Damit liege ein Eingriff in das Persönlichkeitsrecht der Ehegatten vor, das sich aus Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG ergebe.

Damit hat das Gericht klar gesagt, daß die Zweckentfremdung von Individualinformationen ein Grundrechtsverstoß sei, damit die — fundamentale — „Zweckentfremdungsregel" anerkannt und verfassungsrechtlich grundgelegt.

Entsprechend dem für die Untersuchung der Topoi entwickelten Prüfungsschema für Artikel 2 Abs. 1 GG wird nun im folgenden zuerst am Wesensgehalt des Artikels 2 Abs. 1 GG und dann an den Bestandteilen der „verfassungsmäßigen Ordnung" geprüft, welche Möglichkeiten und Beschränkungen sich für Verwaltung hinsichtlich des Austausches von Individualinformationen ergeben.

3.1. Wesensgehalt von Artikel 2 Abs. 1 GG

Anläßlich des ersten Topos — Ermittlung von Individualinformationen durch öffentliche Stellen — wurde entwickelt, daß der Bedarf einer Behörde an Informationen sich am Verwaltungsergebnis zu orientieren habe. Die Ermittlung von Individualinformationen für das Verwaltungsergebnis war nur zulässig, wenn die betreffende Information als Minimal- oder Unterstützungsinformation zu bewerten war, wobei die Ermittlung von Unterstützungsinformationen im Rahmen der Verhältnismäßigkeit liegen mußte.

Der *Austausch* von Individualinformationen und ihre Ermittlung sind insoweit — rechtlich gesehen — *ähnliche* Sachverhalte. In beiden Fällen handelt es sich darum, daß Behörden Zugang zu Informationen bekommen, die sie zur Erfüllung ihrer Aufgaben und damit zur Erstellung konkreter Verwaltungsergebnisse benötigen. In beiden Fällen geht es rechtlich darum, die Auswirkungen von Artikel 2 Abs. 1 GG dabei zum Tragen kommen zu lassen, wobei in beiden Fällen die Reichweite von Artikel 2 Abs. 1 angesichts seiner Ausprägung als informationelles Selbstbestimmungsrecht gleich groß ist. Diese Gemeinsamkeiten rechtfertigen es, die für die Ermittlung gewonnenen Ergebnisse auch für den Austausch fruchtbar zu machen.

Demnach ist eine Behörde nur dann *zum Informationsaustausch berechtigt, wenn die begehrte Individualinformation im Hinblick auf das von der ersuchenden Behörde zu erstellende Verwaltungsergebnis als Minimal- oder Unterstützungsinformation zu bezeichnen ist.* Dabei sind Minimalinformationen schlechthin erforderlich und ohne Schranken austauschbar, solange — was praktisch immer der Fall sein wird — das angestrebte Verwaltungsergebnis nur eine Teilaussage über die Persönlichkeit enthält (Wesensgehaltsschranke). Unterstützungsinformationen sind nur dann austauschbar, wenn der Wahrscheinlichkeitsgrad der Richtigkeit der Minimalinformationen so gering ist, daß die Minimalinformationen durch weitere Informationen verifiziert werden müssen. Der Austausch von Unterstützungsinformationen ist dann verhältnismäßig [26]).

Dieses Ergebnis deckt sich im wesentlichen mit dem des Scheidungsakten-Urteils des BVerfG [27]): Das Gericht geht ebenfalls von Auswirkungen eines Persönlichkeitsrechtes aus Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 und Artikel 19 Abs. 2 GG auf den Bereich der Rechts- und Amtshilfe aus. Die Auswirkung gewinnt Gestalt im Verhältnismäßigkeitsprinzip, dessen Mißachtung beim Austausch von Informationen aus dem Persönlichkeitsbereich als Verstoß gegen die angeführten Grundrechte angesehen wird [28]). Das Verhältnismäßigkeitsprinzip konkretisiert sich u. a. im Grundsatz der Erforderlichkeit. Mangels substantiierter Darlegung der Erheblichkeit war es in dem vom BVerfG entschiedenen Fall der ersuchten Behörde (hier: einem Gericht) nicht möglich festzustellen, „inwieweit der Inhalt der Ehescheidungsakten Informationen ergeben könnte, die für die Durchführung des Disziplinarverfahrens hätten von Bedeutung sein können" [29]). Deshalb wurde der Verfassungsbeschwerde stattgegeben.

In Weiterführung dieser Gedanken schlüsseln wir den Begriff der Erforderlichkeit in diesem Zusammenhang weiter auf, indem wir in Minimal- oder Unterstützungsinformationen unterscheiden, damit der Gesetzgeber dem Grundgedanken dieses Urteils

---

[24]) Kamlah (3), 22; Kamlah (2), 363 in Generalisierung der fallbezogenen Grundsätze des BVerfG

[25]) BVerfGE in NJW 70, 555

[26]) im Ergebnis auch Forsthoff (4), 51 f. In diesem Zusammenhang soll noch einmal betont werden, daß Feststellung der Verhältnismäßigkeit nichts zu tun hat mit einer Interessenabwägung zur Feststellung eines Verletzungstatbestandes (siehe Evers S. 49 ff.). Insofern sind auch manche Ausführungen Düwels leicht mißverständlich (z. B. S. 236 Nr. 19; S. 233 Nr. 9).

[27]) BVerfG in NJW 70, 555 f.

[28]) vgl. auch BVerfGE 24, 404

[29]) BVerfG a. a. O.

im Datenschutzrecht möglichst weitgehend Geltung verschaffen kann.

Zu der inhaltlichen Beschränkung auf Minimal- und Unterstützungsinformationen kommt die formelle auf die Zuständigkeit:

3.2. Grundprinzipien der staatlichen Ordnung

3.2.1. Gewaltenteilung

Auch hier wird die Gewaltenteilung relevant in ihrer Ausformung als Zuständigkeitsregelung im Verwaltungsbereich. Dabei entfaltet die Feststellung Ellweins [30]) wieder ihre Gültigkeit: Zuständigkeit begrenzt Menge und Art der zur Willensbildung heranzuziehenden Informationen; das bezieht sich auf alle Arten der Informationsgewinnung, also auch auf den Austausch von Individualinformationen. Die Zuständigkeit ist eine Grenze gegen uferlosen Austausch, sie betrifft hier die Zuständigkeit der zugreifenden Behörde zu der Maßnahme, die den Bürger betreffen soll und zu deren Entscheidungsprozeß sie die Information einholt.

Damit ergibt sich als formelle Schranke des Informationsaustausches die Beschränkung auf Anfragen bzw. Zugriffe im Rahmen der Zuständigkeit der abfragenden Behörde.

3.2.2. Gesetzmäßigkeit der Verwaltung

Da der Austausch von Individualinformationen einen Eingriff in das Grundrecht aus Artikel 2 Abs. 1 GG darstellen kann, bedürfen diese Eingriffe möglicherweise einer gesetzlichen Grundlage.

3.2.3. Rechtsnatur des Austausches von Individualinformationen

Da Artikel 2 Abs. 1 GG das Recht des einzelnen enthält, darüber zu bestimmen, wer welche Information unter welchen Umständen erhält, und da deshalb der Austausch dieser Informationen ohne eine Mitwirkungsmöglichkeit des Betroffenen u. U. einen Eingriff in Artikel 2 Abs. 1 GG darstellt [31]), kommt es in Betracht, den Austausch von Individualinformationen auf die Rechtsnatur eines VA hin durchzuprüfen.

Ist also der Informationsaustausch Verwaltungsakt? Nach dem oben zur Ermittlung, Erfassung und Speicherung Gesagten, kann es nicht verwundern, wenn die durchaus h. M. [32]) auch im Falle des Datenaustausches für den Fall der Weitergabe von Individualinformationen eine Regelung und damit einen Verwaltungsakt ablehnt. So sagt Wolff [33]) etwa „das Ersuchen (sei) keine Anordnung, also weder eine Weisung noch gar ein Verwaltungsakt, sondern eine nichtregelnde *interne* Willenserklärung". Entsprechend kann nur die im Wege der Amtshilfe durchgeführte *Maßnahme,* nicht der Informationsaustausch angefochten werden [34]).

Für diese h. M. ist es dann konsequent, daß Geheimhaltungspflichten einer ersuchenden Behörde gegenüber nicht anerkannt werden [35]). Insofern handle es sich — so wird argumentiert — um „Mitteilungen im dienstlichen Verkehr", für die die Verschwiegenheitspflicht der Beamten gemäß § 39 Abs. 1 BRRG, § 61 BBG nicht gelte [36]). Dabei wird von den meisten Autoren [37]) kein Unterschied gemacht, ob das Amtsgeheimnis private oder öffentliche Interessen betrifft. Soweit der globale Hinweis auf § 61 BBG, § 37 BRRG abgelehnt wird, wird etwa gesagt, die „ersuchte Behörde (habe) pflichtgemäß abzuwägen, ob die Preisgabe privaten, vertraulichen Wissens nach den Umständen geboten ist" [38]). Diese h. M. hat zur Konsequenz, daß sich der Datenaustausch im rechtsfreien Raum bewegt oder er im pflichtgemäßen Ermessen (ein Ausdruck, der nicht genauer definiert wird) der ersuchten Behörde liegt. Da zudem Rechtsmittel nur gegen die Maßnahmen der *ersuchenden* Behörde zulässig sein sollen [39]), hat der Betroffene derzeit keine Möglichkeit, den bloßen Informationsaustausch, der noch nicht zu einer Maßnahme gegen den Betroffenen führt, mit Rechtsmitteln anzugreifen. Dieser Auffassung scheint sich auch der Gesetzgeber angeschlossen zu haben. So läßt er die Ablehnung eines Amtshilfeersuchens nur zu, „wenn durch die Hilfeleistung dem Wohle des Bundes oder eines Landes Nachteile bereitet wurden (§ 33 Abs. 2 Nr. 2 LVerG von Schleswig-Holstein; ebenso § 5 Abs. 2 Nr. 2 BVwVfG).

Die Auffassung der h. M. ist zu Recht von Kamlah [40]) bekämpft worden, der — insoweit zu Recht — eine „Verrechtlichung" des Informationsaustausches fordert und anscheinend den Austausch von Individualinformationen für einen Verwaltungsakt hält [41]). Sie wird auch nach der Entscheidung des BVerfG im „Scheidungsaktenurteil" [42]) neu zu überdenken sein.

Dabei ist freilich zu berücksichtigen, daß der Begriff des Verwaltungsaktes in der Ausprägung, die er von Rechtsprechung und Lehre erfahren hat, auf die hier zu behandelnde Problematik nicht so recht paßt. Zwar wäre es dogmatisch möglich, ihn auf Fälle auszudehnen, die nach derzeitiger Auffassung dem Bereich des verwaltungsinternen Handelns angehören. Doch ist es fraglich, ob damit dem betroffenen Staatsbürger in einer Weise geholfen werden kann, die seinem Rechtsschutzbedürfnis am besten entspricht. Auf dieses Problem wird in Zukunft Rechtsprechung und Lehre verstärkt ihr Augenmerk zu richten haben.

Für den Zweck des Gutachtens bedarf diese Frage keiner endgültigen Klärung. Unabhängig davon, ob es sich bei dem Austausch von Individualinformationen um einen Verwaltungsakt handelt oder nicht,

---

[30]) Ellwein (2), 104 f.
[31]) so die Aussage der Zweckentfremdungsregel
[32]) Wolff (2), 119 ff.
[33]) (2), 119
[34]) vgl. dazu v.d. Groeben - Unach § 35 N. 21
[35]) Düwel, 93 FN 42
[36]) vgl. hierzu auch die beiden Beispiele aus der Rechtsprechung bei Düwel, 92 f.
[37]) vgl. etwa Wolff (1), 119
[38]) so Forsthoff (1), 99
[39]) Wolff (1), 120
[40]) Kamlah (3), 18, in diese Richtung auch Düwel, 104 ff.
[41]) Er spricht diese Konsequenz nicht explizit aus. Sie ergibt sich notwendig aus seiner in (DÖV), 363 erhobenen Forderung nach einer Rechtsgrundlage für den Datenaustausch.
[42]) in: NJW 70, 555

hat der Gesetzgeber eines Datenschutzgesetzes den Interessen des Betroffenen durch besondere Regelungen Rechnung zu tragen.

4. Zusammenfassung: Entwicklung der rechtlichen Regelungen

Hinsichtlich der *Rechtsgrundlage* kann folgendes festgestellt werden: Ist der Austausch — wie hier zugrunde gelegt — kein VA, so bedarf er gleichwohl einer *formellen Rechtsgrundlage* [43]). Diese Grundlage kann in einer Norm des Datenschutzgesetzes oder des VwVfG Wirklichkeit werden. An die Einhaltung des Bestimmtheitsgrundsatzes sind — da es sich nicht um einen VA handelt — keine strengen Anforderungen zu stellen. Es genüge die Normierung der beiden Schranken des Informationsaustausches als subjektiv-öffentliches Recht bei Anfechtung des Verwaltungsergebnisses [44]). Wie auch bei der Ermittlung besteht der rechtliche Kontrollmechanismus aus zwei Teilen: Zum einen wird der Verwaltung gesetzlich vorgeschrieben, was sie beim Informationsaustausch zu beachten hat; zum anderen bekommt der Bürger Rechte, um die Einhaltung dieser Vorschriften gerichtlich überprüfen lassen zu können.

4.1. Vorschriften für die Verwaltung

Zunächst sind die für die Ermittlung gefundenen Ergebnisse auch hier von Bedeutung:

— Alle Verwaltungsbehörden sind berechtigt, im Rahmen ihrer *Zuständigkeit* auf Individualinformationen zuzugreifen, die sie nicht selbst ermittelt haben.

— Die Individualinformation, auf die zugegriffen wird, muß im Hinblick auf das Verwaltungsergebnis entweder als Minimal- oder Unterstützungsinformation anzusehen sein. Der Zugriff auf Unterstützungsinformationen ist nur im Rahmen der Verhältnismäßigkeit zulässig. Die Verhältnismäßigkeit bemißt sich danach, wie hoch der Wahrscheinlichkeitsgrad der Richtigkeit einer Minimalinformation zu veranschlagen ist.

Diese Vorschriften könnten jedoch umgangen werden, wenn die zugreifende Behörde die Informationen, die sie im Austausch erlangt hat, bei sich speichern dürfte. Vielmehr muß sichergestellt werden, daß die zugreifende Behörde bei jedem Fall, in dem sie auf den Austausch angewiesen ist, von neuem einer Zulässigkeitsprüfung hinsichtlich ihres Zugriffs unterworfen wird. Dies wird bei integrierten Datenverarbeitungssystemen durch Einschaltung eines — offenzulegenden — Berechtigungsprogramms verwirklicht werden.

Deshalb folgender zusätzlicher Regelungsvorschlag:

— *Eine Behörde darf Individualinformationen nicht bei sich speichern, die sie auf dem Wege des Austausches erlangt hat.*

Endlich ist noch zu bedenken, daß ein Löschungsanspruch des Bürgers, der die Verwendung rechtswidrig ermittelter Informationen verhindern würde, hier abwegig ist, da die Speicherung der ersuchenden Behörde verboten ist. Deshalb bleibt nur der Weg, der Behörde, die durch rechtswidrigen Austausch eine Individualinformation erlangt hat, zu verbieten, diese Information einem Verwaltungsergebnis zugrunde zu legen. Deshalb folgender Regelungsvorschlag:

— *Eine Behörde darf Individualinformationen, die sie durch einen rechtswidrigen Informationsaustausch erlangt hat, nicht zur Grundlage eines Verwaltungsergebnisses machen.*

Darüber hinaus erscheint es noch zweckmäßig, kurz darauf hinzuweisen, daß diese Vorschriften mit den Regelungen über die Amtshilfe nichts zu tun haben. Sie sind enger als diese und regeln Fälle, die — wie oben nachgewiesen — vom Amtshilferecht bisher nicht erfaßt werden. Das schließt nicht aus, daß die Behörden — vornehmlich, solange noch weitgehend manuell verarbeitet wird — *zusätzlich* die Vorschriften des EVwVfG bzw. der GVG zu beachten haben. Der Hinweis müßte deshalb lauten:

— *Die Vorschriften über das Verfahren bei Rechts- und Amtshilfe bleiben unberührt.*

4.2. Rechte des Bürgers

Da der Austausch kein Verwaltungsakt ist, sind diese Rechte Ausformungen des allgemeinen Leistungsanspruchs.

Wichtig ist ein *Auskunftsrecht,* das den Betroffenen über den Inhalt der ausgetauschten Informationen unterrichtet; weiterhin müssen Datum des Austausches und Anschrift der zugreifenden Behörde mitgeteilt werden.

Zusätzlich muß ihm eine *Unterlassungsklage* gegen künftige rechtswidrige Austauschvorgänge zustehen. Sie kann mit einer einstweiligen Verfügung nach § 123 VwGO rasch durchgesetzt werden. Der Anspruch auf Unterlassung ergibt sich aus dem subjektiv öffentlich-rechtlichen Anspruch auf Einhaltung der Vorschriften für die Verwaltung, die damit auch hinsichtlich des Austausches einer gerichtlichen Kontrolle unterliegt, und ist entsprechend dem oben zu Topos I. 4. gemachten Vorschlag zu normieren.

Bei Verstoß gegen diese Rechte und dadurch entstandenem Schaden kann ein *Schadenersatzanspruch* nach dem — auf schuldloses Handeln auszuweitenden — Amtshaftungsrecht geltend gemacht werden.

5. Rechtspolitische Beurteilung des Ergebnisses

Die Verfasser sind sich bewußt, daß das Ergebnis bei Verwaltungsfachleuten auf Bedenken stoßen wird. Von diesen wird insbesondere vorgebracht, daß derartige Ergebnisse einerseits unpraktikabel seien, da sie die Verwaltung zu stark binden würden und daß

[43]) Podlech, 475; Düwel, 105; Kamlah (2), 363; Kamlah (3), 18

[44]) vgl. oben I, 4.

andererseits der Bürger keinen Grund habe, der Verwaltung so massiv zu mißtrauen; sie sei guten Willens, den Schutz des Bürgers zu respektieren, und es sei letztlich die politische Aufgabe aller, dafür zu sorgen, daß der Verwaltungsapparat nicht in undemokratische Hände gelange.

Diese Einwände sind nur zum Teil zutreffend; im folgenden sollen einige Punkte herausgestellt werden, die das Ergebnis auch von der *rechtspolitischen Seite* her stützen sollen.

— Es wurde bereits dargestellt, welche enorme Bedeutung dem Informationsaustausch in der modernen Verwaltung zukommt. Austausch ermöglicht es, beliebig viele Informationen über einen Bürger an einer Stelle anzuhäufen; Dossierbildung vollzieht sich über den Austausch. Das Schreckgespenst vom allwissenden „Leviathan Verwaltung" zeigt das Bild der perfekten Austauschverwaltung. Will man dieses Schreckgespenst glaubwürdig bannen, so sind dazu in ganz überwiegendem Maße Regelungen für den Informationsaustausch erforderlich. Vereinfacht wird man sagen können, daß die Effektivität des gesamten Datenschutzes in der öffentlichen Verwaltung von der Art der Regelung des Austausches abhängt. Geht man dabei von einer Schutzwürdigkeit des einzelnen hinsichtlich seiner Individualinformationen aus, so ist das ein Gesichtspunkt, der — wenigstens prinzipiell — Praktikabilitätsgesichtspunkten vorzuordnen ist [45]).

— Angesichts des verwaltungsinternen Ablaufs des Zugriffs anderer Behörden (möglicherweise erfährt die Behörde, die die Informationen hat, nichts vom Zugriff!) ist — wenigstens nach der bisherigen Übung — der Bürger darüber uninformiert, an wen seine Informationen gelangt sind. Eine wirksame Kontrolle des Informationsaustausches durch den Betroffenen ist aber nur dann möglich, wenn es nicht dem Zufall überlassen bleibt, ob er etwas davon erfährt [46]). Deshalb ist die Einführung eines Auskunftsrechtes unerläßlich, das der einzige Weg für den Betroffenen ist, die Rechtmäßigkeit des Austausches gerichtlich nachprüfen zu lassen (eben über einen Unterlassungsanspruch). Im wesentlichen wird dadurch die bisherige Rechtslage nicht verändert und der Verwaltung keine unzumutbaren Lasten aufgebürdet.

— Die vorgelegte Lösung ist auch *nicht unpraktikabel.* Beispielsweise *erspart sie der Verwaltung, vor dem Austausch die Zustimmung des Betroffenen einzuholen,* eine Forderung, die im Zusammenhang mit dem Amtsgeheimnis immer wieder erhoben wurde [47]). *Ebenso entfällt die (Unmengen vom Papier und Kosten verschlingende) Erstellung von printouts.* Da außerdem eine allgemeine formelle Rechtsgrundlage des Informationsverarbeitungsverfahrens inerhalb eines Verwaltungsverfahrens- oder eines Datenschutzgesetzes rechtsstaatlichen Prinzipien nicht widersprechen dürfte, ist eine zu starke Bindung der Verwaltung, die sie an die Grenze der Ineffizienz bringen würde, nicht zu befürchten.

— Die vorgelegte Lösung läßt der Verwaltung soviel Raum, daß von Beschränkungen, die aus einem übersteigerten Mißtrauen hergeleitet werden könnten, nicht die Rede sein kann. *Die Lösung ermöglicht es der Verwaltung, im wesentlichen wie bisher zu verfahren;* das einzig Neue ist die Auskunftspflicht; verwaltungsgerichtlicher Kontrolle war die Verwaltung auch bisher ausgesetzt.

[45]) Das ist nichts Neues: auch bisher war die Verwaltung gehalten, die Entscheidungen der Verfassung höher zu stellen als Arbeitseffizienzen. Das ist geradezu ein Prinzip des Rechtsstaats (vgl. Podlech, 475).
[46]) Simitis (2), 681
[47]) Düwel, 233 N. 9; Forsthoff (1), 99

VI. Topos Informationsweitergabe an Dritte

1. Allgemeines

1.1. Definition

Informationsweitergabe an Dritte liegt vor, wenn eine Behörde einem anderen als einer Behörde oder dem Betroffenen selbst Informationen zugänglich macht.

1.2. Abgrenzung

Die oben [1]) angegebene allgemeine Definition für Informationsweitergabe (Abgabe einer eigenen Information an außenstehende Dritte) ist für den Bereich der Verwaltung deshalb zu allgemein, weil sich eine rechtliche Beurteilung danach zu richten hat, wem von der Behörde Informationen zugänglich gemacht werden. Gibt sie *an einen Privaten* (z. B. eine Werbefirma oder eine staatliche Stelle mit rein fiskalischen Aufgaben) weiter, so verläßt sie damit den verwaltungsinternen Bereich, und die rechtliche Beurteilung muß sich nach den verfassungs- und privatrechtlichen Gesichtspunkten richten. Das ist der Regelungsbereich dieses 6. Topos [2]). Gibt sie dagegen an eine andere Behörde weiter, so handelt es sich um den schon behandelten Fall des Informationsaustausches (5. Topos). Angesichts dieser unterschiedlichen Sachverhalte empfiehlt es sich, beide Sachverhalte definitorisch auseinanderzuhalten.

[1]) siehe oben B. II. 2.
[2]) Geschieht die Weitergabe an Private innerhalb eines *integrierten* öffentlich-privaten Systems: dann Informations*verbund* (7. Topos).

1.3. Beispiel

Als *Beispiel* für eine Weitergabe an Dritte lassen sich aufführen:

Eine Behörde gibt Angaben aus den Personalakten an eine Werbefirma oder an ein sonstiges privates Unternehmen. Eine Behörde gibt Namen und Adressen aller 20jährigen an ein Industrieunternehmen. Ein Landesjustizprüfungsamt gibt Namen und Adressen aller Rechtsreferendare einer Versicherung an (die möglicherweise noch vom Staat getragen wird). Das Finanzamt gibt die Adressen aller Steuerschuldner an eine Auskunftei.

Im folgenden wird untersucht, welche Möglichkeiten oder Beschränkungen für die Verwaltung sich hinsichtlich einer Weitergabe an Dritte ergeben. Dies richtet sich — wie bei allen Topoi — nach den Auswirkungen von Artikel 2 Abs. 1 GG auf diesen Sachverhalt.

2. Schutzbereich

Das aus dem Persönlichkeitsrecht entspringende Selbstbestimmungsrecht des einzelnen umfaßt auch, wie angegeben, die Bestimmung darüber, wem eine Individualinformation zukommen soll. Damit ist eine solche Weitergabe an Dritte in jedem Falle eine Beschränkung des Artikels 2 Nr. 1 GG. Selbst eine Einwilligung des Verletzten beseitigt diese Feststellung nicht, da es sich dabei dogmatisch allenfalls um einen Rechtfertigungsgrund handeln würde, der aber den Beschränkungstatbestand bestehen läßt [3]).

3. Zulässigkeit einer Beschränkung

3.1. Weitergabe mit Einwilligung

Gibt eine Behörde eine Information an einen privaten Dritten mit Einwilligung des Betroffenen weiter, dann liegt in dieser Einwilligung die Zustimmung des Betroffenen zu einer Grundrechtsbeeinträchtigung. Beispielsweise ist es in manchen Behörden üblich, sich durch eine Unterschrift des Betroffenen seiner Zustimmung zu einer Weitergabe zu versichern. Diese Einwilligung in die Verletzung eines Grundrechts ist jedoch problematisch.

In der Literatur wird die Meinung vertreten [4]), daß der Staat aus Artikel 1 Abs. 1 Satz 2 die objektive Verpflichtung habe, die Menschenwürde des einzelnen ohne Rücksicht auf ein subjektives Einverständnis des Betroffenen zu schützen. Wann aber ist die Menschenwürde tangiert? Ist das der Fall, wenn der Betroffene in die Weitergabe von Namen und Adresse an eine Werbefirma einwilligt, oder erst, wenn er in die Weitergabe von Eintragungen aus seinen Personalakten, die seine charakterlichen Fähigkeiten enthalten, an künftige Arbeitgeber einwilligt?

[3]) Erman - Weitnauer, Anhang zu § 12, N. 4 a
[4]) Maunz - Dürig - Herzog, Artikel 1 N. 36
[5]) Stein, 201

„Griffiger" als die Menschenwürde ist auch hier wieder der Wesensgehalt des Artikels 2 Abs. 1, der ja Artikel 1 einschließt. Die Menschenwürde ist dann betroffen, wenn der Kernbereich des Artikels 2 Abs. 1 GG berührt ist. Das ist dann der Fall, wenn der Betroffene durch die Weitergabe sich einer Fremdbestimmung aussetzt. Dies trifft ganz sicher dann zu, wenn Informationen nach außen dringen, die den einzelnen für andere steuerbar machen, wo also der Betroffene keine Möglichkeit zur Gegenwehr mehr hat. So würde — um an die letzten Beispiele anzuknüpfen — der Betroffene sich gegen ein Angebot eines Handelsunternehmens, das etwa Prospekte über Autozubehör zusendet, wohl wehren können; er braucht das Angebot einfach nicht anzunehmen. Besitzt dagegen jemand Informationen über psychische Merkmale oder über dem Unbewußten angehörende Bereiche der Persönlichkeit — etwa aus Einstellungstests — so kann er den Betreffenden steuern, ohne ernstliche Gegenwehr befürchten zu müssen, wenn er sich nur darauf versteht, die Schwächen des Betroffenen auszunützen. Da der Betroffene die Steuerungsabsicht gar nicht merkt, ist er hilflos.

Zusammenfassend kann also gesagt werden: *Eine Einwilligung in die Weitergabe von Individualinformationen an Dritte ist dann unzulässig, wenn der Betroffene sich dadurch ohne Möglichkeiten einer Gegenwehr in die Hand des Empfängers begibt. Die Weitergabe solcher Informationen ist deshalb — trotz Einwilligung des Betroffenen — für die Verwaltung verboten.* Betrifft die Einwilligung dagegen Informationen, die nicht den Wesensgehalt von Artikel 2 Abs. 1 GG berühren (und das dürfte der Regelfall sein), so ist ein privatrechtlicher Vertrag zwischen dem Betroffenen und der Verwaltung zu konstruieren, der eine Weitergabe an Dritte vorsieht. Die Weitergabe unterfällt damit der Privatautonomie. Man könnte nun meinen, auch hier stelle sich das Problem der unzulässigen Einwilligung, da sie sich nach § 138 BGB als sittenwidrig erweisen könnte. Doch ist auch hier die oben vorgenommene grundrechtliche Wertung einschlägig. Denn nach der Lehre von der mittelbaren Drittwirkung der Grundrechte ist § 138 BGB eine der Einbruchstellen der grundgesetzlichen Wertvorstellungen in das Privatrecht. Ist die Einwilligung verfassungsrechtlich zulässig, so kann sie auch nicht nach § 138 BGB sittenwidrig sein.

3.2. Weitergabe ohne Einwilligung

Die Weitergabe ohne Einwilligung des Betroffenen ist nur im Rahmen von Artikel 2 Abs. 1 GG zulässig. Dazu ist zu prüfen, ob der Wesenskern von Artikel 2 Abs. 1 angetastet ist oder gegen die in Artikel 20 niedergelegten Grundprinzipien verstoßen wird.

3.2.1. Wesensgehalt von Artikel 2 Abs. 1 GG

Unter Anwendung der oben gefundenen Formel von der informationellen Autonomie des einzelnen [5]) ist der Wesensgehalt von Artikel 2 Abs. 1 GG dann durch eine Weitergabe verletzt, wenn damit eine Fremdbestimmung des einzelnen bewirkt wird. Das

ist dann der Fall, wenn der Betroffene die Weitergabe der Information nicht selbst veranlaßt hat. Es gilt die Entfremdungsregel auch hier [6]): Dem Betroffenen steht zu zu bestimmen, wer welche Individualinformationen an wen weitergeben darf.

Damit ist grundsätzlich jede Weitergabe an Dritte ohne Einwilligung verboten, von den „allgemein zugänglichen" Informationen abgesehen [7]).

3.2.2. Grundprinzipien der staatlichen Ordnung

Dieses Ergebnis wird erhärtet, wenn man das Rechtsstaatsprinzip heranzieht (Artikel 20 GG), nämlich den Grundsatz, daß der einzelne vor unnötigen Eingriffen der öffentlichen Gewalt bewahrt bleiben soll [8]). Die Weitergabe ist dann ein unnötiger Eingriff, wenn sie zur Erfüllung einer der Verwaltung übertragenen Aufgabe nicht erforderlich ist. Das ist dann der Fall, wenn sie dem Prinzip der Verhältnismäßigkeit widerspricht [9]). Damit ist grundsätzlich jede Weitergabe an Private, die nicht im Rahmen der Verwaltung tätig sind, unzulässig. Es sind keine Gründe ersichtlich, die der Verwaltung dies erlauben würden.

3.3. Schutz vor Beschränkung ohne Einwilligung

Um das Nach-außen-Dringen von Informationen aus dem Verwaltungsbereich zu verhindern, kennt das geltende Recht die Figur der Amtsverschwiegenheit. (Inwieweit die Amtsverschwiegenheit verwaltungs*intern* bedeutsam ist, ist nur für den Informations*austausch,* nicht aber für die *Weitergabe* relevant). Sie hat sich in vielen Normen niedergeschlagen [10]). Dabei wird meist ein bestimmter Personenkreis der Amtsverschwiegenheit unterstellt [11]) und die im Zusammenhang mit ihrer Tätigkeit erfaßten Informationen zum Amtsgeheimnis erklärt.

Das Auftreten der neuen, in der Verwaltung tätigen Gruppe von mit der Informationsverarbeitung betrauten Menschen und die Häufung unterschiedlicher Angaben, Ergebnisse, Unterlagen und Programme bei dieser Gruppe veranlaßten bereits manchen Gesetzgeber zur Statuierung eines besonderen „Datengeheimnisses" [12]).

Eine Definition dieses Datengeheimnisses ist in § 3 Abs. 1 Hess. DatenschutzG versucht worden: Die Vorschrift verbietet es den mit der Datenverarbeitung betrauten Personen, ihre Kenntnisse, die sie im Zusammenhang mit ihrer Arbeit erlangt haben, anderen zugänglich zu machen. Es bleibt unklar, wem gegenüber dieses Verbot gilt: gegenüber privaten Dritten oder gegenüber anderen Behörden oder gar gegenüber Mitgliedern derselben Behörde? Klar wird es erst, wenn man sich ins Gedächtnis ruft, daß das „Datengeheimnis" offensichtlich mit dem Amtsgeheimnis identisch ist. Amtsgeheimnis ist dabei ein Geheimnis, dessen Kenntnis sich im wesentlichen auf Amtsträger und Behörden beschränkt und in Ausübung amtlicher Funktionen erlangt worden ist [13]). Diese Definition sagt implizit aus, daß eine innerhalb der Verwaltung vorhandene Information Dritten — d. h. außerhalb der Verwaltung stehenden Personen — verborgen bleiben soll. Unter Berücksichtigung dieser Erkenntnis kann nun für „Datengeheimnis" definiert werden: *Datengeheimnis ist ein Geheimnis, dessen Kenntnis sich im wesentlich auf Personen beschränkt, die mit Angelegenheiten der Datenverarbeitung betraut sind. Es verpflichtet diesen Personen vornehmlich, ihr im Zusammenhang mit der Datenverarbeitung erworbenes Wissen — insbesondere die Kenntnis von Individualinformationen — Dritten, d. h. außerhalb der Verwaltung stehenden Personen, nicht mitzuteilen.*

Dieses Datengeheimnis ist in der Tat unerläßlich, zumal es praktisch keine technischen Mittel gibt, um die an der Datenverarbeitungsanlage tätigen Personen an einem Mißbrauch zu hindern.

Weiterhin erfüllt das Datengeheimnis die Funktion, für eine Auskunftserteilung der Behörden nur die nicht dem Datengeheimnis unterfallenden Informationen zuzulassen. Freilich ist auch die Erteilung von Auskünften an rechtliche Gesichtspunkte gebunden, die von sich aus eine unkontrollierte Weitergabe verbieten. „Ein allgemeines Recht auf Auskunftserteilung durch Behörden haben Privatpersonen nicht, jedoch kann sich ein Auskunftsanspruch aus einer vorhandenen öffentlich-rechtlichen Beziehung ergeben" [14]).

So bleibt noch die Forderung, die unzulässige Weitergabe an Dritte durch geeignete organisatorische und technische Mittel vornehmlich für die Personen zu verhindern, die nicht an der Informationsverarbeitung beteiligt sind [15]).

Als Kontrollmaßnahmen sind aus Artikel 2 Abs. 1 GG Beseitigungs- und Unterlassungsansprüche, bei Schäden auch Entschädigungsansprüche begründbar [16]).

4. Zusammenfassung

Es wird im Hinblick auf ein Datenschutzgesetz vorgeschlagen:

Alle im Bereich der Verwaltung vorhandenen Individualinformationen unterliegen hinsichtlich ihrer Weitergabe an private Dritte einem Datengeheimnis. Die Weitergabe ist nur mit Einwilligung des Betroffenen zulässig. Bei Weitergabe ohne Einwilligung hat der Betroffene einen Unterlassungsanspruch gegen die weitergebende Behörde und einen Beseitigungsanspruch gegen den Empfänger.

---

[6]) siehe oben Topos V. 3.
[7]) siehe oben Topos I. 2.1.1.
[8]) BVerfGE 17, 313 ff.
[9]) Maunz - Dürig - Herzog, Artikel 20 N. 115
[10]) vgl. die Aufzählung bei Düwel, 50 ff.
[11]) z. B. § 61 BGB; § 14 SoldatenG
[12]) vgl. § 3 des Hessischen Datenschutzgesetzes, weiterhin Punkt 1 der Dienstanweisung der Datenzentrale Schleswig-Holstein und § 3 des CDU-Entwurfs eines Datenschutz-Gesetzes für Rheinland-Pfalz
[13]) Düwel, 232 Nr. 3
[14]) Wolff (1), 291
[15]) siehe § 2 Hess DSchG
[16]) Gallwas, 127 bis 137

Bei Entstehung eines Schadens ist Ersatz zu leisten. Auch immaterieller Schaden ist zu ersetzen, falls es sich um eine (oben erweiterte) Amtspflichtverletzung eines Beamten (im haftungsrechtlichen Sinn) handelt.

Diese Grundsätze gelten wegen gleicher Interessenlage auch für die *Informationsveröffentlichung* [17]).

[17]) s. o. Vorbem. zu Topoi V. ff., 1. Fallgruppe

VII. Topos Informationsverbund

1. Definition und Bedeutung

1.1. Definition

Informationsverbund liegt allgemein bei *Koppelung von Informationssystemen zwecks integrierter Datenverarbeitung* vor. Hier soll der Begriff eingeengt gebraucht werden für Verbund-Informationssysteme *mit mindestens einem öffentlichen und einem privaten Informationssystem* bei — zumindest teilweiser — integrierter Datenverarbeitung. Er ist dann gegeben, wenn die Datenverarbeitungsanlagen öffentlicher und nicht-öffentlicher Stellen derart miteinander verbunden sind, daß zwischen ihnen — zumindest teilweise — Informationen ungehindert ausgetauscht [1]) werden können.

Die Definition zeigt, daß es sich beim Informationsverbund im hier definierten Sinn um etwas Neues handelt: um den Verbund von computerunterstützten Informationssystemen. Da der Verbund das ganze System betrifft, werden die bisher getrennt abgehandelten Stadien der Informationsverarbeitung teilweise miteinander erörtert.

Es ist aber angesichts handfester Hinweise auf die bereits beabsichtigte Realisierung von Datenverbundssystemen notwendig, sich im Gutachten eingehender damit zu befassen und für die Praxis akzeptable Regelungen zu finden.

Da es eventuellen Gefahren zu wehren gilt, sollen einige negative (reale und hypothetische) Möglichkeiten aufgezeigt werden:

1.2. Beispiele

So haben etwa Vertreter privater Versicherungen erklärt, das Personenkennzeichen, das für den Bereich der staatlichen Verwaltung eingeführt werden soll, auch in ihrem Bereich zu verwenden. Wirtschaftlich sinnvoll ist dieses Vorhaben dann, wenn über das PKZ es den Versicherungen ermöglicht wird, auf im Verwaltungsbereich unter demselben PKZ gespeicherte Informationen zurückzugreifen.

So können bei Bestehen eines Verbundsystems zwischen einer privaten Krankenversicherung und der staatlichen Gesundheitsbehörde (woran die Krankenversicherungen sicher sehr interessiert wären!) die Angaben einer Person, die der Versicherung beitreten will, sofort auf ihre Richtigkeit überprüft werden. Es wäre ja möglich, daß der Beitrittswillige bei der Schilderung seines Gesundheitszustands eine meldepflichtige Geschlechtskrankheit vergessen oder verschwiegen hätte.

Ein anderes Beispiel wäre ein Verbundsystem aller Krankenanstalten mit der Polizei. Eine Person, die wegen Verletzungen aus einer Schlägerei ein Krankenhaus aufsuchen muß und dort ihre Personalien angibt, würde sofort der Gefahr polizeilicher Ermittlungen ausgesetzt sein, wenn die Personalien sowie Art und Herkunft der Verletzung über das Verbungsystem der Polizei zukommen.

Eine weitere Motivation für den Verbund ist das wachsende Planungsinteresse des Staates an Daten aus der Privatwirtschaft. Ein Verbundsystem würde dem Staat wesentlich weiterhelfen. Um beispielsweise den finanziellen staatlichen Einsatz auf dem Gebiet des Wohnungsbaus optimal kalkulieren zu können, bedarf die Verwaltung u. a. einer großen Menge von Angaben über die Auftrags- und Kostenlage in der privaten Bauwirtschaft, über die soziale Struktur in verschiedenen Wohnsiedlungen und über die Perspektiven, die sich aus der Einführung des Städtebauförderungsgesetzes hinsichtlich der Forderungen von Grundstücksverkäufen ergeben.

Ein letztes Beispiel: Um soziale Katastrophen zu vermeiden, müßten Regierung und Verwaltung über die Personallage in den wichtigsten Großbetrieben informiert sein. Denn nur so ist es möglich, bei Massenentlassungen frühzeitig einer Arbeitslosenwelle bereits präventiv durch Staatsaufträge großen Stils zu begegnen.

1.3. Bedeutung

Freilich sind Verbindungen zwischen Staat und Privatwirtschaft nichts prinzipiell Neues; auch bisher gab es vielfältige Querverbindungen personeller, organisatorischer und juristischer Art; insofern sei es nicht einzusehen, so könnte man argumentieren, daß durch einen Datenverbund eine neue Lage entstünde. Doch liegt es hier wie überall, wo integrierte EDV-Systeme eingeführt werden: Die manuelle IV, die isoliert voneinander in vielen Behörden parallel verlief, enthielt so viele Reibungsflächen, Schwerfälligkeit und unpräzise Zusammenarbeit, daß dadurch der einzelne genügend geschützt wurde.

[1]) Das Wort ist hier untechnisch zu verstehen!

Der Datenverbund bringt nun zur personellen, organisatorischen und juristischen Verbindung eine neue hinzu, nämlich die technische, die die weitere funktionelle Integration der Aufgaben und die Reorganisation der Informationsströme im Gefolge hat. Der Verbund beseitigt die Schwerfälligkeit durch minimale Arbeitszeiten, er hebt die räumlichen Entfernungen auf, er zwingt Staat und Wirtschaft ungeachtet ihrer Interessengegensätze zur präzisen Zusammenarbeit, denn die hohen Kosten eines Verbundsystems sind nur dann wirtschaftlich angelegt, wenn ein möglichst genaues und effektives Zusammenwirken erreicht wird. Mit dem Wegfall dieser Hemmnisse ist gleichzeitig für den einzelnen der Schutz verschwunden, der in der konventionellen IV lag. Er steht einer reibungslos arbeitenden Maschinerie schutzlos gegenüber, die zu völlig verschiedenen Zwecken dem Staat bzw. Privaten gegebene Informationen zu einem hybriden Neuen integriert.

2. Rechtliche Würdigung

2.1. Grundgedanken

Insofern stellt mithin der Datenverbund etwas Neues dar, das rechtlicher Würdigung bedarf. Dabei sind folgende Gesichtspunkte zu beachten:

a) Der Datenverbund als Integration der Informationsverarbeitung öffentlicher und privater Stellen ist nicht einheitlich öffentlichem oder privatem Recht zu unterwerfen. Vielmehr verlangt ein integrierter Sachverhalt auch eine integrierte rechtliche Lösung, die also sowohl öffentliche als auch private Regelungen umfaßt. Dazu kommen noch strafrechtliche Gesichtspunkte.

b) Aus Artikel 2 Abs. 1 wurde ein Selbstbestimmungsrecht des einzelnen hinsichtlich seiner Individualinformationen abgeleitet; dieses Selbstbestimmungsrecht muß auch im Datenverbund gewährleistet sein.

c) Ein eigener Vorschlag für eine datenschutzrechtliche Regelung des Datenverbunds ist aber nur sinnvoll, wenn die rechtlich relevanten Vorgänge nicht schon in den Topoi über die Verarbeitung von Individualinformationen durch öffentliche und nichtöffentliche Stellen geregelt sind.

   Dabei ist davon auszugehen, daß trotz verschwimmender Grenzen und trotz der tatsächlichen Verquickung zwischen öffentlicher Verwaltung und Wirtschaft die rechtliche Verschiedenheit beider Bereiche weiterbesteht. Es ist geradezu ein unverzichtbares Charakteristikum des im GG konzipierten deutschen Rechtssystems, die Handlungen des Staates gegenüber dem einzelnen rechtlich anders zu bewerten als die der einzelnen untereinander. Die Rechtsgründe, die dem Staat bei Eingriffen in den Rechtsbereich des einzelnen zur Seite stehen, sind eben grundlegend andere als die eines Privaten, der in den Rechtsbereich eines einzelnen eingreift. Aus dieser Tatsache leitet ein ganzes Rechtsgebiet, das sich „Öffentliches Recht" nennt, seine Existenzberechtigung ab. Und entsprechend dieser Trennung hat das öffentliche Recht auch ein Kriterium entwickelt, das seinen Regelungsbereich von dem des Privatrechts abgrenzt: die Erfüllung einer materiell öffentlich-rechtlichen Aufgabe, d. h. Verwaltungstätigkeit zur Wahrnehmung von Angelegenheiten von Gemeinwesen und ihren Mitgliedern [2]).

2.2. Reduktion auf bekannte Topoi

Mit dieser Begründung darf versucht werden, die rechtliche Würdigung des Datenverbundes in die Topoi der Ermittlung, Erfassung, Verarbeitung, des Austausches und der Löschung der Individualinformationen durch öffentliche und nicht-öffentliche Stellen aufzulösen.

Für die Informationsermittlung und -weitergabe sei dies kurz ausgeführt:

Ermittelt eine Behörde, so unterliegt diese Ermittlung der hier vorgeschlagenen Regelung. Will sie ermittelte Informationen an Private *abgeben,* so bedarf sie dazu der Einwilligung des Betroffenen (und zwar auch *im* Verbund!); Verbundsysteme, die etwa per on-line Zugriff ohne diese Einwilligung Individualinformationen an Private abgeben, sind deshalb verfassungswidrig.

Ermittelt ein Privater, so unterliegt er darin zunächst den oben aufgeführten strafrechtlichen Vorschriften. *Gibt* er die ermittelte Information an eine Stelle der öffentlichen Verwaltung *ab,* so kann sich die Verwaltung damit nicht um die Einhaltung der Ermittlungsvorschriften drücken. Zwar handelt es sich im Sinne des Gutachtens um eine Weitergabe, die der Einwilligung des Betroffenen bedarf, wenn es sich nicht um allgemein zugängliche Informationen handelt. Aber für die öffentliche Verwaltung stellt sich dieser Vorgang zugleich als Ermittlung dar, der den dafür gefundenen Regelungen unterliegt, also nur im Rahmen ihrer Zuständigkeit und nur in bezug auf Minimal- und Unterstützungsinformationen zulässig ist. Da der einzelne rechtlich gehalten ist, behördlich zulässige Ermittlungen zu dulden, bedarf es insoweit keiner Einwilligung für die Weitergabe. Denn die Behörde könnte sich die Information auch direkt vom Betroffenen ohne dessen Einwilligung holen. Im übrigen bleibt es aber bei den oben für Informationsermittlung, -erfassung usw. sowie Informationsweitergabe entwickelten Regeln.

Ein Datenverbund, der den hier dargelegten Regelungen nicht entspricht, würde damit nicht nur dem hier vorgeschlagenen Datenschutzgesetz widersprechen, sondern auch verfassungswidrig sein, da er die aus Artikel 2 Abs. 1 abgeleiteten Rechte des einzelnen negieren würde. Verfassungsrechtlich bedenklich ist beispielsweise damit auch der in der Diskussion aufgetauchte Vorschlag, die Kontrolle eines umfassenden Datenverbundes einem eigenen „Parlament" zu unterstellen, das aus den Vertre-

[2]) Wolff (1), 13; vgl. auch oben zur Definition des „Öffentlichen"

tern von Interessengruppen gebildet werden soll. Denn die Kontrolle von Grundrechtsverletzungen durch den Staat unterliegt nach Artikel 19 Abs. 4 nur den Gerichten, die Kontrolle der Rechtmäßigkeit des Handelns von Privaten nach der abschließenden Aufzählung der Organe, die Staatsgewalt ausüben, nach Artikel 20 Abs. 2 ebenfalls den Gerichten. Rechtlich möglich wäre es aber, derartige Kontrollinstanzen in einen Rechtsweg einzubauen, der die eigentliche Kontrolle, also das Recht, mit Verbindlichkeit eine Rechtsverletzung festzustellen, bei den Gerichten beläßt.

VIII. Topos Informationslöschung

1. Definition und Schutzbereich

Löscht die Verwaltung gespeicherte Individualinformationen, so daß ihre Verwendung in keiner Weise mehr möglich ist, dann bestehen folgende Fälle:

— Entweder benimmt sie sich einer Eingriffsmöglichkeit in den Freiheitsraum des Bürgers: Dann wird insoweit Artikel 2 Abs. 1 GG nicht verletzt.

— Oder die Verwaltung löscht Informationen, auf deren Bestehen der Bürger ein Recht hat, z. B. das Vorliegen einer Amnestie.

— Oder die Löschung wird *nicht* vorgenommen, obwohl der Bürger ein Recht auf Löschung hat. Beispiel: Die Daten sind unrechtmäßig erfaßt und gespeichert. Eine Straftat wird nicht getilgt trotz Fristablaufs — erhebliche Behinderung der Entfaltung der Persönlichkeit (z. B. Resozialisierung) bereits durch die Existenz solcher Daten, ferner durch die technischen Möglichkeiten von Austausch und Weitergabe [1]).

[1]) Eyermann - Fröhler, § 42 Anm. 41
[2]) Evers, 53 Anm. 20
[3]) Zum vieldiskutierten Recht bzw. der Pflicht zur periodischen Löschung der gespeicherten Individualinformationen ergeben sich folgende 2 Fälle:
— Recht des Bürgers? vgl. hierzu die Ausführungen in Teil D
— Recht der Verwaltung? ebd.

2. Zulässigkeit einer Beschränkung

Die Löschung bzw. Nichtlöschung ist solange rechtmäßig, als nicht Rechtsvorschriften das Gegenteil anordnen. Solche Rechtsvorschriften sind beispielsweise § 5 Straftilgungsgesetz sowie verwaltungsinterne Anordnungen über die Vernichtung von Informationen, Akten und Aufzeichnungen.

Im Unterschied zu einigen anderen Phasen der IV ist die Löschung von Individualinformationen als rechtliches Problem bereits erkannt und normativ geregelt worden. Deshalb kann auf eine verfassungsrechtliche Prüfung bestehender Löschungsvorschriften verzichtet werden.

Soweit es sich dabei um Maßnahmen von Justizbehörden handelt (und das wird oft der Fall sein), sind diese entweder über § 23 und § 24 EGGVG oder über den normalen Verwaltungsweg erzwingbar [2]).

Für ein DSchGesetz ergibt sich:

Da das Problem bereits weitgehend erkannt und geregelt ist, würde ein DSchGesetz nichts Neues bringen. Wünschenswert wäre lediglich ein Hinweis, daß die bereits vorhandenen Löschungsbestimmungen auch — und besonders — bei EDVAn durchzusetzen sind [3]).

IX. Topos Einsichts- und Auskunftsrechte, Berichtigungs- und Löschungsansprüche

1. Verhältnis der Rechte zueinander

Bisher wurde wiederholt von einzelnen dieser Rechte gesprochen. Hier ist der Ort, sie zusammenfassend zu erörtern. Als direkte Folge des Interpretationsergebnisses von Artikel 2 Abs. 1 GG ergibt sich, daß dem einzelnen Möglichkeiten zur Verfügung stehen müssen, um den Gang der Verarbeitung seiner Individualinformationen verfolgen und bei rechtlichen und tatsächlichen Mängeln einschreiten zu können. *Hier ist der rechtliche Sitz von Einsichts-, Auskunfts-, Berichtigungs- und Löschungsrechten.*

Man würde sich nun die Sache zu leicht machen, wenn man dem einzelnen diese Rechte einfach kumulativ zur Verfügung stellte. Vielmehr stehen diese Ansprüche in einem bestimmten Verhältnis zueinander, dessen Klärung die Voraussetzung dafür ist, um die Zweckmäßigkeit eines Anspruchs für den Einzelfall festzustellen. Denn es sind sehr wohl Fälle denkbar, in denen beispielsweise zwar ein Berichtigungs-, aber kein Auskunftsrecht zum

Zuge kommt. Es gilt also, die Ansprüche inhaltlich zu klären und ihr Verhältnis zueinander zu untersuchen.

Gemeinsam ist jedoch allen Ansprüchen, daß zuerst Individualinformationen im Bereich der Verwaltung vorliegen müssen, und zwar in fixierter Form: Denn nur eine fixierte Information kann eingesehen, berichtigt oder gelöscht werden. *Somit sind alle Ansprüche erst vom Augenblick der Speicherung einer Individualinformation an geltend zu machen.*

Nunmehr gilt es, die Unterschiede im einzelnen zu untersuchen. Als erste Unterscheidung bietet sich an: Einsichts- und Auskunftsrechte sind nur Rechte, die die *Unterrichtung des Betroffenen* sicherstellen. Berichtigungs- und Löschungsansprüche dagegen ermöglichen es dem Betroffenen, die Konsequenzen aus der Unterrichtung zu ziehen und seine Rechte auch durchzusetzen. *Einsichts- und Auskunftsrechte seien deshalb Unterrichtungsansprüche, Berichtigungs- und Löschungsansprüche oder Folgeansprüche genannt.* Unterrichtungsansprüche sind die Voraussetzung zur Geltendmachung von Folgeansprüchen. Die bloße Gewährung von Unterrichtungsansprüchen würde dem Bürger wenig nützen: Das Wissen um eine Rechtsverletzung ist noch nicht unbedingt gleichbedeutend mit der Möglichkeit, die Rechtsverletzung auch zu beseitigen. Umgekehrt ist die bloße Gewährung von Folgeansprüchen für den einzelnen sinnlos, wenn er keine Gelegenheit hat festzustellen, wann er seine Rechte geltend machen kann. So kann für ein Datenschutzgesetz nicht die Gewährung von Unterrichtungs- oder Folgeansprüchen, sondern nur die Verbindung von Unterrichtungs- und Folgeansprüchen in Betracht kommen.

2. Die einzelnen Ansprüche

2.1. Unterrichtungsansprüche

2.1.1. Einsichtsrecht

Das Einsichtsrecht als Unterrichtungsanspruch ist dabei zu verstehen als das Recht des Bürgers, eigenhändig Individualinformationen aus Unterlagen zu entnehmen, die in der Verfügungsgewalt der öffentlichen Verwaltung sind. Die Verwaltung muß ihm diese Unterlagen nur zugänglich machen, darüber hinaus braucht sie nicht tätig zu werden.

Dies ist der Fall bei Akten, die in herkömmlicher Form geführt werden. Aus ihnen ersieht der Bürger, welche Individualinformationen im Bereich der Verwaltung von ihm existieren und wer diese Informationen erhielt. Anders ist die Lage aber, wenn der Akteninhalt einer EDVA eingespeichert wird: Ein Einsichtsrecht im oben definierten Sinn nützt dem einzelnen nichts, da er etwa aus ihm vorgelegten Magnetbändern nichts entnehmen kann. Auch die Programme, die ihm Auskunft darüber geben sollen, wer auf die Informationen zugreifen kann, oder bereits zugegriffen hat, werden dem Normalbürger, der keine Ausbildung in den Programmiersprachen genossen hat, nichts sagen. Wohl aber besteht die Möglichkeit, über Bildschirm im Dialogverkehr die gewünschten Informationen abzufragen. Außerdem kann man einen Speicherauszug verlangen, evtl. gegen entsprechende Verwaltungsgebühr. Abgesehen davon, daß dies bereits einem Auskunftsrecht sehr nahekäme, würde der print-out zwar über Art und Inhalt der gespeicherten Information etwas aussagen, jedoch nichts darüber, wer auf diese Informationen zugreifen kann bzw. zugegriffen hat. Eine Protokollpflicht der Behörde, verbunden mit dem Einsichtsrecht, könnte dem abhelfen [1]). Ein Einsichtsrecht krankt eben daran, daß es dem Bürger auferlegt, aus den zugänglich gemachten Informationen auch tatsächlich etwas zu entnehmen. Es ist keinem Bürger zuzumuten, sich unter Umständen durch einige hundert Seiten print-out durchzuarbeiten und sie auf ihre Richtigkeit zu überprüfen. Ein Einsichtsrecht ist dann unbrauchbar, wenn es dem Bürger mangels Spezialkenntnissen unmöglich ist, aus dem ihm vorgelegten Material Informationen zu entnehmen. Eine solche Lage bringt aber die Einführung der EDVA mit sich; ein Einsichtsrecht ist also nur bedingt geeignet: zwar notwendig, aber für sich allein ungenügend.

2.1.2. Auskunftsrecht

Das Auskunftsrecht als Unterrichtungsanspruch beinhaltet, daß der Bürger von der speichernden Behörde Informationen darüber bekommt, welche Individualinformationen über ihn ermittelt und gespeichert sind, und wer auf diese Informationen zugreift. Dabei bekommt der Fragende die Materialien, die diese Informationen über ihn enthalten, nicht zu Gesicht; die Behörde muß ihm diese Informationen nicht nur zugänglich machen, sie muß selbst aktiv informieren und die Information aufbereiten (verdichten). Das Auskunftsrecht beinhaltet, daß die Auskunft erst erteilt ist, wenn der Auskunftsuchende in der Lage ist, die Information aufzunehmen. Der Bürger muß also keine Programme lesen, er kommt mit der EDVA gar nicht erst in Berührung. Damit wird der Nachteil des Einsichtsrechts beim Auskunftsrecht vermieden.

Hinsichtlich der Rechtsnatur der Auskunft ergibt sich nichts Neues: wie auch bisher ist die Auskunft kein Verwaltungsakt, abgesehen von dem Fall, daß die Behörde ein bestimmtes Verhalten zusagt [2]). Dogmatisch ist also das Auskunftsrecht die Festlegung eines Falles der allgemeinen Leistungsklage.

Ein Auskunftsrecht, das direkt aus Artikel 2 Abs. 1 hergleitet wird, muß inhaltlich uneingeschränkt sein, soweit es sich im Rahmen dieser Vorschrft hält, d. h. soweit es die eigenen Individualinformationen des Auskunftssuchenden betrifft [3]). Im einzelnen muß sich das Auskunftsrecht also erstrecken auf

— den Inhalt der gespeicherten Individualinformationen (z. B. dreimonatige Gefängnisstrafe eingetragen für den Auskunftssuchenden X),

[1]) s. u. 2.1.3. zum Datenjournal

— das Datum der Eingabe von Individualinformationen, das gleichzeitig das Datum der Ermittlung mit angeben muß,

— das Datum jeden Zugriffs, der nicht von der ermittelnden Behörde vorgenommen wurde,

— eindeutige Bezeichnung von Namen und Anschrift der zugreifenden Behörde oder Person,

— inhaltliche Angabe der Individualinformationen, die Gegenstand des Zugriffs waren,

— den Rechtsgrund des Zugriffs.

Wird die Auskunft so umfassend erteilt, so sind auch die rechtlich bedeutsamen Phasen der Informationsverarbeitung erfaßt: Datum von Ermittlung und Austausch, Inhalt der ermittelten bzw. ausgetauschten Informationen; die Inhaltsangabe der gespeicherten Daten gibt Auskunft über etwaige Veränderungen. Kann mangels Vorliegens einer Information keine Auskunft erteilt werden, so muß mit einer Löschung gerechnet werden.

2.1.3. Datenjournal

Nach der rechtlichen Grundlegung des Auskunftsrechts stellt sich nun die Frage, wie eine derartig umfassende Auskunft praktisch verwirklicht werden kann, ohne einerseits der Verwaltung unzumutbare Arbeitslasten aufzubürden, und ohne andererseits das rechtlich begründete Auskunftsbedürfnis des einzelnen zu schmälern.

Erforderlich ist zunächst, daß alle für eine Auskunft relevanten Vorgänge registriert werden. Dies geschieht am zweckmäßigsten in einem sog. *Datenjournal,* also einem Protokoll über alle relevanten Vorgänge, welches über ein entsprechendes Programm im Rahmen eines jeden Informationssystems automatisch zu erstellen wäre.

Auskunftsrecht und Datenjournal gehören also sachlich zusammen[4]*; die Auskunft ist bei EDVA ohne Datenjournal nicht ausreichend zu erteilen.* Dabei ist das Datenjournal über entsprechend geschützte Programme (Datensicherung!) automatisch abzuspeichern.

Es fragt sich nun weiter, in welcher Weise Auskünfte aus dem Datenjournal erteilt werden können. In Betracht kommt die Zusendung eines Auszugs, der die erfragten Angaben enthält. Das ist arbeitsmäßig kaum zu bewältigen, obwohl es denkbar ist, Programme zu erstellen, die diese Auszüge selbständig zusammenstellen und ausdrucken. Das Problem ist die Kostenfrage.

§ 5 Abs. 1 des IPA-Vorentwurfs bestimmt, daß die Auszüge gebührenfrei sein sollen. Zweifellos würden dadurch der Verwaltung hohe Kosten erwachsen[5]). Als rechtlicher Gesichtspunkt wäre hier ins Feld zu führen, daß der Bürger nicht mit Gebühren belastet werden darf, wenn er eine Rechtsverletzung feststellen und dagegen Folgeansprüche geltend machen will. Es würde gegen Artikel 19 Abs. 4 GG verstoßen, wenn die Höhe der Gebühren so festgesetzt würde, daß damit dem finanziell schwachen Bürger der Weg zum Gericht praktisch versperrt wäre[6]). Möglich wäre allerdings eine geringe Gebühr, die einerseits jeder Bürger aufbringen kann, und andererseits die Verwaltungskosten in kleinerem Umfang halten würde. So könnte man an einen Betrag denken, der 5 DM nicht überschreitet. Sinnvoller ist die Einrichtung entsprechender Datensichtstationen mit Benützung auf Anfrage ohne automatische Zusendung von print-outs, kombiniert mit gebührenniedrigem Ausdruck von gewünschten Daten.

Die Normierung eines Auskunftsanspruchs hat noch einen weiteren Vorteil: Der Bürger bedient sich seiner nur dann, wenn er sich durch die Informationsverarbeitung in seinen Rechten verletzt glaubt. Die Verwaltung ist also nicht verpflichtet, jede Ermittlung oder jeden Austausch dem Betroffenen durch Zusendung eines print-outs zu melden; eine derartige Pflicht würde die Verwaltung überlasten und den Bürger mit einem Wust von Papier eindecken, den er bald nicht mehr zu bewältigen vermag; obendrein ist nichts so gut geschützt als das, was in einem unbewältigbaren Berg von print-outs verborgen ist . . .

2.2. Die Folgeansprüche

2.2.1. Berichtigungsanspruch

Ein Berichtigungsanspruch folgt aus dem aus Artikel 2 Abs. 1 GG fließenden Recht des einzelnen, für die Richtigkeit seiner Individualinformationen Sorge tragen zu können. Berichtigungsansprüche sind also Ansprüche, die auf den Inhalt einer gespeicherten Information abzielen. Der Anspruch kann geltend gemacht werden, wenn entweder die betreffende Information falsch gespeichert ist (Falschspeicherung) oder eine richtig gespeicherte Information inhaltlich umgestaltet wird (Informationsveränderung).

Über die Wortbedeutung hinaus muß der Berichtigungsanspruch das Recht beinhalten, fälschlich gelöschte Informationen wieder speichern zu lassen.

Da die Berichtigung einer Information kein Verwaltungsakt ist (auch nicht die Neuspeicherung nach vorangegangener fälschlicher Löschung), ist der Berichtigungsanspruch dogmatisch ebenfalls die gesetzliche Festlegung eines Falles der allgemeinen Leistungsklage.

---

[2]) BVwG in VwRspr. 12, 233; OVG Münster in OVGE 13, 167

[3]) Simitis (2), 681; H. Weber, 56

[4]) vgl. auch IPA-Vorentwurf § 5 Abs. 1

[5]) vgl. dazu Dr. Hauff, MdB, in: KEDV 14, 22

[6]) vgl. dazu BVerfGE 11, 143 und 14, 284; BVwGE 8, 102 ff.

[7]) Nur mittelbar hierher gehört die Frage der regelmäßigen Löschung von Ballastinformationen; unserer Auffassung nach sollte auf absehbare Zeit *keine* einmal gespeicherte Individualinformation endgültig gelöscht, sondern auf langsamere externe Speicher (Band, Magnetkarten) umgespeichert werden, bis durch sorgfältige Untersuchung dieses sehr verwickelte Problem nach allen Seiten befriedigend gelöst ist — z. B. unter der Berücksichtigung des Interesses künftiger historischer Wissenschaft an den Anfängen der Verwaltungsautomation!

2.2.2. Löschungsanspruch

Der Löschungsanspruch [7]) endlich besagt, daß der Bürger das Recht hat,

— gespeicherte Informationen löschen zu lassen, wenn ihre Ermittlung rechtswidrig war;

Beispiel: Eine Kommunalverwaltung erfragt das Einkommen eines Bürgers in einer anderen Stadt, obwohl dieser mit der Kommune in keiner Rechtsverbindung steht. Die Behörde ermittelt damit eine Information, die nicht mehr Unterstützungscharakter hat.

— rechtmäßig ermittelte Informationen löschen zu lassen, wenn die Speicherung zur Zeit der Geltendmachung des Anspruchs rechtswidrig ist.

Beispiel: Nach § 7 Abs. 1 Nr. 1 StraftilgungsG muß die Geldstrafe des X nach fünf Jahren getilgt werden. Nach sechs Jahren erfährt X, daß seine Strafe nicht getilgt ist. Wenn er *jetzt* seinen Löschungsanspruch geltend macht, so ist er begründet. Hätte er ihn nach vier Jahren geltend gemacht, so wäre der Anspruch nicht begründet.

Der erste Fall zeigt, daß die Wirkung die Folge unrechtmäßiger Ermittlung sein muß. Ein Löschungsanspruch in dieser Ausprägung hat also nur dann einen Sinn, wenn die Ermittlung einigermaßen faßbaren Regelungen unterworfen ist. Auch die Umkehrung ist richtig: Die rechtliche Regelung der Ermittlung ist sinnlos ohne Löschungsanspruch. Der Austausch ist mit dem Löschungsanspruch ebenfalls in Verbindung zu bringen: denn ausgetauschte Informationen über einzelne dürfen nicht gespeichert werden.

Der zweite Fall ist rechtlich bereits geregelt: Er betrifft die Tilgungsvorschrift für bei der Verwaltung — hier hauptsächlich bei der Justizverwaltung — geführten Register. Ein Hinweis auf diese Vorschriften, der allerdings den Ausnahmecharakter klarstellen müßte, dürfte für ein Datenschutzgesetz genügen.

Auch der Löschungsanspruch ist ein Fall der allgemeinen Leistungsklage; er ist gegen die speichernde Behörde zu richten.

X. Topos Organisatorische Kontrollmöglichkeiten

1. Notwendigkeit

Unter organisatorischen Kontrollmöglichkeiten sollen im folgenden die Möglichkeiten des Datenschutzes verstanden werden, die sich aus der Staats- und Behördenorganisation ergeben und die geeignet sind, die Verarbeitung von Individualinformationen durch öffentliche Stellen wirksam zu kontrollieren. Konkret geht es also um die Frage, welche bereits bestehende oder neu zu schaffende Stelle im Staatsaufbau geeignet und in der Lage ist, die Verwaltung hinsichtlich ihrer Informationsverarbeitung zu überwachen.

Diese Art der Kontrolle kann sich jedoch *nicht als Alternative* zu den Kontrollmöglichkeiten des einzelnen verstehen. *Vielmehr ist sie integrierender Bestandteil eines umfassenden, die Verarbeitung von Individualinformationen betreffenden Regelungssystems* [1]). Zutreffend bemerkt Simitis dazu: „Je präziser freilich die individuelle Kontrolle ausgestaltet wird, desto deutlicher macht sich die Notwendigkeit einer institutionellen Absicherung bemerkbar. Das zeigt sich schon am einfachen Beispiel der Mitteilungspflicht (hier: Auskunftspflicht): Sie erfüllt ihre Aufgabe nur, wenn jederzeit ein Überblick über die bestehenden Datenbanken gewonnen und überdies die strikte Einhaltung ihrer Pflichten nachgeprüft werden kann" [2]).

Die Notwendigkeit derartiger organisatorischer Kontrollmaßnahmen läßt sich mit Podlech auch aus dem Rechtsstaatsprinzip herleiten. Geht man nämlich davon aus, daß Informationsverarbeitung durch die Verwaltung die Möglichkeit potentieller Beeinflussung durch die Verwaltung in sich bringt, so haben wir es — bei fehlender institutioneller Kontrolle — mit unkontrollierter öffentlicher Macht zu tun. Aber „unkontrollierte öffentliche Macht widerspricht dem Rechtsstaatsprinzip" [3]).

2. Reichen die bisher vorhandenen Mittel der verwaltungsinternen Aufsicht aus?

Die Verwaltung verwirklicht institutionelle Kontrolle ihres Handelns bisher im hierarchisch gegliederten Behördenaufbau. Innerhalb eines Zweiges kontrolliert eine höhere Behörde die niedrigere. Dabei wird als Mittel der Kontrolle — entsprechend dem Maß an Selbständigkeit, das einzelne Behörden durch verfassungsmäßige Rechte ihrer Verwaltungsträger genießen [4]) — Rechts- und/oder Fachaufsicht angewandt. Die Ausübung beider Formen der Aufsicht muß zwangsläufig mit einem Recht der oberen Behörde gekoppelt sein, das diese berechtigt, sich über alle Angelegenheiten der unteren Behörde zu unterrichten [5]); nur so ist es der Aufsichtsbehörde möglich, bei Unregelmäßigkeiten rechtlicher und/oder tatsächlicher Art einzuschreiten.

Dieses hier — bewußt nur grob skizzierte — System beruht demnach darauf, daß das Handeln einer untergeordneten Behörde für die Aufsichtsbehörde

[1]) so auch Podlech, 475
[2]) Simitis (2), 681
[3]) Podlech a. a. O.
[4]) vgl. Artikel 26 Abs. 2 GG
[5]) vgl. das sog. Informationsrecht in § 111 BayGO

überschaubar ist. Die Aufsichtsbehörde muß tatsächlich zur Kenntnisnahme in der Lage sein. Ob diese Überschaubarkeit nach der Einführung von EDVA und dem Existieren einer integrierten Verwaltung oder gar eines Datenverbundes noch gegeben ist, muß bezweifelt werden. Hier geht die Verknüpfung und der Austausch von Informationen intern vor sich, ja es ist nicht einmal sicher, ob eine speichernde Behörde vom Zugriff einer fremden Behörde etwas erfährt. Wie kann dann eine Aufsichtsbehörde etwa der speichernden Behörde den Austausch verbieten? *Wenn nur noch das fertige Verwaltungsergebnis die Maschine verläßt, läuft die Aufsichtsbehörde Gefahr, ihre Aufsicht darauf beschränken und den Entstehungsvorgang aus ihrer Kontrolle entlassen zu müssen.*

Daraus erhellt, daß eine Kontrolle nur wirksam ist, wenn sie die maschineninternen Vorgänge erfaßt. Diese Vorgänge werden durch *Programme* gesteuert. Programme bestimmen, welche Behörde auf welchen Speicher zugreifen darf, Programme bestimmen, welche Individualinformationen verknüpft oder verdichtet werden und Programme verhindern den Zugriff Unbefugter. Man kann ohne Übertreibung sagen: Das Verwaltungsverfahren — verstanden als „nach außen" [6]) wirkende Fähigkeit der Behörden, die auf Prüfung der Voraussetzungen, die Vorbereitung und den Erlaß eines VAes oder den Abschluß eines öffentlich-rechtlichen Vertrags (kurz: auf Erstellung eines Verwaltungsergebnisses) gerichtet ist [7]), — wird programmiert, genauer: durch Programme abgebildet und gesteuert. Soll sich eine Kontrolle aber auf das Verwaltungsverfahren beziehen, *so muß sie die Programme kontrollieren* [8]). Dazu ist es notwendig, die Programme beurteilen und ihre Auswirkungen abschätzen zu können. Hieraus resultiert die Forderung: *Nur genehmigte und — in entsprechender Form — veröffentlichte Programme dürfen verwendet werden* [9]).

Die bisher bestehenden Aufsichtsbehörden können diese Kontrolle nicht leisten. Einerseits fehlt es ihnen an hochqualifizierten Spezialisten, andererseits an der personellen Kapazität, die eine Flut derartiger Programme bewältigen könnte. Ausschlaggebend ist aber, daß die Aufsichtsbehörden ja weithin selbst Nutznießer der Programme sind und sich somit selbst kontrollieren würden, was mit unkontrollierter Machtausübung gleichzusetzen ist.

---

[6]) „nach außen" deshalb, weil hier Schutzbereiche von Artikel 2 Abs. 1 benützt werden können

[7]) vgl. § 8 EVwVfG

[8]) so als erster Podlech, 475

[9]) ungeachtet der (unklaren) Rechtsnatur der Programme; dazu unten 5.1.2.

[10]) Podlech, 473

[11]) Simitis (2), 681

[12]) Luhmann (2), 153 f. Auch Podlech, 474, macht sich das Vorbringen Luhmanns zu eigen.

[13]) Damit verbietet sich auch jede Übertragung von Kontrollfunktionen an die Datenzentralen der Länder, solange diese dem Büro des Ministerpräsidenten zugeordnet und nicht — etwa nach dem Vorbild der Rechnungshöfe — unabhängig organisiert sind.

Da die bisherigen Aufsichtsbehörden also zur weiteren Aufsicht im Informationsverarbeitungsbereich weitgehend umfähig sein werden, kommen als Ausweg zwei Möglichkeiten in Betracht:

— Ausstattung hoher Aufsichtsbehörden mit Personal und Material,

— Neuerrichtung einer speziellen Kontrollbehörde.

3. Ausbau bestehender Aufsichtsbehörden oder Neuerrichtung einer eigenen Kontrollbehörde?

Zweifellos brächte der Ausbau bestehender Aufsichtsbehörden eine Aufblähung dieser Behörden mit sich. Es würde sich dabei etwa um eigene Abteilungen handeln, die den Ministerien einzugliedern wären. Dies ist aber wiederum unzweckmäßig, da die zu kontrollierenden Programme ja nicht zuletzt Verbindungen der einzelnen Verwaltungszweige untereinander betreffen; es müßten also interministerielle Gremien gebildet werden, die eines eigenen Verwaltungsunterbaus bedürften, usf. Von diesem Stand der Erkenntnis ist es in der Tat nicht mehr weit, zu einer selbständigen Kontrollbehörde zu kommen. Sie müßte dann überministeriell organisiert sein. So ergibt sich das etwas erstaunliche Ergebnis, daß innerhalb der Aufsichtshierarchie eine effektive Kontrolle erst „oberhalb" (bzw. neben) der Ministerien einsetzen kann, was für ein eigenes unabhängiges Kontrollamt spricht.

Rechtlich entscheidend ist aber folgender Gesichtspunkt: Wird die Kontrolle innerhalb der Verwaltungshierarchie lokalisiert, so kontrolliert sich die Verwaltung selbst. Dies kann angesichts der Wichtigkeit der personenbezogenen Informationsverarbeitung nur als höchst unbefriedigend bezeichnet werden. So vergleicht Podlech das Datenschutzrecht in seiner Wichtigkeit mit dem BGB [10]). Und Simitis zieht daraus den Schluß: „Kontrollfunktion und Verflechtung mit der Exekutive schließen einander aus" [11]). Die Richtigkeit dieser Aussage ist auch an einer Beobachtung Luhmanns nachzuweisen. Danach besteht eine Anfälligkeit sozialer Systeme — und auch die Verwaltung als ganzes ist ein derartiges soziales System —, zu versuchen, ihre Ziele unter Umgehung lästiger Vorschriften zu erreichen [12]). Gerade das Datenschutzrecht würde und wird von — einigen, nicht allen — maßgeblichen Repräsentanten der Verwaltung als übertrieben und lästig empfunden und bedarf so in hohem Maße einer institutionalisierten Kontrolle, die nicht in den Verwaltungsapparat integriert ist [13]).

Zusammenfassend wird somit festgestellt: Eine wirksame Kontrolle der Verarbeitung von Individualinformationen kann nicht durch den Ausbau bisheriger Aufsichtsbehörden erreicht werden; notwendig ist vielmehr die Errichtung einer speziellen Kontrollbehörde, die nicht in die Verwaltungshierarchie eingegliedert, d. h. mindestens nicht weisungsunterworfen ist.

4. Organisation der Kontrollbehörde

Konkrete Vorstellungen über die rechtliche Organisationsform der Kontrollbehörde sind bis jetzt nur spärlich entwickelt worden. Von den wenigen, die sich darüber Gedanken machen, kommt Simitis zwar zu dem Schluß, eine Kontrollbehörde müsse unabhängig von der Exekutive sein, zeigt aber keinerlei Wege auf, wie dieses Ergebnis in die Tat umzusetzen ist [14]). Auch Steinmüller beschränkt sich darauf, lediglich eine Anmeldepflicht für öffentliche Datenbanken zu fordern, ohne zu sagen, bei welcher Stelle denn anzumelden ist [15]).

Demgegenüber ist der — insoweit — mutige „Entwurf zum Datenüberwachungsgesetz" der IPA hervorzuheben. In seinem § 7 Abs. 1 richtet er ein „Bundesamt zur Überwachung von Datenbanken (BÜD)" ein; es soll als selbständige Bundesoberbehörde organisiert und dem Innen- und Justizminister nachgeordnet sein. Dieser Vorschlag stützt sich auf Artikel 87 Abs. 3 GG.

Die Lösung der IPA ist insoweit zu begrüßen, als sie sich bemüht, das Kontrollamt aus der Verwaltungshierarchie herauszulösen. Bundesoberbehörden sind nur für spezielle Aufgaben eingerichtet [16]) und sind nur hinsichtlich dieses begrenzten Aufgabenkreises dem betreffenden Verwaltungszweig integriert.

Nachteilig ist jedoch auch hier, daß — auch selbständige — Bundesoberbehörden weisungsunterworfen sind [17]). Mißlich erscheint insbesondere die Beziehung zum Innenministerium, das den Löwenanteil kontrollbedürftiger Materie stellt.

Doch dieser Nachteil wird ausgewogen durch § 10 Abs. 1 des gleichen Entwurfs. Nach dieser Vorschrift besitzen der Präsident, die Vorsitzenden und die Beisitzer richterliche Unabhängigkeit und sind insofern — also hinsichtlich ihrer Überwachungstätigkeit und ihrer rechtlichen Maßnahmen — dem Weisungsrecht entzogen. Diese Regelung ist dem § 11 Abs. 1 des Gesetzes über Errichtung und Aufgaben des Bundesrechnungshofes nachgebildet. Ratio legis dieser Norm ist der Gedanke, daß eine wirksame Rechnungskontrolle nur durch eine Stelle durchgeführt werden kann, die nicht selbst am Haushaltsvollzug beteiligt und der Finanzverwaltung eingegliedert ist [18]). Dieser Gedanke ist zu Recht auf die Kontrolle von Informationsverarbeitung zu übertragen: Eine wirksame Kontrolle der Verarbeitung von Individualinformationen ist nur möglich von einer Stelle, die nicht selbst an der Verarbeitung beteiligt und dem Verwaltungsapparat voll integriert ist. Da dies dem oben gefundenen Ergebnis von der Selbständigkeit der Kontrollbehörde entspricht, ist das BÜD der IPA eine gute Lösung.

Auch Podlech bringt einen Vorschlag, der zwar ähnlich klingt, aber von einer anderen Voraussetzung ausgeht [19]). Kernpunkt ist die Unterscheidung von Behörden, die über eine Datenbank verfügen („Unternehmer") und den Benutzern. Ein Benutzer darf auf den „Unternehmer" keinen Einfluß ausüben. Die Unternehmerbehörde ist deshalb nach Artikel 87 Abs. 3 GG als öffentlich-rechtliche Anstalt einzurichten; ihre Beamten müssen die richterliche Unabhängigkeit haben. Umgekehrt dürfen die Unternehmer keinen Einfluß auf die Benutzer haben; sie dürfen beispielsweise keine Daten eingeben und sind nur für die interne Betriebsführung der Zentraleinheit einer EDVA verantwortlich.

Dieser Vorschlag ist in einem entscheidenden Punkt weitgehender und auch effektiver als die Lösung der IPA: *Der Teil der EDVA, in dem das Programm abläuft und der darum der Ansatzpunkt aller Regelung sein müßte, nämlich die Zentraleinheit, wird der Verfügungsgewalt der Verwaltung weitgehend entzogen und somit Organisation als solche als wirksames Kontrollmittel benutzt.* Das hat den Vorteil, daß Kontrolle unabhängig von der momentanen Funktionsfähigkeit einer Überwachungsbehörde wie der BÜD ist. Das hat weiter den Vorteil, daß das Einrichten einer Organisationsform das Einrichten einer ganzen Behörde erspart.

Die Lösung sähe also folgendermaßen aus: Durch Bundesgesetz [20] wird eine öffentlich-rechtliche Anstalt errichtet, in deren Verfügungsgewalt alle Zentraleinheiten, die in der Bundesverwaltung vorhanden sind, übergehen. Die Beamten der Anstalt haben richterliche Unabhängigkeit und sind insofern dem Justizminister — dem die Anstalt dienstrechtlich wohl am zweckmäßigsten zu unterstellen wäre — nicht weisungsunterworfen. Entsprechendes gelte für die Länder [21]).

Die Verfasser sehen dies als die beste Lösung an. Hinsichtlich ihrer Durchsetzbarkeit geben sie sich — mit Podlech — keinen Illusionen hin. Voraussetzung wäre ein Verzicht auf wichtige Funktionen bei den einzelnen Ministerien, vor allem beim Innenministerium. Richtig sagt Podlech, daß damit nicht der Verzicht auf rechtlich Zulässiges, sondern der Verzicht auf die Möglichkeiten von rechtlich Unzulässigem verlangt wird [22]). Doch ist mindestens zweifelhaft, ob sein dringender Appell an die rechtspolitische Weitsicht der Politiker — hauptsächlich der Ressortchefs — in absehbarer Zeit Erfolg haben wird.

Wird die Lösung von Podlech nicht verwirklicht, so sehen die Verfasser auch die Lösung der IPA als vertretbar im Sinne dieses Gutachtens an.

5. Befugnisse der Kontrollbehörde

5.1. Die Lösung von Podlech

5.1.1. Keine Kontrollbehörde

Podlechs Lösung paßt deswegen so gut in das System dieses Gutachtens, weil sie die Kontrolle

[14]) Simitis (2), 681
[15]) Steinmüller (1), 88
[16]) vgl. die Aufzählung im „Sartorius" nach Artikel 146 GG
[17]) Wolff (2), 148
[18]) Wolff (3), 317
[19]) Podlech, 475
[20]) siehe Artikel 87 Abs. 3 GG
[21]) In unterschiedlicher Form nähern sich die verschiedenen „Landesämter für Datenverarbeitung" diesem Ideal, ohne es freilich zu erreichen.
[22]) Podlech, 475

der Rechte des einzelnen den Gerichten überläßt, was im Hinblick auf Artikel 19 Abs. 4 GG die geradlinigste Lösung ist, und keine zusätzliche Kontrollbehörde erfordert. Verwaltungsinterne Kontrolle ist hier wesentlich eine Frage der Organisation (und deckt sich insofern nicht nur mit modernen Auffassungen über das Gewaltenteilungsprinzip, sondern auch der modernen Organisationstheorie). Rechtskontrolle kommt den Gerichten zu.

5.1.2. Rechtliche Beurteilung von Programmen

Oben wurde festgestellt, daß das Verwaltungsverfahren programmiert werden wird. Nun enthält das Verwaltungsverfahren nicht nur reine Verfahrenvorschriften, die die Rechte des Bürgers nicht berühren, sondern ist auch zu Eingriffen geeignet, wie beim Austausch von Individualinformationen. Nach dem Rechtsstaatsprinzip bedürfen diese Eingriffe einer formellen Rechtsgrundlage, einer Norm. Somit ergibt sich, daß Programme, in denen konkrete Austauschvorgänge geregelt sind, (zumindest auch in Teilen) Normcharakter besitzen. Welcher Art diese Norm ist, ist hier zweitrangig; entscheidend ist, daß Programme nicht mehr als Verwaltungsvorschriften bezeichnet werden können. Sie müssen veröffentlicht werden [23]), bedürfen aufsichtlicher (oder besser: „unternehmerischer" i. S. Podlechs) Genehmigung, und unterliegen gerichtlicher Nachprüfung (§ 47 VwGO; Artikel 93 Abs. 1 Nr. 2 und Nr. 4 a GG).

Ein Kontrollamt ist insoweit überflüssig. Die Verfasser schlagen für das Amt, das über die Zentraleinheiten verfügen soll, die Bezeichnung *„Bundesinformationsamt"* oder *„Bundesinformationshof"* vor [24]). Entsprechend heißt die Landesbehörde „Landesinformationsamt" bzw. „-hof".

5.2. Die Lösung der IPA

Diese Lösung ist mit den Grundgedanken des Gutachtens dann vereinbar, wenn das BÜD den Rechtsweg, der für den einzelnen nach Artikel 19 Abs. 4 GG besteht, nicht praktisch versperrt. In § 6 Abs. 2 gibt der Entwurf dem Betroffenen das Rechtsmittel in die Hand, die Durchsetzung seiner Ansprüche dem BÜD zu überlassen (für den weiteren Rechtsweg siehe dann §§ 13 bis 28). Die Bedenken werden jedoch durch § 14 Abs. 1 teilweise beseitigt, der eine Verfahrensbeteiligung des einzelnen oder von Gruppierungen garantiert.

Ansonsten halten die Verfasser die Befugnisse des BÜD hinsichtlich der Verarbeitung von Individualinformationen für ausreichend. Da sie jedoch den Vorschlag Podlechs favorisieren, verzichten sie auf eine inhaltliche Wiederholung des § 12 des Entwurfs.

---

[23]) Podlech, 475. Wie dies zu geschehen hat, etwa in Form von zu standardisierenden Programmbeschreibungen, mag dahinstehen.

[24]) Weitere EDV-Befugnisse außerhalb des Datenschutzrechts können diesem Amt selbstverständlich übertragen werden, sofern es nicht dadurch seine Funktion gefährdet.

Teil D

Informationsverarbeitung durch nicht-öffentliche Stellen

D. Informationsverarbeitung durch nicht-öffentliche Stellen

I. Grundsätzliches

1. Gang der Untersuchung

1.1. Zusammenfassung der bisherigen Ergebnisse

Die Ausführungen in den Teilen A bis C haben z. T. allgemeine Ergebnisse gebracht, die auch — zumindest als Prämissen — für den folgenden Teil D gelten. Sie sollen hier kurz vorangestellt werden:

— Die in Teil A, systematische Grundlegung, beschriebene potentielle Gefahr (automatisierter Informationsverarbeitung) stellt sich im Bereich der privaten Informationsverarbeitung genauso dar. Insoweit werden die dort gemachten Ausführungen im folgenden vorausgesetzt: Den ungeheueren positiven Möglichkeiten moderner Informationsverarbeitung steht eine gleichgroße potentielle Gefahr für den einzelnen wie für gesellschaftliche Minderheiten gegenüber.

— Diese umfassende Bedeutung der Informationsverarbeitung hat zur Folge, daß die obersten Kriterien für eine Regelung in der Verfassung gesucht werden müssen; nur sie ist weit genug, der gesamten Problematik Rechnung zu tragen.

In Teil C wurde das Selbstbestimmungsrecht über Individualinformationen im Begriff der allgemeinen Handlungsfreiheit angesiedelt. Diese Erkenntnis soll als grundlegend für die gesamte Datenschutzproblematik im folgenden Teil übernommen werden.

— Weiterhin werden wir auch die Topoi-Methode der Unterscheidung der einzelnen Phasen der Informationsverarbeitung beibehalten, was sich für eine effektive Regelung als unbedingt notwendig erwiesen hat; vgl. Teil B.

— Auch für die Phasen der Informationsverarbeitung gelten im folgenden prinzipiell die oben festgelegten Definitionen.

[1]) s. u. 2.
[2]) s. u. 3.
[3]) s. u. 4.
[4]) s. u. 5.

1.2. Weiteres Vorgehen

Die Darstellung der Probleme der Informationsverarbeitung durch nicht-öffentliche Stellen muß beginnen mit einer *Systematik* nicht-öffentlicher Informationssysteme, da die unterschiedlichen Typen auch unterschiedliche Probleme mit sich bringen können [1]).

Daran anschließend wird die derzeitige Rechtslage geschildert und kritisiert, sodann zusammenfassend die Regelungsbedürftigkeit dargetan [2]).

Kriterien für ein zu erstellendes Gesetz sind zunächst aus dem Grundgesetz zu entnehmen. Die Untersuchung an Hand zweier verschiedener Gedankengänge führt zur Formulierung konkreter Kriterien [3]).

Nach dem Ausscheiden der Informationssysteme zur Weitergabe an die Öffentlichkeit und der sonstigen internen Informationssysteme werden die speziellen Probleme der Informationssysteme zur Weitergabe an Private und der internen zweckgebundenen Informationssysteme erörtert [4]).

2. Regelungsmaterie (Prüfungsgegenstand)

2.1. Notwendigkeit einer Systematik

Die im folgenden angesprochenen privaten, d. h. nicht-öffentlichen Informationssysteme umfassen eine Vielzahl verschiedenster informationsverarbeitender Stellen. So fallen darunter unterschiedliche Typen wie Auskunfteien, Nachrichtendienste, Personalbüros, Dokumentationsunternehmen.

Dieser ganze Bereich kann nicht umfassend in einer einzigen Bestimmung geregelt werden. Die Unterschiede tatsächlicher Art, wie

— Art der verarbeiteten Informationen und

— Art der beteiligten Interessen,

machen es erforderlich, zunächst die einzelnen Typen in eine Systematik zu bringen. Diese Systematik muß es erlauben,

— sämtliche denkbaren Arten von Informationssystemen zu erfassen,

— und eine so feine Untergliederung zu erstellen, daß sie mit einheitlichen Regelungen faßbar sind. Sie setzt die Festlegung einiger einschlägiger Begriffe voraus.

2.2. Definition

vgl. Schaubild

2.2.1.

— *Informationsverarbeitung zur Weitergabe* (Weitergabe-IS) wird von Informationssystemen betrieben, die gewerblich zum Zwecke der Weitergabe an Dritte Informationen verarbeiten (z. B. Detekteien, Nachrichtenbüros, Dokumentationsunternehmen)

2.2.1.1.

a) *an die Öffentlichkeit*

betrifft vor allem Presseunternehmen und Massenmedien

2.2.1.2.

b) *an einzelne*

betrifft Unternehmen, die auf Wunsch Informationen an einzelne Dritte abgeben *(„gewerbliche IS/IV")*; z. B. Auskunfteien und Detekteien.

2.2.2.

— *Informationsverarbeitung zur internen Verwendung* (interne IS)

dient als Hilfsmittel zur Optimierung einer andersartig zweckbestimmten Tätigkeit, ohne als Hauptzweck Informationen an Dritte weitergeben zu wollen (z. B. Personalkarteien, Mitgliederkarteien, Arztkarteien, innerbetriebliche Forschungsinformationssysteme)

— *Zweckgebundene (interne) Informationsverarbeitung* findet statt zum Zwecke der Verwendung im Beruf, im Rahmen eines bestehenden Rechtsverhältnisses oder innerhalb einer Organisation *(„innerbetriebliche IS/IV")*; z. B. Personaldateien, Mitgliederkarteien und Arztakten.

2.3. Erläuterungen

— vgl. Schaubild

2.3.1. Erste Ebene

In der ersten Ebene zur Untergliederung wird eine Unterscheidung nach der *Zielsetzung* des Systems vorgenommen. Die grundsätzlichen Typen werden Weitergabe-Informationssysteme und interne Informationssysteme genannt.

2.3.1.1.

Weitergabe-Informationssysteme lassen sich durch folgende Gegebenheiten kennzeichnen:

— Das IS wird zum Zwecke der gewerblichen Verarbeitung von Informationen betrieben, welche an alle Dritte weitergegeben werden.

— Der Betroffene steht außerhalb dieses Vorgangs. Der Sammelnde besitzt überwiegend ein geschäftliches Interesse am Vorhandensein der Information und ist nicht an der Person des Betroffenen interessiert;

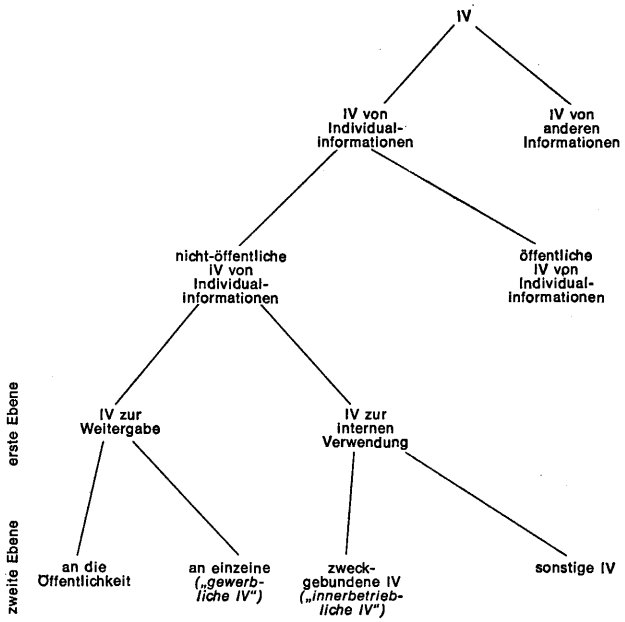
— d. h., Betroffener und Sammelnder stehen sich rechtlich unabhängig gegenüber; zwischen ihnen besteht kein tatsächlich oder rechtlich bestimmtes Kontaktverhältnis — wie etwa ein Arbeitsverhältnis.

— Die Auswirkungen der Informationsverarbeitung auf den Betroffenen entstehen mittelbar, nämlich erst dann, wenn die Informationen an den eigentlichen Empfänger weitergegeben werden.

2.3.1.2.

Interne Informationssysteme weisen dagegen andersartige Merkmale auf:

SCHAUBILD ZU 2. UND 3.



— Die Informationsverarbeitung stellt ein Hilfsmittel zur Optimierung andersartig zweckbestimmter Tätigkeit dar (etwa das Führen einer Personalkartei zwecks Gehaltsberechnung).

— Der Betroffene und der Sammelnde stehen zueinander in einem Verhältnis, welches die Grundlage für die Verarbeitung von Individualinformationen bildet und gleichzeitig einen Rahmen absteckt, innerhalb dessen sie stattfindet (z. B. Arbeitsverhältnis).

— Derjenige, der die Informationen sammelt, besitzt aufgrund dieses Rahmenverhältnisses ein direktes Interesse an der Person des Betroffenen. Dieser Umstand hat zur Folge, daß die Auswirkungen auf den Betroffenen unmittelbar eintreten.

— Die Weitergabe der Information gehört nicht zum unmittelbar verfolgten Verarbeitungsziel (wenn sie auch in der Realität gelegentlich durchaus üblich ist) [5]).

2.3.2. Zweite Ebene

Die Unterscheidungen auf der 2. Ebene knüpfen an die *Bedeutung* des Informationssystems an, hauptsächlich gemessen an den tatsächlichen sozialen Auswirkungen der Informationsverarbeitung.

2.3.2.1.

Die Weitergabe-Informationssysteme werden aufgrund der speziellen Stellung von Presse und Massenmedien unterteilt in:

Weitergabe-Informationssysteme an die Öffentlichkeit (Presse, Rundfunk, Fernsehen) und

Weitergabe-Informationssysteme an einzelne (Detekteien u. ä.)

2.3.2.2.

Bei den internen Informationssystemen unterscheiden wir *zweckgebundene und sonstige.*

Der Grund dafür ist die Tatsache, daß etwa ein privates Notizbuch oder eine Schlagwortkartei von Personalkarteien eines Betriebes u. ä. getrennt werden sollen. Ausschlaggebend waren die Gesichtspunkte der sozialen Bedeutung und des Vorliegens eines Kontaktverhältnisses.

3. Darstellung und Kritik der derzeitigen rechtlichen Situation

Zur Zeit gibt es in der Bundesrepublik Deutschland kein umfassendes Datenschutzgesetz, das den privaten Bereich erfaßt. Normen, die die „Information" unter dem Aspekt der sogenannten Privatsphäre regeln, finden sich recht verstreut in unterschiedlichen Gesetzen; das wird unter 3.1. ausgeführt. Daneben gibt es das von der Rechtsprechung entwickelte allgemeine Persönlichkeitsrecht; dazu unter 3.2.

Der Darstellung schließt sich jeweils eine Kritik an.

3.1. Verstreute einzelne Bestimmungen

3.1.1. Strafrecht und UWG

Für den Umgang mit Individualinformationen kommen folgende §§ in Betracht:

— § 268 StGB

Fälschung technischer Aufzeichnungen [6]); Beispiel: absichtlich entstellter bzw. unvollständiger Computerausdruck,

— § 274 StGB

Urkundenunterdrückung; Beispiel: Unbefugtes Löschen (Vernichten) von Individualinformation,

— § 168 StGB

Personenstandsfälschung,

— §§ 298, 299 StGB

Briefgeheimnis, Abhörverbot regelt Fälle unerlaubter Verschaffung von Informationen,

— § 300 StGB

Berufsgeheimnis; stellt die unbefugte Weitergabe fremder Geheimnisse durch bestimmte Personen unter Strafe,

— im UWG werden kredit- und wettbewerbsschädigender Umgang mit Informationen (auch Individualinformationen) zum Teil erfaßt: §§ 1, 12, 14 und 15.

Kritik:

Der Schutz der sog. Privatsphäre steht zumeist (außer §§ 298, 299, 300 StGB) nicht im Vordergrund. Individualinformationen werden nur zum Teil (etwa bezüglich des Kredits) gegen bestimmtes Verhalten geschützt (Fälschen, Vernichten).

3.1.2. Arbeitsrecht

Hier geht es darum, die sog. Privatsphäre des Arbeitnehmers gegenüber dem Arbeitgeber zu schützen.

Für die Beschaffung von Informationen über den Arbeitnehmer durch den Arbeitgeber gibt es keine besonderen Regelungen — hier spielt sich alles im Rahmen der Privatautonomie ab. Auf die bestehen-

[5]) vgl. Kamlah (1), 51
[6]) anwendbar bei Informationsverarbeitung durch Computer; str., vgl. Kienapfel, 163 ff.

den Personalakten und deren Führung hat der Arbeitnehmer keinen Einfluß und kein eigenes Einsichtsrecht [7]). Allenfalls kann der Betriebsrat im Rahmen seiner Aufgaben nach § 54 Abs. 1 BetrVerfG die Vorlage von Personalunterlagen und Einsicht in die Personalakten verlangen, § 54 Abs. 2 BetrVerfG.

Die Weitergabe von Informationen durch den Arbeitgeber wird in der Hinsicht geregelt, daß der Arbeitnehmer gemäß § 630 BGB ein Zeugnis verlangen kann. Darüber hinaus kann der Arbeitgeber an andere Arbeitgeber Auskünfte erteilen [8]). Diese Auskünfte müssen wahrheitsgemäß sein [9]). Nach einer umstrittenen Entscheidung des BGH [10]) muß der auskunftgebende Arbeitgeber seinem ausgeschiedenen Arbeitnehmer auf Verlangen die erteilte Auskunft mitteilen.

Kritik:

Ein gesetzlicher Schutz des Selbstbestimmungsrechts des Arbeitnehmers ist nicht ausreichend vorhanden. Die Beschaffung von Informationen steht dem Arbeitgeber wegen seiner sozialen Überlegenheit praktisch frei. Die Personalakten sind dem Einfluß des Arbeitnehmers fast gänzlich entzogen. Auf die Weitergabe von Informationen hat der Arbeitnehmer keinen Einfluß. Die — zudem umstrittene — Rechtsprechung läßt nur Maßnahmen *nach* der Weitergabe zu. Eine Verletzung der sog. „Privatsphäre" kann dadurch nicht verhindert werden.

3.1.3. Gewerberecht

Das Gewerberecht gibt zwar dem einzelnen Bürger keine direkten Rechte gegen einen Gewerbetreibenden (etwa: Auskunftei, Detektei). Doch kann es seine sog. „Privatsphäre" indirekt durch Regelungen des Geschäftsbetriebes und durch Aufsichtsmaßnahmen schützen. Diese Sicht gewerberechtlicher Normen ist neu.

Unter dem Aspekt „Schutz der Individualinformationen" kann man folgende Normen sehen:

— § 14 GewO

Anzeigepflicht [11]),

— § 33 d Nr. 3, § 34 a Abs. 1 Nr. 1, § 34 b Abs. 1 Nr. 1, §§ 35, 57 GewO

Zuverlässigkeit (nicht jedermann darf Individualinformationen gewerbsmäßig verarbeiten),

— § 4 VO

über das Bewachungsgewerbe (Verschweigenspflicht des Gewerbetreibenden bezüglich der ihnen bekanntgewordenen Individualinformationen).

Eine Kritik dieser Normen erscheint unangebracht, da das Gewerberecht bislang nicht als Mittel zum Schutz der sog. „Privatsphäre" gesehen wurde. Seine Maßnahmen sind daher nur als Ansätze zu betrachten.

3.1.4. Bank- und Versicherungsrecht

Hier verhält es sich ähnlich wie im Gewerberecht. Die Banken- und Versicherungsaufsicht wäre generell geeignet, Individualinformationen des einzelnen indirekt zu schützen. Nach § 81 Abs. 2 Nr. 1 VAG kann z. B. die Aufsichtsbehörde Anordnungen treffen, die geeignet sind, „Mißstände zu beseitigen, welche die Belange der Versicherten gefährden".

Banken- und Versicherungsaufsicht dient aber wie die Gewerbeaufsicht in erster Linie öffentlichen und wirtschaftlichen Interessen der Gesamtheit (Allgemeinheit), nicht so sehr dem Schutz des einzelnen Bürgers. In der Praxis ist man sich der Problematik wohl bewußt, wie uns ein privater Brief des Versicherungsaufsichtsamtes bewies.

Für das Kreditwesen sieht die Aufsichtsbehörde jedoch bislang keine Möglichkeiten zu Maßnahmen. Das ging ebenfalls aus einem privaten Brief hervor.

Das *Bankgeheimnis* ist gesetzlich nicht normiert, sondern lediglich Inhalt der vertraglichen oder vorvertraglichen Beziehungen zwischen Bank und Kunden. Wegen der sozialen Macht der Kreditinstitute ist das Bankgeheimnis jedoch nicht als ausreichender Schutz anzusehen. Die Reichweite dieser Abmachung liegt in der Hand der Kreditinstitute. Wie beim Gewerberecht erscheint eine eingehendere Kritik als im Text auch hier nicht angebracht.

3.2. Das allgemeine Persönlichkeitsrecht

Das BGB enthält dem Wortlaut nach keine Norm, aufgrund derer sich der Bürger auf zivilrechtlichem Wege gegen Beeinträchtigungen seiner sog. „Privatsphäre" wehren könnte.

Mit der Einführung eines „allgemeinen Persönlichkeitsrechts" in den Katalog der „sonstigen Rechte" in § 823 Abs. 1 BGB hat der BGH [12]) eine Entwicklung eingeleitet, die in zunehmendem Maße auch die Berücksichtigung der sog. „Privatsphäre" ermöglichte. Das „allgemeine Persönlichkeitsrecht" wurde jedoch — im Hinblick auf die Herleitung aus der allgemeinen Handlungsfreiheit des Artikels 2 Abs. 1 GG — unter dem Blickwinkel der Durchsetzung eigener Interessen [13]) oder der „freien und eigenverantwortlichen Selbstbestimmung" [14]) gesehen.

---

[7]) *anders die zur Debatte stehende Neufassung des BetrVerfG: Bundesratsdrucksache Nr. 715/70 §§ 81 bis 84*
[8]) BAG AP KA § 630 Nr. 1
[9]) BAG, a. a. O.
[10]) NJW 59, 2011
[11]) vgl. IPA-Entwurf, § 1, 2
[12]) seit E 13, 334
[13]) BGHZ 24, 79
[14]) OLG Hamburg NJW 67, 2316

Es wurde nicht in Zusammenhang gebracht mit dem Begriff der Information über die Persönlichkeit.

Eine Analyse der Entscheidungen zeigt jedoch, daß es beim allgemeinen Persönlichkeitsrecht stets um Informationen über die Person des Betroffenen geht. Dies verdeutlicht das Problem einiger einschlägiger Entscheidungen: Inhalt eines Privatbriefes [15]), ärztliche Aufzeichnungen über den Gesundheitszustand [16]), heimliche Tonbandaufnahmen [17]), die Überwachung eines Ehepartners durch einen heimlich in die Wohnung eingeführten Dritten [18]), die Veröffentlichung von Scheidungsabsichten [19]). Diese Probleme lassen sich meist mit dem Begriff „Indiskretion" umschreiben [20]). In all diesen Fällen ist der Umgang mit Informationen, also die Informationsverarbeitung, Kern des Problems. Das bedeutet, daß Verletzungen eines Persönlichkeitsrechts durch Informationsverarbeitung zivilrechtlich vom allgemeinen Persönlichkeitsrecht erfaßt werden. Der Betroffene wird durch § 823 Abs. 1 BGB geschützt. Im folgenden soll nun untersucht werden, wie weit dieser Schutz reicht.

Während sich die Rechtsprechung zunächst noch mit einer allgemeinen Umschreibung des Persönlichkeitsrechts begnügte, taucht in BGH 24, 72 (79) der Begriff der „persönlichkeitsrechtlich geschützten Geheimsphäre" auf. Die Rechtsprechung entwickelte in der Folge nach Hubmann [21]), die sog. „Sphärentheorie" [22]), die vom Oberlandesgericht Hamburg [23]) dargelegt wird: Der Persönlichkeitsbereich wird aufgeteilt in Individualsphäre, Privatsphäre und Intimsphäre. Die Individualsphäre „bewahrt die persönliche Eigenart des Menschen in seinen Beziehungen zur Umwelt" [24]), die Privatsphäre umfaßt das Familienleben und das sonstige Privatleben im häuslichen Kreise [25]), die Intim- oder Geheimsphäre ist die „innere Gedanken- und Gefühlswelt mit ihren äußeren Erscheinungsformen" [26]).

Während öffentliche Darstellungen und wohl auch die Weitergabe von Informationen aus dem Intimbereich gänzlich untersagt sind [27]), dürfen Informationen aus der Privatsphäre nicht ohne zwingenden Grund weitergegeben werden [28]). Die Tatbestände solch zwingender Gründe wurden allerdings recht weit gezogen.

Dogmatisch zeichnet sich das Persönlichkeitsrecht dadurch aus, daß es nur als sog. „Rahmenrecht" [29]) bzw. „partielle Generalklausel" [30]) angesehen wird. D. h. im Gegensatz zu den anderen absoluten Rechten wird hier die Rechtswidrigkeit nicht indiziert [31]), sie muß erst vom Betroffenen dargetan werden. Rechtswidrig ist erst eine Verletzung des Persönlichkeitsrechts, wenn eine Interessenabwägung zuungunsten des Eingreifenden ausfällt [32]).

Die Rechtsfolgen sind die des § 823 BGB: Schadenersatzansprüche für materiellen Schaden, nach der Rechtsprechung auch für immateriellen Schaden [33]), in besonders schweren Fällen (allerdings nur dann, wenn dem Verletzten nur hierdurch Genugtuung zuteil werden kann; bisher nur zugestanden bei schweren Ehrkränkungen [34]), oder erdichteten Zeitungsberichten [35]); in Rechtsanalogie zu §§ 12, 862, 1004 BGB [36]) ein Unterlassungs- und Beseitigungsanspruch, vorbeugend jedoch nur, wenn schon einmal eine Verletzung stattfand. Hubmann [37]) erwägt außerdem noch Bereicherungs- und Aufopferungsansprüche, die sich jedoch auf sehr eng begrenzte Ausnahmefälle beziehen.

Damit läßt sich kritisch zusammenfassen:

Die sog. Privatsphäre wird zivilrechtlich im Wortlaut des BGB überhaupt nicht, von der Rechtsprechung über die Geltendmachung des sog. Persönlichkeitsrechts erfaßt. Obwohl in der Rechtsprechung vom Begriff „Informationen" nicht die Rede ist, betreffen die Entscheidungen ausschließlich die Ermittlung (Überwachung des Ehepartners) und Weitergabe (die übrigen angeführten Fälle) von Informationen über Personen.

Die Rechtsprechung knüpft bei der Auswahl von Kriterien an die Sphärentheorie an. Deren Unbrauchbarkeit, und damit die prinzipielle Unbrauchbarkeit eines Begriffes wie der sog. „Privatsphäre", wurde oben [38]) bereits dargetan. Erwünscht wäre trotz der Zurückhaltung der Rechtsprechung ein Schutz aller Individualinformationen, also der Informationen über alle drei von der Rechtsprechung eingegrenzten „Sphären", in einem noch näher zu bestimmenden Rahmen. Einen solchen umfassenden Schutz kann aber der bereits festgelegte Begriff des „Persönlichkeitsrechts" allein nicht mehr leisten.

Zudem wird ein Rechtsschutz bei einer angeblichen Verletzung des Persönlichkeitsrechts nur unter erschwerten Umständen gewährt. Ein vorbeugender Unterlassungsanspruch ist, solange kein Verstoß vorliegt, überhaupt nicht möglich. Die Rechtswidrigkeit muß vom Betroffenen gesondert dargetan werden, die Beweislage ist damit äußerst ungünstig. Ein immaterieller Schadensersatz ist auf ganz wenige, besonders schwere Fälle beschränkt und obendrein in der Literatur heftig umstritten. Den Betroffenen trifft zudem die Last des Prozeßkostenvorschusses.

Eine Lösung läßt sich somit erst erreichen, wenn ein Schutzgesetz die Rechtsfolgen des § 823 BGB unmit-

---

[15]) BGHZ 13, 334
[16]) BGHZ 24, 72
[17]) BGHZ 33, 20
[18]) BGH NJW 70, 1848
[19]) OLG Hamburg NJW 70, 1325
[20]) vgl. dazu Hubmann (2), 521 ff.
[21]) (1), 217 ff.
[22]) Seidel, 1581
[23]) OLG Hamburg NJW 67, 2314
[24]) ebd.
[25]) ebd.
[26]) ebd.
[27]) ebd.
[28]) BGH NJW 65, 685
[29]) Fikentscher, § 103 II
[30]) Esser, 58
[31]) Fikentscher, ebd.
[32]) siehe dazu BGHZ 24, 72
[33]) BGHZ 26, 349; 39, 124; BGH NJW 65, 685
[34]) BGH NJW 65, 2595
[35]) BGH NJW 65, 685
[36]) BGH 38, 206
[37]) S. 349 ff., insbesondere 363 ff.
[38]) B. I.

telbar gewährt, und wenn die dort vorgesehenen Rechte ergänzt werden.

3.3. Regelungsbedürftigkeit

Nach dieser Einzelanalyse läßt sich die Regelungsbedürftigkeit der Materie einfach dartun:

Der Bereich der Individualinformationen ist überhaupt nicht geschlossen geregelt; dort wo er geregelt ist, ist er auf die herkömmliche Struktur der Informationsverarbeitung angelegt, deren Gefahren bei weitem nicht die Gefahren einer Informationsverarbeitung mit Hilfe von EDVAn erreichen [39]). Auf der anderen Seite erfordert der Schutz des Individuums vor diesen Gefahren einen solchen umfassenden Schutz.

Der Umfang der Regelung muß sich teilweise auch auf schon bestehende Bestimmungen beziehen, da diese völlig unzureichend [40]) und zudem nicht EDV-gerecht sind. Das bedeutet ein Ineinandergreifen einer umfassenden, geschlossenen Regelung und der Neufassung bereits bestehender verstreuter Vorschriften.

4. Regelungskriterien aus dem Grundgesetz

Die Erstellung eines neuen Gesetzes, das die Materie in wünschenswertem Umfang neu regelt, setzt eine Untersuchung voraus, welche Kriterien das Grundgesetz für diese Regelung zur Verfügung stellt. Die Berücksichtigung dieser Kriterien geschieht einerseits, um verfassungswidrige Bestandteile des Gesetzes zu vermeiden, andererseits, um das Gesetz in die Zielvorstellungen der bundesdeutschen Verfassung zu betten.

Es werden zwei Gedankengänge angestellt, von denen *der erste* von einem modernen Verfassungsverständnis ausgeht, das nicht mehr nur starr das Verhältnis Staat—Bürger, sondern allgemein die tatsächlichen Gewaltverhältnisse im Staatsbereich im Auge hat. Das führt dazu, den sog. *„sozialen Gewalten"* ähnliche Beschränkungen aufzuerlegen, wie sie auch der Staat hat, 4.1.

Der zweite Gedankengang knüpft an die mehr liberalistische Deutung des GG an und zeigt, daß auch die „sozialen Gewalten" Grundrechtsträger sind, so daß auf diesem Wege eine Interessenabwägung notwendig wird, bei der die Gewaltverhältnisse ebenfalls zu berücksichtigen sind, 4.2.

Die Synthese dieser Gedankengänge ergibt den Rahmen, innerhalb dessen sich das zu erstellende Gesetz aufzuhalten hat. Die dabei aufgestellten Grundsätze können dann als Ausgangspunkt für die konkrete Gesetzesgestaltung gewählt werden, 4.3.

4.1. Verhältnis Informationssystem — Bürger

4.1.1. Informationssystem als soziale Gewalt

Die Entwicklung dieses Begriffes begann zur Weimarer Zeit, als zum ersten Mal der Ausdruck „soziale Gewalt" geprägt wurde [41]).

Das geschah im Zusammenhang mit der Diskussion über den Grundrechtsschutz des wirtschaftlich Schwachen gegenüber seinem privaten Rechtsgenossen [42]).

Diese Problematik ist im Verhältnis einzelner zu gesellschaftlichen Gruppen und (Interessen-)Verbänden offensichtlich [43]) und wird häufig auch nur so gesehen [44]). Doch auch die schwache Position einzelner gegenüber wirtschaftlich Starken wird heute weitgehend als schutzwürdig anerkannt [45]).

Der Träger sozialer Macht steht zum Untergeordneten in einem Verhältnis, aus dem jener nicht beliebig ausbrechen kann und das sich auf seine Situation lebensgestaltend auswirkt [46]). Ein derartiges *Kontaktverhältnis besteht* zwischen dem Informationssammler und dem Betroffenen *in der Regel* außer bei innerbetrieblichen IS nicht.

In einem IS steht jedoch ein Personenmodell zur Verfügung, das je nach technischen und informationellen Gegebenheiten eine sehr weitgehende Transparenz der Person herbeiführen kann. Die Aktualität und Geschwindigkeit moderner Informationsverarbeitung erlauben eine umfassende und beliebige Verarbeitung der Individualinformationen — und damit der Person. Daraus folgt, daß ein Informationssystem sehr wohl Macht bereitstellt; ihm ist es freigestellt, zu welchem Zweck und in welchem Umfang eine Person durch ihr gespeichertes Modell „verarbeitet" wird. Die möglichen Auswirkungen sind ebenso gefährlich wie das Ausgeliefertsein des Individuums an einen sozial Mächtigeren. Diese Tatsache bewirkt eine akute Gefährdung der individuellen Rechtssphäre, indem Eingriffsmöglichkeiten in elementarste Rechte geschaffen und bereitgestellt werden: Menschenwürde, freie Entfaltung der Persönlichkeit, Handlungsfreiheit, Selbstbestimmung.

IS müssen insofern als soziale Machtfelder 1. Ranges bezeichnet werden.

4.1.2. Bindung an die Grundrechte

Der Problemkreis „soziale Gewalt" wird im Hinblick auf die Bindung dieser Gewalten an die Grundrechte erörtert [47]). Der einzelne Bürger wird durch die Grundrechte gegen Beeinträchtigungen seiner Rechtssphäre durch die Staatsgewalt geschützt. Bedrohungen durch andere, sozial mächtige Bürger werden jedoch nur — sofern man liberalistischen Anschauungen folgt — in dem Rahmen des Privatrechts geregelt. In einem Rechtsbereich also, der für den unter Privaten, von ebenbürtigen Partnern ausgehenden Rechtsverkehr bestimmt ist.

---

[39]) Simitis (2), 675
[40]) vgl. die Ausführungen zum Arbeitsrecht
[41]) Leisner, 230 FN 20
[42]) ebd.
[43]) v. Mangoldt - Klein, Vorbem. A. II. 4. c, S. 63
[44]) Maunz - Dürig - Herzog, Artikel 21 N. 25; Loewenstein (1), 16, 367 ff.
[45]) Nawiasky, in: Nawiasky - Leusser, Vorbem. vor Artikel 98, S. 178; v. Mangoldt - Klein, Vorbem. A. II. 4. c, S. 64; Leisner, 253; BAGE 1, 194
[46]) Leisner, a. a. O.
[47]) Hesse (2), 149; Stein, 224; Leisner, 252, 293; Nipperdey (2), 19, 23

Die Bindung des Staates an die Grundrechte ist nun gerade darin begründet, daß der Staat als Träger überlegener Sozialmacht [48]) in einem sozialen Überordnungsverhältnis zum Bürger steht. Wenn die soziale Übermacht von einem Privaten ausgeht und „sich das Unterlegenheitsverhältnis dem Unterlegenheitsverhältnis gegenüber der Staatsgewalt nähert", so führt Müller [49]) aus, „da drängt die innere tatsächliche Natur der in Frage stehenden sozialen Beziehung eine Reaktion des Grundrechtsschutzes auf".

Die Bindung Privater (sozialer Gewalten) an Grundrechte, die in dieser gesellschaftlichen Problematik angelegt ist, wird gemeinhin als „Drittwirkung" bezeichnet. Demgegenüber ist festzuhalten, daß die Problematik der Drittwirkung nur bei der Rechtsanwendung akut wird [50]). Hier sollen jedoch Kriterien für den Gesetzgeber erarbeitet werden. Die Bindung des privaten Machtträgers an grundrechtliche Wertungen im Rahmen der Rechtsentstehung erfolgt dagegen über ein Gesetz. Hierbei ist nicht gleichgültig, von welchem Grundrechtsverständnis das Grundgesetz ausgeht.

Die aus dem 19. Jhd. stammende liberalistische Sicht der Grundrechte versteht die Grundrechte lediglich als subjektive öffentliche Rechte gegenüber dem Staat, die entweder einen status negativus, activus oder positivus gewährleisten [51]).

Zwar ist dieser Aspekt nicht generell abzulehnen [52]), doch vermag er allein das Wesen der Grundrechte nicht völlig zu erfassen [53]). Vielmehr hat sich die Bedeutung der Grundrechte dahin gehend gewandelt, daß sie nicht nur das Individuum gegen den Staat sichern, sondern Grundlage jeder menschlichen Gesellschaft (Artikel 1 Abs. 2 GG) sind [54]). Sie gewährleisten ein bestimmtes, wertbezogenes Ordnungsgefüge [55]), sie sind Grundelemente objektiver Ordnung des Gemeinwesens [56]), objektive Normen für die gesamte Rechtsordnung [57]).

Dieses Grundrechtverständnis bedeutet für den Gesetzgeber, daß die Ausübung sozialer Gewalt auch dann an die Grundrechte gebunden ist, wenn sie durch Private geschieht [58]). Die Wirkung der Grundrechte ist nicht zweiseitig (Verhältnis zum Staat), sondern allseitig [59]), auch auf Private angelegt. Diese Auffassung soll den folgenden Ausführungen zugrunde gelegt werden.

[48]) Stein, 223
[49]) S. 161
[50]) Leisner, 316 f.; wohl auch Hubmann (2), 111
[51]) Jellinek, 94 ff.
[52]) Stein, 220; Nipperdey (2), 23
[53]) Stein, a. a. O.; Nipperdey (2), a. a. O.; Müller, 163 ff.
[54]) Stein, 221
[55]) Müller, a. a. O.
[56]) Hesse (2), 11
[57]) Nipperdey (2), a. a. O.; Leibholz - Rinck, vor Artikel 1 bis 19 Anm. 2; ständige Rspr. des Bundesverfassungsgerichts, vgl. E 21, 372
[58]) Stein, 224; Hesse (2), 149
[59]) Müller, 163
[60]) Hesse (2), 147
[61]) ebd.
[62]) vgl. dazu die Ausführungen bei Kamlah (1), 27
[63]) Simitis (2), 674

4.1.3. Spezielle Grundrechte

Nachdem festgestellt ist, daß die dem Grundgesetz zugrunde liegenden Wertungen dahin gehen, auch private Gewalten ähnlichen Beschränkungen zu unterwerfen wie den Staat, sind die einzelnen Bestimmungen des Grundgesetzes nun auf ihre Relevanz für den Bereich der privaten Informationssysteme durchzuprüfen.

Im Anschluß an Teil C des Gutachtens können wir uns hier an die oben angeführte Auswahl spezieller Grundrechte halten. Auch hier ist darauf hinzuweisen, daß diese speziellen Grundrechte keine Abgrenzung eines Bereiches der Privatsphäre ermöglichen. Sie stellen vielmehr nur punktuell einige Bereiche des „Faktors Information" heraus, die aus historischen Gründen einen besonderen Schutz erfahren haben.

Mit Teil C läßt sich damit auch für die private Informationssysteme feststellen:

Das grundsätzliche Verbot, Informationen über die religiöse Überzeugung zu ermitteln, muß auch für Private gelten. Rechte und Pflichten können im Bereich des Privaten nur gegenüber den Religionsgemeinschaften bestehen. Insofern wäre also auch hier eine Ausnahme vom generellen Verbot zu machen; Artikel 4 GG i. V. m. Artikel 136 WRV.

4.1.3.1.

Fraglich ist, ob dieses generelle Verbot sich auch auf die politische Überzeugung erstreckt. Es ist anerkannt, daß *Artikel 4* ein „Grundelement objektiver demokratischer und rechtsstaatlicher Ordnung" [60]) darstellt, und damit eine „Voraussetzung eines freien politischen Prozesses" [61]) ist. Auch die Erwähnung des „weltanschaulichen Prozesses" in Artikel 4 Abs. 1 deutet, ausgelegt im Lichte des institutionalisierten Schutzes politischer Überzeugung durch Artikel 9, darauf hin, daß die Intention des Grundgesetzes dahin geht, auch die Freiheit der politischen Überzeugung zu garantieren. Die Gefahr, die der Freiheit der politischen Überzeugung potentiell von privaten Informationssystemen droht, kann nicht unterschätzt werden, wie amerikanische Beispiele zeigen [62]).

Wenn damit private Informationssysteme den Grundrechtsbindungen unterworfen werden sollen, erscheint ein entsprechendes Verbot der Verarbeitung religiöser und politischer Individualinformationen angebracht. Auch hier ergibt sich aus der Zweckbestimmung von Artikel 4 eine Ausnahme für die Informationssysteme, die auf entsprechende Informationen angewiesen sind. Das wären hier die Informationssysteme, die von politischen Parteien unterhalten werden (falls solche überhaupt neben einem parlamentarischen Informationssystem für sinnvoll erachtet werden).

Hier zeigt sich wieder die Verflechtung von Individualdatenschutz und Kollektivdatenschutz: Die — mit einigem Mißtrauen zu betrachtenden — eventuellen künftigen Partei-Informationssysteme erübrigen sich (und sind zu verbieten) dann, wenn das „Informationsgleichgewicht" [63]) zwischen Legislative und Exekutive auch bezüglich der IS der Re-

gierung/Verwaltung und des Parlaments gewahrt ist. Dann kann die Regierungspartei sowohl auf das parlamentarische wie das Exekutivsystem zugreifen, die oppositionellen Parteien haben wenigstens die Möglichkeiten des parlamentarischen Informationssystems. Außerhalb des Parlaments stehenden Parteien Informationssysteme zu gewähren, erscheint bedenklich. Im Hinblick auf den Gleichheitssatz sind u. U. die Grundsätze des Parteienfinanzierungsgesetzes beizuziehen.

4.1.3.2.

Artikel 8 will die Kommunikation gewährleisten, die Voraussetzung von Meinungsbildung oder Vorformung des politischen Willens ist [64]). Eine solche Kommunikation vollzieht sich zu einem wesentlichen Teil in Versammlungen [65]). Informationen über die Teilnahme an Versammlungen gefährden diesen Prozeß. Daher muß die Verarbeitung auch dieser Informationen beschränkt werden. Für sie gilt also das gleiche wie zu 4.1.3.1.

4.1.3.3.

Artikel 10 schließlich verbürgt einen „wesentlichen Bestandteil der Unverletzlichkeit der Privatsphäre" [66]). Es wäre zu untersuchen, ob nicht das gegen den Staat gerichtete Verbot der Verletzung des *Brief- und Fernmeldegeheimnisses* auch auf private Informationssysteme insoweit Anwendung zu finden hätte, als zumindest der Inhalt nichtveröffentlichter Briefe und Ferngespräche nicht in ein Informationssystem aufgenommen werden darf. Für das nicht-öffentlich gesprochene Wort versieht allerdings bereits § 298 StGB die Aufnahme und Weitergabe mit einer Strafdrohung, und damit mit einem generellen Verbot.

4.1.4. Artikel 2 Abs. 1 GG

Entsprechend dem Vorgehen in Teil C ist nun nach den nur einzelne Aspekte berücksichtigenden speziellen Grundrechten das „Quellgrundrecht" des Artikels 2 Abs. 1 in Erwägung zu ziehen. Auch hier schließen wir uns der herrschenden Meinung an, die Artikel 2 Abs. 1 als die Gewährleistung der allgemeinen Handlungsfreiheit interpretiert [67]).

Ebenfalls entsprechend den oben ausgeführten Gedankengängen muß weiterführend festgestellt werden, daß die allgemeine Handlungsfreiheit das Verfügungs- und damit das Zurückbehaltungsrecht bezüglich aller Individualinformationen umfaßt, also als „informationelles Selbstbestimmungsrecht" zu verstehen ist.

[64]) Hesse (2), 154
[65]) ebd.
[66]) Hesse (2), 146
[67]) vgl. Maunz - Dürig - Herzog, Artikel 2 Abs. 1 N. 11
[68]) Maunz - Dürig - Herzog, Artikel 2 Abs. 1 N. 12
[69]) vgl. v. Mangoldt - Klein, Artikel 2 Anm. IV 3
[70]) Artikel 2 Anm. 11
[71]) Hamann - Lenz, Artikel 2 Anm. B. 5; vgl. auch v. Mangoldt - Klein, Artikel 2 Anm. IV 1 a; Maunz - Dürig - Herzog, Artikel 2 Abs. 1 N. 13
[72]) Maunz - Dürig - Herzog, Artikel 2 Abs. 1 N. 13
[73]) Maunz - Dürig - Herzog, Artikel 2 Abs. 1 N. 36
[74]) s. o. Teil C
[75]) Palandt - Degenhardt, § 903 BGB Anm. 2 b

Das bedeutet für das in diesem Gedankengang angesprochene Grundrechtsverständnis, daß Artikel 2 Abs. 1 nicht-öffentlichen Informationssystemen in der gleichen Weise die Verarbeitung von Individualinformationen verbietet wie dem Staat. Dieses grundsätzliche Verbot ist allerdings auch hier durch die Schrankentrias einzuschränken. Da wir soziale Gewalten bezüglich der Grundrechtsbindung dem Staat gleichgestellt hatten, muß es auch den sozialen Gewalten rechtspolitisch zugebilligt werden, aus den Schranken der Grundrechte Berechtigungen herzuleiten.

4.1.5. Ausnahmen aus den Schranken von Artikel 2 Abs. 1

Die allgemeine Handlungsfreiheit des Bürgers aus Artikel 2 Abs. 1 GG findet ihre Grenzen an der sog. „Schrankentrias" der Rechte anderer, des Sittengesetzes und der verfassungsmäßigen Ordnung. Überträgt man, wie hier geschehen, die Bindungswirkung der Grundrechte auch auf soziale Gewalten, so sind die Schranken beim grundsätzlichen Verbot eines Eingriffs in die allgemeine Handlungsfreiheit als *Berechtigungen, dies ausnahmsweise dennoch zu tun,* zu verstehen; so wie sich für den Staat aus den Schranken Artikel 2 Abs. 1 ein für die Zukunft ermächtigender Gesetzesvorbehalt ergibt [68]).

4.1.5.1.

Zunächst scheidet an dieser Stelle *das Sittengesetz* aus. Diese Schranke ist schlecht faßbar [69]). Man kann wie Leibholz-Rinck [70]) darunter den Bereich des Geschlechtlichen, der Intimsphäre verstehen. Insoweit gewährt das Sittengesetz aber kein Eingriffsrecht, sondern ein Recht auf Achtung dieser Sphäre. Das Sittengesetz hat somit passiven Charakter. Es schränkt die Handlungsfreiheit ein, ohne jemandem ein Eingriffsrecht für den Fall des Verstoßes zu gewähren.

4.1.5.2.

Anders dagegen die Schranke der *„Rechte anderer"*. Darunter sind subjektive (öffentliche und private Rechte einzelner (nicht der Allgemeinheit oder des Staates) zu verstehen, die einwandfrei verfassungsrechtlich fundiert sind [71]). Diese Bedeutung entspricht somit der Bedeutung von „Rechte Dritter" in § 903 BGB [72]).

Soweit Menschenrechte betroffen sind, gilt das Prinzip der Unverzichtbarkeit von Grundrechten [73]). Hier handelt es sich jedoch um Kriterien zur Ausgestaltung des Privatrechts, die aus Artikel 2 GG gewonnen werden sollen. Vorgenommen werden soll eine Konkretisierung von Artikel 2 GG im Privatrecht. Damit müssen auch privatrechtliche Grundsätze zugrunde gelegt werden [74]).

Auf privatrechtlichem Gebiet kann man sich der „Rechte einzelner" durch Zustimmung grundsätzlich begeben [75]). Dieser Grundsatz ist zu übernehmen, wenn aus Artikel 2 Kriterien für privatrechtliche Regelungen gewonnen werden sollen. Die Entäußerung von Rechten darf jedoch nicht dazu führen, daß sich der einzelne sämtlicher Rechte begibt. Dieser Grundrechtsgedanke findet sich im Privatrecht in §§ 134, 138 wieder; denn die Wertungen des Grund-

gesetzes sind als Maßstab der gesamten Rechtsordnung immanent [76]). So, wie der Staat den Kerngehalt der Grundrechte nicht berühren darf, kann auf Rechte unter Privaten nicht in unbegrenztem Maße verzichtet werden. Wenn sich der Private seiner elementarsten Rechte (Kern der Grundrechte) begibt, kann eine Zustimmung nach §§ 134, 138 nichtig sein [77]).

Damit kann zusammenfassend gesagt werden:

Eine Einschränkung des freien Selbstbestimmungsrechts über Individualinformationen durch einen Privaten liegt dann nicht vor, wenn der Betroffene zugestimmt hat. Die Zustimmung unterfällt den Rechten anderer; in Artikel 2 Abs. 1 GG. Begrenzt wird die Zustimmung dadurch, daß der Kernbereich des Artikels 2 Abs. 1 GG nicht berührt werden darf.

Daß Artikel 2 Abs. 1 GG außer der durch die Schrankentrias eingeschränkten allgemeinen Handlungsfreiheit auch einen solchen Kern gewährleistet, wird seit neuem auch von der Rspr. anerkannt [78]).

4.1.5.3.

Rechte anderer können aber auch durch die Rechtsordnung in beliebiger Anzahl neu begründet werden. Insoweit überschneidet sich die Schranke der Rechte anderer mit der Schranke der *verfassungsmäßigen Ordnung* [79]).

Da die Erörterungen Kriterien für den Gesetzgeber geben sollen, kommen an dieser Stelle als Untersuchungsgegenstand innerhalb der verfassungsmäßigen Ordnung nur *Normen von Verfassungsrang* in Betracht. Einfache Gesetze können nach dem Grundsatz lex posterior derogat legi priori aufgehoben werden. Normen, die Rechte gegen einzelne gewähren, können im Grundgesetz *nur innerhalb der Grundrechte* auftreten.

Es stellt sich nun die Frage, ob die Informationssysteme im Rahmen der verfassungsmäßigen Ordnung als Rechtfertigung für Eingriffe gegen den Bürger Grundrechte geltend machen können. Informationssysteme sind soziale Gewalten und werden als solche in ihrem Verhältnis zum Bürger grundsätzlich dem Staat gleichgestellt. Unbestrittenermaßen kann der Staat sich dem Bürger gegenüber nicht auf Grundrechte berufen [80]). Das bedeutet aber, daß auch Informationssysteme als soziale Gewalten grundsätzlich *keine Grundrechte gegenüber dem Bürger* geltend machen können.

Die *Konsequenz* dieses Ansatzes ist, daß die allgemeine Handlungsfreiheit des Bürgers als „informationelles Selbstbestimmungsrecht" gegenüber privaten Informationssystemen als sozialen Gewalten grundsätzlich keinen Beschränkungen unterliegt, da die Schranken des Artikels 2 Abs. 1 dem Informationssystem keine Rechte gegen den Bürger gewähren.

[76]) BVerfGE 7, 158 (205); 10, 302 (322); BGHZ 33, 145 (149); 38, 317 (319 ff.)
[77]) Palandt - Danckelmann/Heinrichs, § 138 Anm. 2 a
[78]) BVerfG NJW 70, 555
[79]) vgl. dazu auch v. Mangoldt - Klein, Artikel 2 N. IV 1 b
[80]) vgl. statt aller Maunz, § 14 Abs. 2 11
[81]) Maunz - Dürig - Herzog, Artikel 5 N. 16, 17

4.2. Grundrechtsschutz des Informationssystems? — Informationssystem und Staat

Der soeben vorgestellte Gedankengang geht von der Hypothese aus, daß auf Grund der realen Gewaltverhältnisse nicht-öffentliche Informationssysteme ähnlichen Beschränkungen zu unterwerfen sind wie der Staat bzw. die öffentlichen Informationssysteme. Dabei fand zunächst keine Berücksichtigung, daß der „Inhaber" eines nicht-öffentlichen Informationssystems selbst Privatmann ist und damit für sich gegenüber staatlichen Beschränkungen die Grundrechte geltend machen kann. Dieser Schutz kann keinem Privaten versagt werden, auch wenn man seine Machtbefugnisse zum Anlaß nimmt, ihn als „soziale Gewalt" Grundrechtsbindungen zu unterwerfen.

Im folgenden soll untersucht werden, welche Grundrechte der Inhaber eines Informationssystems geltend machen kann.

4.2.1. Spezielle Grundrechte

An speziellen Grundrechten kommen Artikel 5, 12 und 14 in Frage.

4.2.1.1. Artikel 5

Die diesbezügliche Problematik von Artikel 5 läßt sich in einer Frage zusammenfassen:

Inwieweit können sich Träger privater Informationssysteme auf Artikel 5 GG berufen, d. h., sich aus allgemein zugänglichen Quellen informieren?

a) Artikel 5 Abs. 1 GG gewährt *jedermann* das Recht, seine Meinung in Wort, Bild, Schrift frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Träger dieses Grundrechts („jedermann") kann jede natürliche und juristische Person sein, soweit sie sich im Anwendungsbereich des GG und damit der Staatsgewalt der Bundesrepublik Deutschland befindet [81]). Artikel 5 GG ist somit auf Träger privater Informationssysteme anwendbar, soweit es sich um natürliche oder juristische inländische Personen handelt.

b) Artikel 5 Abs. 1 schützt die Freiheit der geistigen Kommunikation zwischen den einzelnen Individuen. Geschützt wird nicht nur die Freiheit der Meinungsäußerung, sondern als deren Voraussetzung auch die Freiheit der Meinungsbildung. Unter der „Informationsfreiheit" versteht man das im Artikel 5 Abs. 1 S. 1, 3. Var. geschützte Recht, sich aus „allgemein zugänglichen Quellen" ungehindert zu unterrichten, als Voraussetzung der Meinungsäußerung.

   Da „Meinungen" nicht nur Urteile oder Stellungnahmen wertenden Inhalts sind, sondern auch schon bloße Tatsachenmitteilungen — denn jede bloße Tatsachenmitteilung enthält notwendig eine Stellungnahme zu den Informationsquellen und das wertende Urteil, daß sich die Tatsachen so und nicht anders verhalten, und ist somit nicht wertungsfrei —, ist für die *Ermittlungstätigkeit* privater IS Artikel 5 Abs. 1 S. 1, 3. Var. GG einschlägig.

c) Nach Artikel 5 Abs. 1 S. 1 GG haben Träger privater Informationssysteme wie jede natürliche oder juristische Person das Recht, sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Das umfaßt auch die *Erfassung* und Speicherung der auf diese Weise erhaltenen Informationen.

d) Dieses Recht findet nach Artikel 5 Abs. 1 seine *Schranken* in den Vorschriften der „allgemeinen Gesetze" (vor allem den gesetzlichen Bestimmungen zum Schutz der Jugend und in dem Recht der persönlichen Ehre).

Träger privater Informationssysteme müssen ihre Informationen zunächst wie jedermann aus allgemein zugänglichen Quellen beziehen können. Eine Informationsquelle ist dann allgemein zugänglich, wenn sie „allgemein oder zumindest im konkreten Einzelfall geeignet und dazu bestimmt ist, daß ein individuell nicht bestimmbarer Personenkreis von ihrem Inhalt Kenntnis erlangt" [82]). Das sind in erster Linie Massenmedien, wie Presse, Fernsehen, Rundfunk, Film, Ausstellungen, Anschläge etc.

Von der Weiterentwicklung der Technik und den gesellschaftlichen Lebensgewohnheiten wird es abhängen, *ob auch vom Staat geschaffene Informationssysteme allgemein zugängliche Informationsquellen* werden.

Soweit private Informationssysteme aus allgemein zugänglichen Quellen Informationen ermitteln wollen, findet ihr Recht auf freies Recherchieren in den allgemeinen Gesetzen seine Schranken. Untersagt ist ihnen eine Betätigung, bei der etwa Strafvorschriften oder bürgerlichrechtliche Bestimmungen verletzt werden. Sobald sich die Meinungsbildung durch Recherchieren von Informationen nicht auf ihre ideelle Wirkung beschränkt, sondern gleichzeitig auch Rechtsgüter gefährdet, hat jedes Rechtsgut den Vorzug vor der Meinungsbildung. Das bedeutet, Träger privater Informationssysteme sind im Recherchieren von Informationen sehr beschränkt. Informationssysteme der öffentlichen Verwaltung, die Individualinformationen enthalten, werden niemals allgemein zugängliche Informationsquellen sein.

Etwas anderes könnte gelten, soweit in staatlichen Informationssystemen Sachinformationen verarbeitet werden. Hier könnte ein Zugriffsrecht Privater bestehen. Dieses Ergebnis erscheint jedoch rechts- und staatspolitisch höchst bedenklich. Öffnet man staatliche Informationssysteme privater Kenntnisnahme, dann führt dies zu der höchst unerwünschten Folge, daß das ohnehin durch die Lobby gestörte „Informationsgleichgewicht" zwischen Staat und Wirtschaft noch weiter zugunsten der Wirtschaft verschoben wird.

Dem Kundigen werden bereits zu einem noch früheren Zeitpunkt als bisher potentiell alle Pläne der Regierung und Verwaltung durch geeignetes Recherchieren im öffentlichen Informationssystem offenbar, so daß potente wirtschaftliche Interessenvertretungen zuungunsten nichtwirtschaftlicher Interessen eine ungerechtfertigte Vorzugsstellung erhalten.

Es wäre zu überlegen, ob gewerblichen und innerbetrieblichen Informationssystemen der Zugriff auf öffentliche Informationssysteme nur in beschränktem Maße gewährt werden sollte. Der Bürger und die Massenmedien jedoch können abfrageberechtigt sein.

Wie dies rechtlich unter den Prämissen eines oben behaupteten Grundrechts auf Information zu erreichen ist, erscheint unklar, zumal die nicht im Parlament vertretenen Träger realer Macht über ihnen freundlich gesinnte Presseorgane wieder Zutritt erhalten. Das Problem ist nicht ausdiskutiert und kann hier nur aufgezeigt werden.

4.2.1.2. Artikel 12

Artikel 12 schützt nicht gesetzlich verbotene Berufe [83]). Ein Privater könnte sich also nicht darauf berufen, das zu erstellende Gesetz verbiete eine Betätigung, die er sich zum Beruf gemacht habe. Artikel 12 gewährt das freie Recht der Berufswahl, es garantiert jedoch weder den Fortbestand einer bestimmten Berufsart, noch schließt es die Möglichkeit zu einer Regelung der Berufsausübung aus. Die den Inhaber eines Informationssystems betreffenden Bestimmungen würden jedoch in jedem Fall nur eine Berufsausübungsregel darstellen, da gemäß obiger Ausführung zumindest das Recht, sich aus allgemein zugänglichen Quellen zu informieren, nicht beschnitten wird. Zudem ist hier darauf hinzuweisen, daß Artikel 12 nur ein Recht auf Ausübung des Berufs gewährt, nicht aber ein Recht, im Rahmen eines Berufs bestimmte Handlungen gegenüber Personen vorzunehmen. Das bedeutet praktisch: Würde der Gesetzgeber — was durchaus zu wünschen wäre — Detekteien und ähnlichen Ausforschungsunternehmen die Verwendung von EDVAn verbieten (und damit das private Informationsgewerbe an der Wurzel treffen), wären solche Regelungen Berufsausübungsregeln, die ohnedies unter einfachem Gesetzesvorbehalt stehen.

Dies wäre um so mehr zu wünschen, als sonst auch staatliche Stellen, sollten ihre Informationssysteme ihren Wünschen nicht voll genügen, sich an die gewerblichen Informationssysteme wenden könnten, gegebenenfalls sie sogar durch staatliche Förderung ihren Zwecken anbequemen. Daß solche Möglichkeiten selbst im demokratischen Rechtsstaat nicht von der Hand zu weisen sind, zeigen zur Genüge die Belege aus der amerikanischen Literatur.

4.2.1.3. Artikel 14

Das gleiche gilt für Artikel 14: Er schützt nicht gesetzlich verbotene Informationssysteme.

[82]) Maunz - Dürig - Herzog, Artikel 5 N. 87

[83]) Maunz - Dürig - Herzog, Artikel 12 N. 19; BVerfGE 7, 397

4.2.2. Artikel 2 Abs. 1

Neben den speziellen Grundrechten kann der Inhaber eines Informationssystems aber auch die allgemeine Handlungsfreiheit gemäß Artikel 2 Abs. 1 GG geltend machen. Artikel 2 Abs. 1 schützt anerkanntermaßen auch die Freiheit gewerblicher Betätigung [84]). Zunächst kann daraus eine grundsätzliche Freistellung der Verarbeitung von Informationen abgeleitet werden, da Informationsermittlung bis zur Informationsweitergabe ohne Zweifel Handlungen darstellen, die unter Artikel 2 Abs. 1 fallen.

Auf Grund der Schrankentrias kann die allgemeine Handlungsfreiheit allerdings insoweit durch Gesetz eingeschränkt werden, als dieses Gesetz der verfassungsmäßigen Ordnung entspricht. Ein solches Gesetz entspricht nun aber der verfassungsmäßigen Ordnung, wenn es auf der einen Seite die speziellen Grundrechte dessen berücksichtigt, der die allgemeine Handlungsfreiheit für sich in Anspruch nimmt [85]), auf der anderen Seite aber auch nicht gegen grundrechtlich verbürgte Freiheiten der Betroffenen vorgeht. Zu diesen grundrechtlich verbürgten Freiheiten der Betroffenen gehört entsprechend dem oben entwickelten Gedankengang das Recht auf die Informationen über den eigenen Individualbereich.

4.3. Ergebnis: Interessenabwägung

Damit kann die *Konsequenz* formuliert werden:

Geht man davon aus, daß auch der Träger von nicht-öffentlichen Informationssystemen für sich selbst die grundrechtlich verbürgten Rechte, vor allem die allgemeine Handlungsfreiheit, geltend machen kann, steht der Gesetzgeber vor der Notwendigkeit, innerhalb des Rahmens, der vom Wesensgehalt der Grundrechte des Inhabers auf der einen Seite, vom Wesensgehalt der des von der Informationsverarbeitung Betroffenen auf der anderen Seite gespannt wird, eine *Interessenabwägung* vorzunehmen. Diese Interessenabwägung muß den Grundwertungen des Grundgesetzes gerecht werden.

Dies führt aber entsprechend dem diesem Gutachten zugrunde gelegten Verständnis des Grundgesetzes dazu, die potentielle Gefährlichkeit von Informationssystemen entscheidend zu berücksichtigen. Die Interessenabwägung fällt also überwiegend zuungunsten des privaten Informationssystems aus. Daraus folgt, daß die Informationsverarbeitung von Individualinformationen, die nicht aus allgemein zugänglichen Quellen stammen, grundsätzlich verboten ist, wenn und solange kein „rechtlicher Grund" für eine Ausnahme vorliegt.

Freilich ist dabei zu berücksichtigen, daß spezielle Grundrechte, die der Träger eines Informationssystems gegenüber dem Staat geltend machen kann, einen Bereich abstecken, innerhalb dessen sich der Bürger auch von privaten Informationssystemen Eingriffe gefallen lassen muß: Dies ist im wesentlichen der Bereich, in dem sich der Bürger durch Vertrag oder Einwilligung freiwillig einer gewissen Begrenzung unterworfen hat, ferner der Bereich von Individualinformationen, die aus allgemein zugänglichen Quellen erhältlich sind.

Überhaupt verboten werden muß die Verarbeitung von Individualinformationen, die den durch spezielle Grundrechte geschützten Bereich des Betroffenen berühren.

Damit lassen sich die Kriterien für das Privat-DschRecht festlegen. Sie verdichten sich zu folgenden *allgemeinen* Grundsätzen:

1. In nicht-öffentlichen Informationssystemen dürfen nur solche Informationen verarbeitet werden, die aus allgemein zugänglichen Quellen stammen oder solchen zu entnehmen sind.
2. Innerhalb eines Vertragsverhältnisses oder aufgrund eines Vertrags oder der Einwilligung des Betroffenen dürfen auch solche Individualinformationen verarbeitet werden, die zur Abwicklung des Vertragsverhältnisses notwendig sind, bzw. die von Vertrag oder Einwilligung umfaßt sind.
3. Folgende Informationen dürfen in nicht-öffentlichen Informationssystemen überhaupt nicht verarbeitet werden:
   - — Informationen, die die religiöse oder weltanschauliche Überzeugung betreffen (Ausnahme: Glaubensgemeinschaften),
   - — Informationen, die die politische Überzeugung betreffen (Ausnahme: politische Parteien),
   - — Informationen, die über die Teilnahme an einer politischen Versammlung oder Kundgebung Aufschluß geben,
   - — Informationen, die den Inhalt nicht-veröffentlichter Briefe oder Ferngespräche wiedergeben.

   Diese allgemeinen Grundsätze sind nun für die verschiedenen Arten der privaten Informationssysteme und ihrer Informationsverarbeitung zu konkretisieren.

5. Keine einheitliche Regelung

Ausgangspunkt ist zunächst die Feststellung, daß die Regelung nach den verschiedenen Arten von Informationssystemen unterschiedlich ausfallen muß. Zum zweiten muß berücksichtigt werden, daß die einzelnen Phasen der Informationsverarbeitung unter Umständen unterschiedlich intensiv in die Freiheitssphäre des einzelnen eingreifen. Innerhalb der einzelnen Arten von Informationssystemen ist demnach noch einmal zu unterscheiden zwischen den einzelnen Phasen der Informationsverarbeitung. Oben wurden die Informationssysteme, die Individualinformationen verarbeiten, in vier Gruppen aufgeteilt:

---

[84]) Maunz - Dürig - Herzog, Artikel 2 Abs. 1 N. 43 ff.

[85]) dies aus der unbestrittenen Auffassung des BVerfG — vgl. S. 4, 52 (57) für das Verhältnis von Artikel 2 Abs. 1 und Artikel 6 Abs. 2 — die speziellen Grundrechte im Rang vor Artikel 2 stehen

— Informationssysteme zur Weitergabe an einzelne (gewerbliche IS),

— Informationssysteme zur Weitergabe an die Öffentlichkeit,

— Informationssysteme zur internen zweckgebundenen Verwendung (innerbetriebliche IS),

— Sonstige interne Informationssysteme.

5.1. Nicht alle privaten Informationssysteme sind regelungsbedürftig

Aus den folgenden Überlegungen sollen nun die Informationssysteme zur Weitergabe an die Öffentlichkeit und die sonstigen internen Informationssysteme ausgeschieden werden. Ob das Datenschutzgesetz ungeachtet dessen dennoch Bestimmungen für sie enthalten soll, sei dahingestellt. In unserem Gesetzgebungsvorschlag werden diese Informationssysteme durch entsprechende Bestimmungen ausgeschlossen.

Der Ausschluß ist wie folgt zu begründen:

5.2. Informationssystem zur Weitergabe an die Öffentlichkeit

Informationssysteme, die Informationen an die *Öffentlichkeit* weitergeben, besitzen einen Sonderstatus, der eng mit ihrem öffentlichen Auftrag zusammenhängt [86]).

Den Rahmen für diese Informationssysteme gibt Artikel 5 GG in der Garantie der Pressefreiheit [87]). Einerseits ergeben sich eine Fülle von Spezialproblemen, andererseits liegen in den einzelnen Pressegesetzen bereits Gesetze vor, die zumindest Teilbereiche der Informationsverarbeitung regeln. Damit ist ein Ausschluß dieser Problematik an dieser Stelle gerechtfertigt.

5.3. Sonstige interne Informationssysteme

Die hier verwendete weite Fassung des Begriffs der Informationsverarbeitung hat zur Folge, daß auch private Informationssysteme, die nur zum eigenen Gebrauch angelegt werden, wie etwa private Notizbücher, ebenfalls unter die Regelungsmaterie fallen. Diese IS sind dadurch gekennzeichnet, daß es sich entweder um Bagatellfälle handelt, oder daß das Interesse des Inhabers an der Person des Betroffenen nicht einem Kontaktverhältnis entspringt, sondern einem in der Person des Empfängers liegenden Grund.

Da die Beteiligten in keinem Zusammenhang stehen, zeigt auch die Informationsverarbeitung bis zu dem Punkt, wo die Information weitergegeben wird, keine Auswirkungen. Die Art und der Umfang der Weitergabemöglichkeit schließt ein Regelungsinteresse im Sinne des Schutzes der Allgemeinheit und der gesellschaftspolitischen Bedeutung aus. Die hier betroffenen Probleme liegen auf dem Gebiet der Ehrverletzung, Nachschnüffelei und Indiskretion unter zwei Privaten.

Es reicht nun aber unseres Erachtens aus, diese Probleme mit Hilfe der bestehenden Vorschriften des Strafgesetzbuches und des BGB zu lösen. Für die unterhalb der Schwelle des StGB bleibenden Fälle genügt vorläufig, bis zu einer grundsätzlichen Novellierung des BGB in diesem Punkt, die von Rechtsprechung entwickelte Ausformung des allgemeinen Persönlichkeitsrechts.

Da allerdings die Grenze zu den Informationssystemen zur Weitergabe fließend ist, scheint es gerechtfertigt, im Gesetz eine Abgrenzung vorzunehmen.

Sie sollte einerseits vom Zweck her angelegt sein, andererseits eine quantitative Abgrenzung enthalten, um Mißbrauch vorzubeugen.

Vorzuschlagen wäre, solche Informationssysteme auszunehmen, die lediglich (zur privaten Verwendung im privaten Lebenskreis?) angelegt werden und keine elektronische Datenverarbeitungsanlage verwenden. Informationssysteme dieser Art, die EDVAn verwenden, unterliegen den Bestimmungen für Informationssysteme zur Weitergabe an einzelne.

Damit bleiben für die folgende eingehendere Analyse die Informationssysteme zur Weitergabe an Dritte (II.) und die internen zweckgebundenen Informationssysteme übrig (III.).

[86]) vgl. BGH in NJW 62, 1005; 63, 485; 66, 2010

[87]) vgl. statt aller Maunz - Dürig - Herzog, Artikel 5 N. 118 ff.

II. Informationssysteme zur Weitergabe an Dritte — Konsequenzen für den Gesetzgeber

1. Eingrenzung

Entsprechend der obigen Definition sollen im folgenden Auskunfteien, Detekteien, Adreßverlage und ähnliche Informationssysteme untersucht werden. Dabei soll davon ausgegangen werden, daß solche Informationssysteme *nur in gewerblicher Form* betrieben werden. Andere Formen scheinen nicht regelungsbedürftig zu sein.

2. Gang der Untersuchung

Zunächst werden die Regelungen behandelt, die die Unternehmer objektiv, d. h. unabhängig davon, ob

jemand Ansprüche geltend macht, bezüglich der Verarbeitung von Individualinformationen einschränken, 3. Entsprechend der Zielrichtung des Gutachtens werden Verpflichtungen für den Unternehmer, bestimmte Informationen zu verarbeiten (Rechte *auf* Informationsverarbeitung) nicht behandelt. Die Einschränkungen müssen für jede Phase gesondert bestimmt werden (Topoi, s. o.). Bezüglich der Abgrenzung der einzelnen Phasen wird auf den allgemeinen Teil verwiesen.

Anschließend folgen Ausführungen zu den Erweiterungen der (subjektiven) Rechte des einzelnen, 4. Unter 5. schließen sich Überlegungen zur öffentlichen Kontrolle an, worauf zum Schluß die Strafnormen folgen, 6.

3. Gesetzliche Einschränkungen der privaten Informationsverarbeitung

3.1. Ermittlung

Im Gegensatz zu öffentlichen Stellen sind nichtöffentliche Stellen nicht an den Grundsatz der Gesetzmäßigkeit ihres Handelns i. S. des Verwaltungsrechts gebunden. D. h., sie brauchen für ihre Handlungen keine gesetzliche Grundlage. Das ergibt sich auch schon aus Artikel 2 Abs. 1 und Artikel 12 GG, die jeder private Unternehmer als Inhaber eines Informationssystems für sich in Anspruch nehmen kann.

Für die Informationsermittlung gilt aus diesem Grunde nicht das gleiche wie bei Informationsverarbeitung durch öffentliche Stellen. Dort wurde die Beschränkung der Informationsermittlung als zentrales Anliegen herausgestellt.

Bei der Informationsverarbeitung durch Private treten an diese Stelle die oben angesprochenen grundgesetzlichen Wertungen bzw. die Erwägung der jeweiligen Interessenlagen. Der in Artikel 2 Abs. 1 GG garantierte Freiheitsraum desjenigen, der die Informationen sammelt, kann erst dann eingeschränkt werden, wenn er mit dem Freiheitsraum des Betroffenen kollidiert [1]). Eine solche Kollision kann aber nicht schon dann eintreten, wenn der Inhaber eines Informationssystems die Information lediglich zur Kenntnis nimmt und noch nicht in ein Verarbeitungssystem einbringt. Das würde bedeuten, daß man ihm quasi die Augen verbinden müßte. Der entscheidende Schritt wird erst dann vollzogen, wenn die Information in einer bestimmten Weise fixiert wird.

Damit ist die Informationsermittlung jedem Interessenten freizustellen.

3.1.1. Regelung der Art und Weise der Ermittlung

Ein Gegenargument könnte sich aus den §§ 298, 299 StGB und den durch die Rechtsprechung entwickelten Schutzmöglichkeiten des einzelnen gegen bestimmte Ermittlungsarten gemäß § 823 BGB ergeben.

Eine Analyse von §§ 298, 299 StGB ergibt dagegen, daß hier nur vor untragbaren *Ermittlungsmethoden,* nicht vor der Ermittlung selbst (= z. B. Lesen des Briefes) geschützt werden soll. Diese Normen entwickelten sich nämlich aus Beleidigungs- und Betrugstatbeständen [2]).

Auch die die Ermittlung betreffende Auslegung des allgemeinen Persönlichkeitsrechts schützt den Betroffenen vor *Entartungsformen der Informationsermittlung.*

Inwieweit sich aus diesen konkreten gesetzlichen Bestimmungen Einschränkungen des oben aufgestellten Grundsatzes ergeben, braucht nicht geklärt zu werden. Es ist festzustellen, daß diese Regelungen hinreichen und jeweils in ihrem Rahmen neueren Entwicklungen angepaßt werden müssen (vgl. die Änderung des § 299 StGB).

3.1.2. Alternative zur Freistellung der Ermittlung

Anknüpfend an die bereits vorhandene Regelung der Informationsermittlung bei *öffentlichen* Informationssystemen konnte alternativ zur unter 3.1. vertretenen Meinung auch an eine weitergehende Beschränkung der Ermittlung gedacht werden. Angesichts der Tatsache, daß auch Ermittlungstätigkeiten den Betroffenen massiv stören können, scheint eine Erfassung der in Frage kommenden Tatbestände angebracht. Man denke z. B. an das allzu ausgiebige Recherchieren einer Detektei.

Wenn man sich dieser Argumentation anschließt, finden schon bei der Ermittlung die Erwägungen statt, die zur Regelung der Erfassung und Speicherung führen.

3.1.3. Ausschlußkatalog

Ungeachtet dessen, daß die Informationsermittlung *allgemein* gemäß dem obigen Grundsatz nicht eingeschränkt werden kann, ist noch zu prüfen, ob nicht bezüglich bestimmter, in Ausschußkatalogen festzulegender Informationen eine Einschränkung angebracht ist.

Denkbar wäre zunächst, die Ermittlung von Informationen einzuschränken, die einen derartig hohen Intimitätsgrad besitzen, daß sie grundsätzlich niemanden angehen. Dazu würden etwa Informationen aus dem Ehe- und Sexualbereich zählen. Auch hier gilt jedoch, daß Informationen durch ihre semantische und pragmatische Bedeutung relativ sind; d. h., die an ihnen bestehenden Interessen sind abhängig von Zeit, Ort, Umständen und beteiligten Personen. *Ein allgemeingültiger Ausschlußkatalog kann somit nicht zusammengestellt werden.*

Anders verhält es sich mit Informationen, deren Verarbeitung durch die speziellen Grundrechte ausgeschlossen werden. Bezüglich dieser Informationen wurde oben bereits ein Katalog erstellt [3]):

— Informationen über das religiöse Bekenntnis,

— Informationen über politische Einstellung oder Weltanschauung,

[1]) Für die Kollision von Artikel 5 und Artikel 14 GG vgl. BVerfGE 7, 235.
[2]) Maurach, § 22
[3]) s. o. I. 4.3.

— Informationen, die entgegen Artikel 10 GG erhalten wurden.

Zwar genießen alle Individualinformationen den gleichen Schutz aus dem allgemeinen Grundrecht des Artikels 2 Abs. 1 GG. Darüber hinaus jedoch erfahren die Informationen, die mit den speziellen Grundrechten in Zusammenhang stehen, eben dadurch eine besondere Qualität. Dies muß sich soweit auswirken, daß die oben angesprochene Interessenkollision, die normalerweise noch nicht bei der Ermittlung Platz greift, hier bereits in dieser Phase auftritt. Dies läßt sich durch die pragmatische Überlegung stützen, daß z. B. Informationen über die Teilnahme an politischen Veranstaltungen kaum ohne Absicht zur Verwendung in einer grundrechtswidrigen Weise ermittelt werden können.

Damit läßt sich sagen, daß bezüglich der Information, die durch spezielle Grundrechte geschützt sind und die in diesem Zusammenhang auch im Gesetz zu erwähnen sind, eine Ausnahme von der generellen Freistellung der Informationsermittlung zu machen ist; bezüglich:

— Informationssystemen der religiösen Gemeinschaften,

— Informationssystemen der durch Artikel 4/9 GG geschützten Verbände und Gruppen.

3.2. Erfassung/Speicherung

3.2.1. Allgemeine Individualinformationen

Während dem Inhaber eines Informationssystems die Ermittlung von Informationen grundsätzlich freigestellt sein muß, scheint es fraglich, ob der ihm zustehende Freiheitsraum der Artikel 2 Abs. 1 und Artikel 12 GG auch die Informationsverarbeitung vom *Zeitpunkt des Einbringens ins System* ab deckt.

Der zwischen dem Betroffenen und dem Verarbeitenden vorhandene Interessenkonflikt besteht in folgendem:

— Der Betroffene will die ihn kennzeichnenden Informationen aus einem bestimmten Grunde zurückhalten.

— Der Verarbeitende hat aus einem bestimmten Grunde ein Interesse an der Person des Betroffenen und damit an dessen Individualinformationen.

Der eigentliche Zeitpunkt, an dem diese Interessen aufeinanderprallen, ist im vorliegenden Falle der der Weitergabe. Erst dann gelangen nämlich die Informationen in die Hände desjenigen, der sie zu einem bestimmten Zweck braucht und somit auf die Person des Betroffenen einwirken kann. Dies wäre etwa gegeben, wenn sich ein Arbeitgeber bei einer Detektei über seinen Arbeitnehmer informiert.

Bei dieser Betrachtung wird jedoch nicht berücksichtigt, daß erfaßte und gespeicherte Informationen bereits durch ihre Fixierung konkrete Gefahren heraufbeschwören. Diese Tatsache besteht insbesonders angesichts der Möglichkeiten moderner automatisierter Informationssysteme und ihrer potentiellen Kombinations-, Interpretations- und Verbundmöglichkeiten. In Wirklichkeit zeitigt nämlich bereits die Aufnahme der Informationen in ein System Auswirkungen auf den Betroffenen. Von dem Zeitpunkt ab können nämlich die ihn betreffenden Informationen durch unterschiedliche Arbeitsgänge in völlig andere Sachzusammenhänge gebracht werden, was dem Betroffenen jegliche Kontroll- und Einflußmöglichkeit nimmt.

Gemäß der Grundrechtsauslegung Artikel 2 Abs. 1 müßte demnach die Erfassung und Speicherung von Individualinformationen verboten sein. Der Betroffene kann sich jedoch durch Zustimmung seiner Rechte begeben, solange nicht Artikel 2 Abs. 1 im Kerngehalt betroffen wird [4]).

Die *Erfassung und Speicherung* von Informationen ist also bereits *unter* den *Vorbehalt der Zustimmung* des Betroffenen zu stellen.

Die Zustimmung kann ausdrücklich oder stillschweigend vorliegen. So muß z. B. das Ausfüllen eines Fragebogens als Zustimmung betrachtet werden.

Vom Vorbehalt der Zustimmung ausgenommen sind die Individualinformationen, die aus allgemein zugänglichen Quellen stammen bzw. aus solchen erhältlich sind; z. B. Name, Adresse, Telefonnummer u. ä. Die freie Information aus diesen Quellen steht jedem gemäß Artikel 5 GG zu [5]).

3.2.2. Qualifizierte Individualinformationen

Aufgrund ihrer besonderen Bedeutung dürfen Informationen, die durch die besonderen Grundrechte geschützt sind, *auch mit Zustimmung nicht erfaßt und gespeichert* werden. Sie erfahren diesen besonderen Schutz ja gerade wegen der großen Gefahr, die besteht, wenn diese Informationen in die falschen Hände gelangen.

In Anbetracht der Tatsache, daß sich z. B. die politischen Verhältnisse schnell ändern können, sind so elementare Informationen, wie über religiöses Bekenntnis und politische Überzeugung, sehr gefährlich, wenn sie in einem IS zur Verfügung stehen. Hinsichtlich der Zustimmung kann der Betroffene zu leicht überrumpelt werden.

Es dürfen demnach nicht erfaßt und gespeichert werden:

— Informationen, die das religiöse und weltanschauliche Bekenntnis einer Person betreffen (ausgenommen IS der Glaubensgemeinschaften), Artikel 4 GG;

— Informationen, die die politische Überzeugung der Person betreffen (ausgenommen Informationssysteme der politischen Parteien — falls sie zulässig sind —);

— Informationen, die über die Teilnahme an einer politischen Versammlung oder Kundgebung Aufschluß geben, Artikel 8 GG;

[4]) Nipperdey (2), 28
[5]) s. o. I. 4.2.1.1.

— Informationen, die den Inhalt nicht veröffentlichter Briefe oder Ferngespräche wiedergeben, Artikel 10 GG.

3.2.3. Löschungspflicht

Man könnte daran denken, das Informationssystem zu verpflichten, die Individualinformationen nach einer bestimmten Zeit wieder zu löschen. Diese Löschungsfrist könnte etwa durch Ablauf eines Vertrags- oder Vertrauensverhältnisses zwischen dem Betroffenen und dem Informationssystem bestimmt sein. Die Beteiligten stehen jedoch bei Weitergabe-Informationssystemen in keinem derartigen Verhältnis zueinander. Damit scheidet diese Möglichkeit einer Fristbestimmung aus.

Um jedoch zu verhindern, daß sich die Individualinformationen einer Person beliebig lange in einem Informationssystem befinden, könnte dennoch eine Löschungsfrist von z. B. sieben oder zehn Jahren eingeführt werden [6]). Diese Lösung ist aber für gewerbliche IS zu hart. So kann etwa von einer Auskunftei nicht verlangt werden, daß sie die vorhandenen Informationen löscht, weil sie dann beim nächsten Auftrag völlig neu ermitteln muß. Der einzelne erfährt ausreichenden Schutz durch die ihm zustehenden Löschungs- und Berichtigungsansprüche [7]).

3.3. Veränderung

Die Veränderung von Informationen kann durch Umwelteinflüsse oder durch menschliches Handeln verursacht werden.

3.3.1. Veränderung durch Umwelteinflüsse

Informationen können durch Hitze, Kälte usw. verändert werden. Dagegen sind geeignete Maßnahmen zu treffen, etwa ausreichende Klimatisierung der Verarbeitungsräume, Sicherungen gegen Brand, Wasser u. ä. Derartige Maßnahmen sind Teil der Datensicherung, es wird insoweit auf den diesbezüglichen Exkurs verwiesen [8]).

3.3.2. Veränderung durch Menschen

Grundsätzlich muß die Verarbeitung der Individualinformationen, die rechtmäßig ins System gelangt sind, freigestellt sein, solange die Informationen nicht das System verlassen, also Dritten zugänglich sind. Dieser Umgang mit den Informationen hat noch keine Auswirkungen auf den Betroffenen; es handelt sich um einen rein internen Vorgang. Darüber hinaus besitzt der Verarbeitende kein direktes Interesse an der Person des Betroffenen, sondern erst der Interessent, der die Informationen hinterher erhalten wird. Aus diesem Grunde entstehen ebenfalls keine Folgen aus der internen Verarbeitung.

Wie jedoch die Ausführungen zur Informationsveränderung im Teil C gezeigt haben, ist dabei nach den verschiedenen Arten der Veränderung zu differenzieren.

3.3.2.1. Benutzeränderung

Die veränderte Zuordnung von Informationen zu anderen Benutzern kann zur Folge haben, daß die Informationen in einem völlig anderen Bedeutungszusammenhang gestellt werden. Der Zugriff von Unbefugten ist zu verhindern. Wie im Exkurs Datensicherung gezeigt, läßt sich dies am besten durch Datensicherungsmaßnahmen erreichen. Ein Datenschutzgesetz muß lediglich die Rechtsgrundlage für solche Maßnahmen enthalten.

3.3.2.2. Informationsverknüpfung

Darunter wird die Verknüpfung von Informationen und die sich daraus ergebende Gewinnung neuer Informationen gefaßt. Die Verknüpfung kann zum einen derart vorgenommen werden, daß keine Informationen entstellend verknüpft werden, aber etwa ein umfassendes Personenmodell erstellt wird. Dies ist jedoch kein Problem der Informationsveränderung: der Betroffene hat schon die Möglichkeit zu bestimmen, welche Informationen in das System gelangen. Hat er dieses Recht wahrgenommen, kann das IS aus den vorhandenen auch ein umfassendes Personenmodell erstellen oder sie in sonstiger Weise verknüpfen, solange dadurch keine Entstellungen bewirkt werden.

Zum anderen können bei der Verknüpfung Informationen verfälscht werden, indem etwa die vorhandenen Informationen derart verknüpft werden, daß kein umfassendes, sondern ein aus dem Zusammenhang gerissenes, entstellendes Bild einer Person entsteht [9]). Wollte man eine solche Verarbeitung objektiv (also ohne daß erst der Betroffene eine Rechtsverletzung geltend macht) verbieten, käme das einer objektiven Pflicht zur Wahrheit und Vollständigkeit der Verarbeitung gleich [10]). Im Grunde kann jedoch nur der Betroffene feststellen, ob eine Verzerrung vorliegt oder nicht, dies ist die zentrale Aussage der Relativität der sog. Privatsphäre. Das bedeutet, daß gegen Entstellungen und Verfälschungen von Informationen allein der Betroffene selbst vorgehen kann, indem er einen subjektiven Anspruch auf Entzerrung geltend macht. Dieser Anspruch stellt eine Erweiterung seiner Rechtsschutzmöglichkeiten dar und wird demgemäß unter 4. näher ausgeführt.

3.3.2.3. Informationsverfälschung

Darunter wird die Verfälschung einer Information verstanden, die nicht durch die Verknüpfung dieser Information mit anderen Informationen geschieht, sondern durch inhaltliche Umgestaltung eben dieser Information, z. B. ist ein Geburtsdatum anstatt „1.2.34" als „10.2.34" im System enthalten. Jedoch gilt hier das eben unter 3.3.2.2. Ausgeführte in gleicher Weise: eine Verfälschung kann nur vom Betroffenen beurteilt werden. Insoweit ist ebenfalls auf die Rechtsschutzmöglichkeiten des einzelnen zu verweisen.

---

[6]) so etwa im Kanad. DSchG
[7]) s. u. 4 ff.
[8]) B, Exkurs II
[9]) ähnliches ist bei der Presse möglich, vgl. dazu BGHZ 31, 308 ff.
[10]) Vgl. § 6 des baden-württembergischen Landespressegesetzes; auch hier wird keine Pflicht zur objektiven Wahrheit statuiert.

3.4. Weitergabe

Wie oben ausgeführt, wird das Problem der Informationsverarbeitung im Augenblick der Weitergabe am offensichtlichsten: Die Informationen gelangen dann in die Hände desjenigen, der an dem Betroffenen selbst interessiert ist. Damit sind unmittelbare Auswirkungen auf den Betroffenen selbst zu erwarten. Da dem einzelnen ein alleiniges Bestimmungsrecht über die Verwendung seiner Individualinformationen zusteht, und der Verarbeitende dadurch nicht in seinem Mindestfreiheitsraum nach Artikel 2 Abs. 1 GG beschränkt wird, muß die *Weitergabe von der grundsätzlichen Zustimmung* des Betroffenen abhängig gemacht werden.

Hierfür kommen nicht nur die ermittelten und dann erfaßten Informationen in Frage, die ja bereits zu einem früheren Zeitpunkt zustimmungsbedürftig sind, sondern speziell die in einem bestimmten Verarbeitungsgang gewonnenen neuen Informationen. Außerdem muß dem Betroffenen die Möglichkeit der Kontrolle über den Zusammenhang gegeben werden, in welchem die Informationen nun stehen. Informationssysteme, die Informationen verarbeiten, die den Schutz spezieller Grundrechte genießen [11]), muß die Weitergabe konsequenterweise verboten werden.

3.4.1. Systemverkauf

Als *Sonderfall der Weitergabe von Informationen ist der Verkauf ganzer Systeme oder Dateien* zu betrachten. Hierbei sind zwei Fälle zu unterscheiden:

— Reiner Inhaberwechsel, wobei das eigentliche System bzw. die Datei unberührt bleiben. Das ist etwa der Fall, wenn eine Detektei schließen muß, der Inhaber an jemand anderen verkauft und dieser die gleiche Detektei unter einem anderen Namen weiterführt.

— Verkauf eines Systems bzw. einer Datei und deren Integration in ein(e) andere(s). Dieser Fall wäre gegeben, wenn etwa eine Detektei einen gewissen Informationsbestand an eine Handelsauskunftei oder eine andere Detektei verkauft.

3.4.1.1. Inhaberwechsel

Bei reinem Inhaberwechsel eines Informationssystems muß unterschieden werden, ob sich die Zielsetzung, d. h. der Zweck, den das Unternehmen mit der Informationsverarbeitung verfolgt, geändert hat oder nicht.

Wenn der neue Inhaber das Unternehmen in gleicher Weise weiterführt wie vorher, ändert sich für die Betroffenen nichts an ihrer Situation. Sowohl die Zweckbestimmung der Information wie der Rahmen der Verarbeitungsmöglichkeiten bleibt gleich.

Im Falle einer gleichzeitigen Zweckänderung jedoch besteht die Möglichkeit, daß die Informationen in einen neuen, vom Betroffenen nicht gewollten Zusammenhang gestellt werden. Deshalb muß ihm ermöglicht werden, seine Rechte geltend zu machen. Es erscheint unsinnig, seine Zustimmung zum Verkauf zu verlangen, der Aufwand würde häufig einen Verkauf verhindern. Es genügt, wenn die Betroffenen vom Verkauf benachrichtigt werden, so daß es ihnen unbenommen bleibt, ihre Rechte anschließend wahrzunehmen. Im übrigen wird der Verkauf von der Genehmigung der Aufsichtinstanz abhängig gemacht [12]).

3.4.1.2. Systemverschmelzung

Werden zwei Informationssysteme verschmolzen, ändern sich die Beziehungen zwischen Betroffenem und Informationssystem im gleichen Maße wie bei einem Inhaberwechsel mit Zweckänderung. Dies ist auch dann der Fall, wenn mit der Verschmelzung keine Zweckänderung verbunden ist.

Darum ist ein derartiger Verkauf immer wie der obige 2. Unterfall, Inhaberwechsel mit Zweckänderung zu behandeln.

3.4.2. Zusammenfassung

Das Ergebnis der Ausführungen zur Weitergabe lautet: Jede Detektei, Auskunftei etc. braucht für jeden Informationsverkauf die Zustimmung des Betroffenen. Das bedeutet das scheinbare Ende eines Berufsstandes. Denn kein überwachter Ehemann wird seine Zustimmung zur Weitergabe seiner Informationen über ihn an die überwachende Ehefrau zustimmen. Das gleiche gilt für wirtschaftliches Verhalten. Zusätzliche Schwierigkeit: Die Detektei ist gegenüber der überwachenden Ehefrau verpflichtet, die Information zu liefern, oder zumindest mit Erfolgsaussicht tätig zu werden, weil sich sonst eben die Kunden nicht mehr an die Detektei wenden. Dann aber wird jede Vertragserfüllung aufschiebend bedingt gültig durch Zustimmung des Betroffenen ... Ergebnis auch insoweit: Ende der Detektei. Sie kann sich nicht mehr halten. Eine Möglichkeit, die Zustimmung des Betroffenen zu ersetzen, besteht jedoch nicht. Die Lösung über die Zuständigkeitsverteilung wie im staatlichen Bereich ist hier nicht möglich, da es keine „Zuständigkeit von Detektiven" o. ä. gibt. Es bleibt keine andere Wahl, als die Zustimmung des Betroffenen als Kriterium zur Erlaubnis der Weitergabe bestehen zu lassen.

Die Konsequenz daraus hat jedoch nicht die schwerwiegenden Folgen, wie sie oben geschildert wurden: Denn die Individualinformationen, die die privaten Informationssysteme sammeln, bestehen zum größten Teil aus Informationen, die der Betroffene selbst an eine unbestimmte Öffentlichkeit weitergegeben hat. In diesem Rahmen dürfen sie auch gesammelt werden. — Soweit es sich jedoch um Informationen handelt, die nur zur beschränkten Weitergabe abgegeben wurden (= aus dem Verfügungsbereich des Betroffenen an Dritte entlassen wurden), bleibt das Verbot der Verarbeitung von Individualinformationen bestehen. Es ist insofern angezeigt, eine Vermutung zugunsten der Grundrechtssphäre auszusprechen, d. h. eine Vermutung gegen die rechtmäßige Erlangung der Informationen durch die Detektei. Diese muß also die rechtmäßige Erlangung der Informationen beweisen, also den Nachweis führen, daß die fragliche Information vom Betroffenen für eine unbestimmte Vielzahl freigegeben

[11]) siehe den Ausschlußkatalog D. II. 3.1.3.
[12]) dazu unten

wurde. Hierfür wird oft der Beweis des ersten Anscheins sprechen, den dann der Betroffene wieder entkräften muß.

Um das Auskunftsgewerbe nicht dem Untergang zu weihen, könnte noch eine Alternative erwogen werden, bei manueller Verarbeitung die Weitergabe wie bisher zu gestatten und lediglich die Benutzung von EDVAn zu verbieten [13]).

Diese Auffassung widerspricht jedoch den Intentionen dieses Gutachtens, das das Selbstbestimmungsrecht des einzelnen unbeschränkt gewährleisten und nicht zwischen manueller und automationunterstützter Informationsverarbeitung unterscheiden will [14]).

3.5. Löschung

Wie eingangs schon erwähnt wurde, werden unter 3. nur *Rechte gegen die Informationsverarbeitung* erörtert, hier also auch nur *Rechte gegen Löschung* [15]). Recht gegen Löschung besagt, daß Informationen, die im System gespeichert sind, aus diesem nicht vollständig eliminiert werden dürfen. Dabei ist jedoch zu bedenken, daß in diesem Gutachten der Schutz des einzelnen vor der Informationsverarbeitung (hier: der Löschung) unter dem Aspekt „Abwehr von Eingriffen in die sog. Privatsphäre" behandelt wird. Das von Artikel 2 Abs. 1 GG geschützte Interesse des einzelnen, selbst zu bestimmen, ob seine Individualinformationen der Umwelt zugänglich sind, wird sicher nicht dadurch beeinträchtigt, daß in der Umwelt Informationen gelöscht werden: In diesem Falle wäre es unmöglich, daß jemals gegen seinen Willen seine Individualinformationen zugänglich sind oder gegen seinen Willen verarbeitet werden.

Ein Recht gegen Löschung stellt somit kein Abwehrrecht dar. Es ist vielmehr ein Recht, am Leben aktiv durch die Abgabe von Informationen mitzuwirken. Dieser Aspekt kann jedoch *nicht* dem Schutz der sog. Privatsphäre zugeordnet werden und findet demgemäß hier keine Berücksichtigung.

4. Erweiterter Rechtsschutz des einzelnen [16])

Bei den Untersuchungen zur Unbrauchbarkeit der Privatsphäre hat sich gezeigt, daß eine positive inhaltliche Umschreibung der sog. Privatsphäre unmöglich ist. Jedoch konnte *wenigstens formal* angegeben werden, was *grundsätzlich Gegenstand einer sog. Privatsphäre* sein kann: Die Individualinformationen sind das Schutzobjekt des Datenschutzes i. e. S. Wegen der schon häufig erwähnten *Relativität der sog. Privatsphäre* bzw. der Individualinformationen kann im Grunde *nur der einzelne Betroffene den Umfang* seiner sog. Privatsphäre genau bestimmen. Nur er hat das Recht zu bestimmen, wer welche Information über ihn an wen weitergeben darf. Das führt dazu, daß im wesentlichen Individualinformationen nur mit *Zustimmung* des Betroffenen verarbeitet werden dürfen. Eine andersartige gesetzliche Einschränkung scheint uns nicht möglich zu sein.

Neben diesen Einschränkungen, die von den Inhabern der Informationssysteme beachtet werden müssen, auch ohne daß der Betroffene ein subjektives Recht (einen eigenen Anspruch) geltend macht, muß jeder einzelne den Umfang seiner sog. Privatsphäre auch in der Weise selbst bestimmen können, daß *er in großem Maße seinen Schutz durch eigene Ansprüche selbst verwirklicht.* Wegen der Relativität der sog. Privatsphäre ist gerade auf diesem Wege ein ausgewogener Schutz am ehesten zu erreichen [17]).

Im folgenden werden neben dem Schadenersatzanspruch besonders die Einsichts- bzw. Auskunftsrechte und die Ansprüche auf Löschung, Berichtigung, Ergänzung und Unterlassung untersucht.

4.1. Schadenersatz

Die unzulässige Verarbeitung von Individualinformationen kann dem Betroffenen großen Schaden zufügen. Beispiel: Eine unrichtige Auskunft einer Auskunftei hat zur Folge, daß ein Kredit nicht vergeben wird — oder daß jemand einen Kaufvertrag mit einem Partner abschließt, der in Wahrheit gar nicht erfüllt werden kann.

§ 676 BGB gewährt keinen Schadenersatz, wenn eine *Auskunft* erteilt wird. Als Auskunft im Sinne des § 676 ist jede Weitergabe von Informationen zu verstehen. Die Weitergabe von Individualinformationen an einzelne, die hier untersucht wird, ist nur als Gewerbe oder im Rahmen eines Gewerbes denkbar. Deshalb wird eine Weitergabe in diesen Fällen regelmäßig nur im Rahmen eines ausdrücklichen oder stillschweigenden Vertragsverhältnisses möglich sein. Für diese Ausnahme läßt auch § 676 den Schadenersatzanspruch bestehen. Eine zweite Ausnahme sieht § 676 bei einer unerlaubten Handlung vor. Gemäß § 823 Abs. 2 begeht derjenige eine schadenersatzpflichtige unerlaubte Handlung, der gegen ein den Schutz eines anderen bezweckendes Gesetz verstößt. Ein solches Gesetz ist ein Datenschutzgesetz, welches die hier vorgeschlagenen Regelungen enthält.

Schadenersatz ist nicht nur bei Auskünften zu gewähren, sondern — im Rahmen des § 823 Abs. 2 — *bei jedem Verstoß gegen eine Norm des Datenschutzgesetzes,* gleich, welche Phasen der Informationsverarbeitung diese Norm regelt. Grundsätzlich kann jeder selbst über seine Individualinformationen verfügen; jede Mißachtung dieses Satzes (in

---

[13]) Dieses Verbot wird durch Artikel 12 und 14 GG nicht ausgeschlossen, s. o. D. I. 4.2.1.2. und D. I. 4.2.1.3.

[14]) s. o. zur systematischen Grundlegung

[15]) Ein *Recht auf Löschung* stellt ein *Recht gegen Speicherung* dar und wurde daher auch unter „Speicherung" behandelt.

[16]) Vgl. dazu für den öffentlichen Bereich die im Ergebnis weitgehend gleichen Ausführungen unter C. Topos IX.

[17]) Solche Rechte des Betroffenen enthält auch schon der IPA-Entwurf, §§ 5, 6 — in Anlehnung an die englische Data Surveillance Bill von 1969; vgl. dazu auch Steinmüller (1), 88.

seiner jeweiligen Ausformung) muß daher einen Schadenersatzanspruch geben [18]). Der Anspruch umfaßt auch den *immateriellen Schaden.* Diese Auffassung wird sehr gut dem schwer faßbaren, fast „geistigen" [19]) Charakter dessen gerecht, was man mit der sog. Privatsphäre zu begreifen versuchte.

Es wird dem Betroffenen oft schwerfallen, einen Vermögensschaden nachzuweisen. Um den Anspruch auf Schadenersatz nicht zum großen Teil leerlaufen zu lassen, muß auch bei immateriellen Schäden eine billige Entschädigung in Geld gewährt werden [20]).

4.2. Einsichts- und Auskunftsrechte [21])

Um wirksam sein Verfügungsrecht aus Artikel 2 Abs. 1 GG über seine Individualinformationen ausüben zu können, muß der Betroffene wissen, wo welche Individualinformationen wozu verarbeitet werden. Es genügt nicht, daß der Betroffene dies durch die Umstände, durch Dritte oder durch die sozialen Auswirkungen der Verarbeitung erfährt. Er muß vielmehr umfassende Einsichts- und Auskunftsrechte haben [22]).

4.2.1. Unterscheidung von Einsicht und Auskunft

Einsicht besagt, daß man selbst unmittelbar Zugang zu den gespeicherten Informationen hat, derart, daß die Originale oder getreue Kopien (bei Schriftstücken: Xero- bzw. Fotokopie, bei EDVA: Ausdrucken oder Bildschirm, bei Filmen oder Fotografien: Abzüge) zugänglich sind.

Von einer *Auskunft* sprechen wir dann, wenn die gewünschten Informationen mittelbar, d. h. durch Zwischenschalten eines Dritten, der die inhaltliche Widergabe beeinflussen kann, zugänglich gemacht werden (ein Angestellter teilt die Information mündlich mit oder fertigt einen schriftlichen Auszug an). Meist wird dabei die Information interpretiert gegeben, d. h. in der Weise verändert, daß nur eine Zusammenfassung gegeben wird, eine Inhaltsangabe, oder nur die Art der Information näher bezeichnet wird (z. B. Name, Wohnort, Geburtsdatum statt: Hans Schulze, Regensburg . . .). Eine Auskunft liegt demnach nicht vor, wenn eine EDVA über einen Schnelldrucker die auf einem Magnetband gespeicherten Informationen lediglich ausdruckt, auch wenn dabei Bedienungspersonal tätig werden muß. Beim bloßen Ausdrucken kann nur der Umfang, nicht jedoch der Inhalt der Informationen beeinflußt werden. Eine Auskunft liegt jedoch dann vor, wenn der Ausdruck, für sich genommen, für den Betroffenen unverständlich ist und der Interpretation durch einen Angestellten bedarf.

4.2.2. Ist ein Einsichts- bzw. Auskunftsrecht zweckmäßig?

Grundsätzlich muß dem Betroffenen die Möglichkeit gegeben werden, sich selbst über den Umgang der Informationssysteme mit seinen Individualinformationen zu unterrichten. *Das Einsichtsrecht ist also einem bloßen Auskunftsrecht vorzuziehen.* Sobald allerdings der Betroffene sein Einsichtsrecht nicht sinnvoll nutzen kann, weil er etwa mit einem Computerausdruck nichts anzufangen weiß, muß er das Recht haben, eine Interpretation (Auskunft) zu verlangen.

Ein Einsichtsrecht wird in manchen Fällen nicht zu verwirklichen sein. Bei umfangreichen Informationssammlungen kann es aus technischen oder organisatorischen Gründen praktikabler sein, nur einen Auskunftsanspruch zu gewähren. Eine Einsichtnahme ist weiterhin da nicht möglich, wo zwischen den Individualinformationen des Betroffenen und denen Dritter nicht klar unterschieden werden kann, weil diese fortlaufend miteinander vermengt sind bzw. nebeneinanderstehen. Diese Fragen sind im wesentlichen *Probleme der technischen Realisation* und sollen hier nicht weiter erörtert werden. Es steht zu vermuten, daß der Einsatz von Computern weitgehend ein Einsichtsrecht ermöglichen wird, während bei herkömmlicher manueller Informationsverarbeitung der Aufwand an Zeit und Personal und damit an Kosten zu hoch sein dürfte, zumal wenn umfangreiche Informationssammlungen bestehen. Einsichts- und Auskunftsrechte sind in dreifacher Weise möglich:

— bezüglich des Registers,

— bezüglich des Datenjournals [23]),

— bezüglich des eigentlichen Bestandes an Individualinformationen.

4.2.2.1. Register

Aus dem *Register* kann der einzelne entnehmen, welche IS es überhaupt gibt, wer also grundsätzlich Adressat seiner Ansprüche sein kann. Das Register ist öffentlich; jedermann kann es einsehen. Dies ist ohne Schwierigkeiten möglich. Das Register ist etwa dem Handelsregister vergleichbar; dort wird ebenfalls ein Einsichtsrecht und nicht nur ein Auskunftsrecht gewährt.

4.2.2.2. Datenjournal und Bestand der gespeicherten Individualinformationen

Auch das *Datenjournal* muß dem einzelnen zugänglich sein. Aus dem Datenjournal kann man ersehen, welche Veränderungen der Bestand an Individualinformationen erfahren hat, namentlich, an wen, wann, welche Informationen weitergegeben wurden (Empfänger) bzw. von wem sie ins System ge-

---

[18]) Ähnlich umfassend ist auch § 36 IPA-Entwurf, der (wenn er auch nicht die verschiedenen Phasen der Informationsverarbeitung berücksichtigt) bei jedem Verstoß „gegen eine Vorschrift dieses Gesetzes . . ." einen Schadenersatzanspruch gewährleistet.

[19]) Evers, 21

[20]) ebenso § 36 Abs. 2 IPA-Entwurf; vgl. die Forderung von Simitis (2), 681

[21]) für die entsprechenden Befugnisse bei öffentlichen IS vgl. oben C. IV. 2.1. „Unterrichtungsansprüche"

[22]) Simitis (2), 681 verlangt einen „uneingeschränkten Informationsanspruch".

[23]) zu diesen Begriffen und deren näherer Ausgestaltung s. u. unter „Voraussetzungen einer öffentlichen Kontrolle"

[24]) Simitis (2), 681 führt aus, die Interessen des Betroffenen seien erst dann gewahrt, wenn es möglich ist herauszufinden, wer unzutreffend informiert wurde.

bracht wurden [24]) (Lieferant). Hier ist jedoch besonders darauf zu achten, daß der Betroffene wirklich nur die *ihn* betreffenden Veränderungen erfährt [25]). Unter Umständen wird eine Einsicht dann nicht möglich sein, wenn etwa in einem Buch oder auf einem Ausdruck fortlaufend die aktuellen Veränderungen vermerkt werden. Sieht jemand diese Aufzeichnungen ein, ist nicht gewährleistet, daß er nur die für *ihn* interessanten Aufzeichnungen zur Kenntnis nimmt. In der Regel wird deshalb nur ein Auskunftsrecht zugestanden werden können. Ähnlich sieht *§ 5 IPA-Entwurf* auch kein Einsichtsrecht vor, sondern verpflichtet in Absatz 2 den „Leiter der Datenbank, bei jeder neuen Eingabe und bei jeder Entnahme dem Betroffenen eine verbalisierte Darstellung zuzustellen". Diese Regelung ist jedoch in der Praxis wohl kaum durchzuführen. Der Arbeits- und Kostenaufwand würde die übrige Arbeit der Informationssysteme zu sehr beeinträchtigen, ja sogar unmöglich machen. Gangbar erscheint uns folgender Weg: der *Inhalt des Datenjournals, der sich auf den Betroffenen bezieht,* wird dem Betroffenen *jährlich* [26]) zusammen mit dem *Inhalt der zu diesem Zeitpunkt im System gespeicherten Individualinformationen* des Betroffenen *verbalisiert* zugestellt. Wenn das Informationssystem mit einer *EDVA* arbeitet, erscheint uns dieser Aufwand zumutbar zu sein.

Noch einfacher, und für das IS weniger belastend, ist die Möglichkeit, über ein entsprechendes Abfrageprogramm (und entsprechende Datenorganisation, die durch die Kontrolle gewährleistet werden muß) die jeweiligen Individualinformationen (das vorhandene Personenmodell) auszudrucken bzw. auf Bildschirm sichtbar zu machen. Gelingt der Nachweis der legitimen Informationsermittlung nicht, muß (wieder durch entspr. Programm usw.) auch der Adressatenkreis preisgegeben werden.

Bei *manueller Verarbeitung* jedoch kann wegen des großen Aufwandes diese Verpflichtung nicht auferlegt werden, solange die Kosten dafür dem Informationssystem angelastet werden. Als Ausgleich dafür muß dem Betroffenen allerdings *jederzeit auf eigene Kosten* ein Einsichts- bzw Auskunftsrecht bezüglich seiner vorhandenen Individualinformationen und ggf. deren Veränderung (Eingabe und Weitergabe), wie sie im Datenjournal festgehalten sind, zustehen [27]). Dies gilt sowohl für manuelle Verarbeitung als auch für die Verarbeitung mit Hilfe einer EDVA.

[25]) Bei Informationen, die aus allgemein zugänglichen Quellen stammen und deshalb keinen Verarbeitungsbeschränkungen unterliegen, könnte man daran denken, die Lieferanten und den Empfänger dem Betroffenen nicht zu offenbaren. Mit der Entäußerung dieser Informationen hat sich der Betroffene grundsätzlich *für* eine freie Verarbeitung entschieden. Dementsprechend gering ist auch sein Interesse an den Personen zu bewerten, die solche Informationen weitergeben oder in ein IS einbringen.

[26]) ebenso Simitis (2), 681: dem Betroffenen ist in regelmäßig wiederkehrenden Abständen eine Abschrift der gesammelten Angaben zuzuleiten.

[27]) vgl. Simitis (2), 681: allen Personen, über die Angaben existieren, sind jederzeit sämtliche vorhandenen Informationen offenzulegen.

4.3. Anspruch auf Löschung

Der Betroffene kann — etwa in Wahrnehmung seines Einsichts- bzw. Auskunftsrechts — von der Tatsache Kenntnis erlangen, daß sich eine Information entgegen der in diesem Gutachten entwickelten Grundsätze in einem gewerblichen IS befindet. Dies kann beispielsweise der Fall sein, weil sie *nicht aus allgemein zugänglichen Quellen* stammt oder *nicht mit Zustimmung des Betroffenen* gespeichert wurde.

Das Selbstbestimmungsrecht aus Artikel 2 Abs. 1 GG besagt, daß der einzelne darüber bestimmen kann, wann eine Individualinformation in ein System eingebracht werden darf. Wenn er in diesem Recht übergangen wurde, muß er die Möglichkeit haben, den Vorgang rückgängig zu machen. Das kann nur durch Löschung der Information geschehen.

Es ist nun auch der Fall denkbar, daß der Betroffene die ehemals gegebene *Zustimmung* aus irgendeinem Grunde wieder zurückzieht. Falls dieser Widerruf wirksam ist, was sich nach allgemeinen Grundsätzen beurteilt, ist die betreffende Information ebenfalls ohne Zustimmung gespeichert. Für diesen Fall muß dem Betroffenen gleichfalls ein Löschungsrecht zustehen.

Durch die Löschung setzt der einzelne ein der Speicherung konträrers Recht, die völlige Entfernung der Information aus dem System, durch.

4.4. Anspruch auf Berichtigung

Eine Information, deren sich der Betroffene grundsätzlich begeben will, kann jedoch *inhaltlich falsch* vorliegen; z. B., wenn anstelle des Geburtsdatums „11. 12. 90" das Datum „12. 11. 09" gespeichert ist.

Sein nach Artikel 2 Abs. 1 GG geschütztes Interesse liegt jetzt darin, in einer bestimmten Hinsicht nach außen richtig zu erscheinen. Diesem Interesse wird durch Löschung nicht Rechnung getragen, sondern nur durch Richtigstellung.

Diesen Anspruch berücksichtigt auch bereits der IPA-Entwurf, § 6 Abs. 1. Allerdings setzt jene Regelung voraus, daß der Betroffene eine verbalisierte Darstellung nach § 5 ebd. erhalten hat. Dabei wird übersehen, daß er auch auf andere Weise von der Tatsache Kenntnis erlangt haben kann.

Entgegen § 6 IPA-Entwurf kann weiterhin nicht verlangt werden, daß der Anspruch einer besonderen Begründung bedarf. Dies liefe der Erkenntnis zuwider, daß das Bestimmungsrecht des einzelnen über seine Individualinformationen unbeschränkt ist. Gleiches gilt für den in § 6 ebd. ähnlich geregelten Löschungsanspruch.

4.5. Anspruch auf Ergänzung und Entzerrung

Informationen können nicht nur inhaltlich falsch gespeichert sein. Sie können auch dadurch zu unrichtigen Aussagen führen, daß ein bestimmter Kontext *unvollständig gespeichert* ist. So kann etwa bei einem ehemaligen Mitglied einer radikalen Partei die Tatsache des Austritts fehlen.

Eine ähnliche Situation ergibt sich, wenn eine Information in einen *anderen Zusammenhang* als vorgesehen *gebracht* wird. Dabei handelt es sich um die subtilste Art der Verfälschung, die nur schwer nachzuweisen ist. Sie ist bekannt aus der Praxis geschulter Demagogen, die es verstehen, an der richtigen Stelle die richtige Bemerkung fallen zu lassen. In beiden Fällen stellt sich die Lage für den Betroffenen ähnlich dar wie bei inhaltlich falschen Informationen: Ausschlaggebend kann nur sein, welche Auswirkungen die verfälschte Information zeitigen könnte, wenn sie nach außen gelänge.

Im Falle der Unvollständigkeit muß dem Betroffenen ein *Anspruch auf Ergänzung,* im Falle der Verfälschung durch den Zusammenhang ein *Anspruch auf entzerrende* Darstellung gegeben werden [28]).

4.6. Unterlassungsanspruch

Die Möglichkeit einer Berichtigung, Ergänzung oder Entzerrung allein kann den Betroffenen nicht ausreichend schützen. Er ist nicht vor drohenden künftigen Beeinflussungen gesichert; wenn z. B. eine Detektei oder Auskunftei unberechtigt Individualinformationen weitergegeben hat und konkrete Anhaltspunkte dafür vorliegen, daß sich dieser Fall wiederholen könnte.

Für ähnliche Fälle immaterieller Schädigungen anerkennt auch die Zivilrechtsprechung einen quasinegatorischen Anspruch [29]).

Dieser Anspruch erfaßt auch die unter „sonstiges Recht" des § 823 BGB fallenden Rechte [30]). Zugunsten des einzelnen sollte jedoch nicht der Rechtsprechung die Entscheidung darüber überlassen bleiben, ob das Selbstbestimmungsrecht über Individualinformationen hierunter fällt. Der vorliegende Fall sollte darum durch eine Sondernorm im DSchRecht geregelt werden.

5. Öffentliche Kontrolle, Überwachung [31])

Unter öffentlicher Kontrolle sollen hier die Möglichkeiten verstanden werden, die dem Staat erlauben, die Rechtmäßigkeit der privaten Informationsverarbeitung zu überwachen.

Zuerst wird die Notwendigkeit einer Kontrolle begründet, dann werden die Voraussetzungen für effektive Kontrollmaßnahmen behandelt. Schließlich soll ein Überblick über die vielfältigen Kontrollmaßnahmen gegeben werden.

[28]) vgl. jedoch § 6 Abs. 1 IPA-Entwurf, der nur einen Erweiterungsanspruch vorsieht
[29]) Palandt - Degenhart, § 1004 N. 1) b
[30]) Palandt - Thomas, Einführung vor § 823 N. 8) a
[31]) vgl. für den öffentlichen Bereich die Ausführungen unter C. X.
[32]) zur institutionellen Absicherung vgl. Simitis (2), 681
[33]) Weitergabe-IS sind per definitionem nur als gewerbliche IS möglich.
[34]) ebenso wie etwa die Banken- und Versicherungsaufsicht, vgl. hierzu etwa Boss, 15

5.1. Notwendigkeit und Ziel

Der einzelne wird bei der Wahrnehmung seiner Rechte oft einer finanzstarken und gut beratenen Organisation gegenüberstehen. Er wird sich in einem längerdauernden Rechtsstreit meistens nicht durchsetzen können.

Des weiteren ist er nicht in der Lage, die Zusammenhänge der Verarbeitung seiner verschiedenen Individualinformationen im System bzw. im Systemverbund zu durchschauen. Er sieht alle Vorgänge nur von der Warte des Außenstehenden. Er ist den Möglichkeiten dieser sozialen Mächte weitgehend ausgeliefert. Um die geschilderten Gefahren zu vermeiden, muß eine Institution [32]) geschaffen werden, die mächtig genug ist, die private Informationsverarbeitung zu überwachen. Das kann nur durch öffentliche Kontrolle geschehen. Zusammengefaßt soll diese öffentliche Kontrolle also folgende Funktionen erfüllen:

— Sie muß die subjektiven Rechte des einzelnen ergänzen, indem sie hilft, Verstöße aufzudecken und zu ahnden.

— Sie wirkt präventiv. Von Anfang an werden Maßnahmen in die Wege geleitet, die Verletzungen der Rechte des einzelnen verhindern sollen.

— Die Kontrollinstanz wacht also eigenständig über die Einhaltung der objektiven DSchNormen.

5.2. Voraussetzungen für effektive Aufsichtsmaßnahmen

Damit eine Aufsicht oder Kontrolle der privaten IV überhaupt möglich ist, müssen die folgenden elementaren Voraussetzungen erfüllt sein:

5.2.1. Die Kontrollinstanz

Prinzipiell bestehen zwei Möglichkeiten, die Aufsicht zu institutionalisieren:

— Die Kontrolle wird schon bestehenden Aufsichtsbehörden übertragen,

— die Kontrolle obliegt einer einheitlichen Institution, etwa einer neu zu schaffenden Bundesbehörde für DSch.

Als bestehende Aufsichtsbehörde kommt für Weitergabe-Informationssysteme nur das *Gewerbeaufsichtsamt* in Frage. Alle Weitergabe-Informationssysteme werden gewerblich betrieben [33]). Das heißt, daß eine Kontrolle durch eine einheitliche Behörde gewährleistet ist. Dadurch wird eine Zersplitterung der Aufsicht vermieden. Aber die Gewerbeaufsicht ist nicht auf den Schutz des einzelnen ausgerichtet [34]). In ihrer bisherigen Ausgestaltung vermag sie deshalb nicht, dem DSch gerecht zu werden. Sie müßte für diesen Bereich neu ausgestaltet werden. Wie unten noch zu zeigen ist, sind auch interne Informationssysteme von einer einheitlichen Behörde zu beaufsichtigen. Es empfiehlt sich, für beide Bereiche eine einheitliche Behörde zu schaffen, da das zu schützende Rechtsgut das gleiche ist. Hier soll diese Bemerkung genügen, weitere Hinweise ergeben sich aus E. III. 3.2.1., wo die Frage der Kontrollinstanz

für interne Informationssysteme erörtert wird. Schließlich bleibt zu erwägen — was hier vorgeschlagen wird — ob nicht private (gewerbliche und innerbetriebliche) und öffentliche Informationssysteme der gleichen Kontrollbehörde unterstellt werden sollten, also dem Bundes- bzw. Landes*informationsamt* (bzw. -hof).

5.2.2. Anzeige- bzw. Anmeldepflicht

Zur Ausübung jeglicher Kontrolle muß bekannt sein, *wer* kontrolliert werden soll. Von der Überwachung sollen *alle* gewerblichen Informationssysteme erfaßt werden [35]). Dazu ist eine generelle *Anzeigepflicht* notwendig, wie sie bereits in § 14 GewO besteht. Die Anzeige hat bei der Kontrollinstanz zu erfolgen. Dort wird ein *Register* [36]) über die angemeldeten Informationssysteme geführt. Es ist öffentlich. Jedermann ist ohne Nachweis eines besonderen Interesses einsichtsberechtigt. Es enthält folgende Angaben:

— Name oder Firma,

— Ort der Niederlassung,

— Zweck, der mit der Informationsverarbeitung verfolgt wird,

— Art und Typ der verwendeten technischen Hilfsmittel,

— Verzeichnis über Art und Inhalt der verwendeten Programme,

— Art und Umfang der Datensicherungsmaßnahmen.

Der Zweck der Informationsverarbeitung muß angegeben werden, damit die Kontrollinstanz in der Lage ist, die personelle und technische Organisation des Unternehmens zu beurteilen. Um die Kontrolle auch in technischer Hinsicht vornehmen zu können, etwa bezüglich der Verarbeitung durch automatisierte Systeme, müssen auch die verwendeten technischen Hilfsmittel bekannt sein; z. B. hard- und software einer EDVA. Da die praktische Durchsetzung der Datenschutznormen in erster Linie durch Datensicherungsmaßnahmen geschieht [37]), sind diese ebenfalls zu Überwachungszwecken im Register anzugeben. Das Programmverzeichnis erlaubt eine Beurteilung der Informationsströme im System, das Register muß entsprechende Angaben aufweisen bzw. Hinweise auf ein gesondertes *Programmbuch* geben.

5.2.3. Datenjournal

Eine Eigenart *automatisierter Informationssysteme* besteht in der Undurchschaubarkeit interner Vorgänge für Außenstehende. Um auch hier Transparenz herbeizuführen, müssen Unternehmen, die sich der EDV bedienen, ein *Datenjournal* führen, nicht also Unternehmen, die Informationen manuell verarbeiten. Bei letzteren wäre der Aufwand unzumutbar. Das Datenjournal muß [38]) folgende Angaben enthalten:

— Name und Anschrift jeder Person, an die Informationen weitergegeben wurden, bzw. die Informationen an das System abgegeben hat,

— Datum der Weitergabe bzw. Speicherung,

— Inhalt der weitergegebenen bzw. gespeicherten Informationen.

Durch diese Angaben werden die rechtlich relevanten Vorgänge des Einbringens ins System und der Weitergabe erhellt. Auch der IPA-Entwurf sieht in § 3 das Führen eines Datenjournals vor. Abweichend von der hier vorgeschlagenen Ausgestaltung wird nicht die Quelle angegeben, aus der Informationen ins System gelangt sind. Ebenso fehlt die Art der eingespeicherten Information. Beides ist jedoch zur Kontrolle seitens des Betroffenen und der Kontrollinstanz notwendig. Nur so kann der Informationsfluß vollständig durchschaut werden.

Die im angegebenen Entwurf geforderte Zweckangabe kann im Rahmen des Datenjournals entfallen. Hier werden nur abgelaufene Vorgänge protokolliert. Die Angabe des Verarbeitungszwecks wird in Zusammenhang mit der Zustimmung durch den Betroffenen relevant, wo es um die Entscheidung geht, ob überhaupt weitergegeben oder gespeichert werden darf. Das Datenjournal gewährt nur beschränkt Einsicht [39]).

5.3. Kontrollmaßnahmen

Um der Kontrollinstanz Durchsetzungskraft zu verleihen, muß ihr ein Katalog von Maßnahmen an die Hand gegeben werden.

5.3.1. Genehmigung

Gefahrtragende Anlagen und Unternehmen unterliegen weitgehend einer besonderen Genehmigungspflicht. Diese Genehmigung kann sich einerseits auf die Zulassung zum Geschäftsbetrieb beziehen, wie Errichtung gefährlicher Anlagen, §§ 16 ff. GewO, und Genehmigung von Gewerbetreibenden, §§ 30 ff. GewO. Andererseits kann die Genehmigung zur Vornahme bestimmter Geschäftshandlungen denkbar sein, z. B. § 34 b Abs. 8 Nr. 1 c GewO. Die Genehmigung ist eine der tragenden Maßnahmen des Aufsichtsrechts. Dementsprechend ist auch die Genehmigung gewerblicher Informationssysteme vorzusehen. Die Genehmigung erhält ihren Sinn nicht zuletzt dadurch, daß die Zulassung eines IS von bestimmten *Auflagen* abhängig gemacht werden kann.

5.3.1.1. Zulassung eines Informationssystems

Die Gefährlichkeit von Informationssystemen entspricht nicht der Anlage an sich (vgl. §§ 16 ff. GewO), sondern der Verarbeitung von Informationen. Damit wären Regelungen entsprechend §§ 30 ff. GewO angebracht, die an die *Person des Gewerbetreibenden* und gleichzeitig an die Durchführung des Geschäftsbetriebes anknüpfen. Die Genehmigung bezieht sich auf:

---

[35]) vgl. IPA-Entwurf §§ 1, 2, der jedoch den Kreis der meldepflichtigen Systeme modifiziert

[36]) zum Register und dem Umfang der notwendigen Angaben vgl. Simitis (2), 681

[37]) dazu s. Teil B, Exkurs II

[38]) auch Simitis fordert eine exakte Protokollierungspflicht, (2), 681

[39]) siehe oben 4.2.2.2.

— Die personelle Organisation (persönliche und vom jeweiligen System abhängige fachliche Eignung der Mitarbeiter).

— Die technische Organisation (Thesaurus, Programme, Datensicherungsvorkehrungen).

Im Rahmen dieser Genehmigung können auf das Informationssystem zugeschnittene individuelle Auflagen gemacht werden. Wenn diese Voraussetzungen nicht (mehr) vorliegen, kann die Genehmigung versagt (zurückgenommen) werden.

5.3.1.2. Genehmigung bestimmter Geschäftshandlungen

Die oben, 3.4.1., dargestellten Fälle des Verkaufs von ganzen Informationssystemen sollen aufgrund ihrer besonderen Bedeutung unter die Voraussetzung der Genehmigung gestellt werden. Im Falle eines reinen Inhaberwechsels ohne Zweckänderung des Systems ist die Genehmigung ohne weiteres zu erteilen.

Die drei anderen Fälle der Zweckänderung bei Inhaberwechsel und des Verkaufs an ein anderes Informationssystem mit und ohne Zweckänderung führen zur Überprüfung nach den oben entwickelten Kriterien. Darüber hinaus besteht bei diesen Arten des Verkaufs von Informationssystemen die Gefahr, daß die Individualinformationen Verknüpfungsmöglichkeiten und Beziehungen entstehen lassen, die der einzelne nicht mehr zu überblicken vermag. Es dürfen keine Informationszusammenballungen entstehen, die ein umfassendes Personenmodell des Betroffenen ermöglichen. Die Beurteilung einer derartigen Gefahrenlage kann an sich nur der einzelne leisten. Ihm fehlen jedoch dazu die notwendigen Kenntnisse und technischen Möglichkeiten. Deswegen muß diese Aufgabe von der Kontrollinstanz übernommen werden.

Trotzdem bleibt dem einzelnen sein Recht unbenommen, selbst über seine Individualinformationen zu bestimmen, da er nach Erteilung der Genehmigung vom Verkauf benachrichtigt wird.

5.3.2. Überwachung von Verarbeitungsprogrammen und Datensicherungsmaßnahmen

Die Kontrolle der Behörde darf sich nicht nur auf den Zeitpunkt der Genehmigung beschränken, sondern muß sich auch auf den Geschäftsbetrieb, also auf die gesamte Informationsverarbeitung erstrekken. Das hat zur Folge, daß die Kontrollinstanz sämtliche Arbeitsgänge nachvollziehen *können* muß, was besonders bei Verbundsystemen Voraussetzung dafür ist, daß die Verarbeitung transparent gemacht werden kann. Sonst würde die Kontrolle leerlaufen.

Zuerst bedürfen die *Datensicherungsmaßnahmen* als Konkretisierung der Datenschutznormen ständiger Überwachung, da sie bereits für die Genehmigung vorausgesetzt werden und speziell auf die Gefahren des betreffenden IS zugeschnitten sind. Eine wichtige Komponente der Datensicherung sind die *Sicherungsprogramme*. Sie verhindern sowohl ungewollte Informationsveränderungen als auch unberechtigten Zugriff.

5.3.3. Unterstützung von Einzelrechten

Der einzelne hat zwar dem Informationssystem gegenüber relativ umfassende Ansprüche. Gibt jedoch das Informationssystem diesen Ansprüchen nicht statt, ist er auf den unerquicklichen, langwierigen Rechtsweg angewiesen. Wie bereits im IPA-Entwurf, § 6 Abs. 2, 4, vorgeschlagen wurde, besteht ein Ausweg darin, daß sich der Betroffene an die Kontrollinstanz zur Wahrnehmung seiner Rechte wenden kann. Diese muß zu seiner Unterstützung Anordnungen treffen können, die geeignet sind, Mißstände, die nach Maßgabe eines Datenschutzgesetzes Beeinträchtigungen der Rechte der Betroffenen darstellen, zu beseitigen. Sie muß zur Wahrnehmung der berechtigten Interessen des Betroffenen auf dem Verwaltungswege tätig werden können, etwa indem sie nach Zurücknahme der Einwilligung die Löschung von Individualinformationen verfügt.

5.3.4. Einsichtsrecht der Kontrollinstanz

Um ihren Aufgaben und Zielen gerecht werden zu können, muß die Kontrollinstanz die gesamte Informationsverarbeitung durchschauen können. Das bedeutet, ihr muß ein umfassendes Einsichtsrecht zustehen. Das Einsichtsrecht gewährleistet eine objektive Beurteilung der privaten Informationsverarbeitung. Ein bloßes Auskunftsrecht kann wegen seiner subjektiven Komponente — der Interpretation durch das Informationssystem — nicht genügen. Das Einsichtsrecht der Kontrollinstanz muß sich darauf erstrecken, von wem Individualinformationen zu wem gelangen *(Informationsfluß)*. Weiterhin interessieren die tatsächlich vorhandenen Informationen *(Informationsbestand)* und die software, mit deren Hilfe die Informationen verarbeitet werden *(Programme)*, sowie die *Datensicherungsmaßnahmen*.

5.3.4.1. Informationsfluß

Diesbezügliche Angaben sind im Datenjournal enthalten. Die unbeschränkte Einsichtnahme ins Datenjournal eröffnet der Kontrollinstanz auch eine unbeschränkte Kenntnis von Individualinformationen. Aus diesem Grunde ist es unerläßlich, die Bediensteten zur *Verschwiegenheit* zu verpflichten, vgl. § 9 KWG.

5.3.4.2. Informationsbestand

Auf den ersten Blick scheint es unnötig, die Kontrolle auf den Datenbestand auszudehnen, da die einzelne Information nur vom Betroffenen beurteilt werden kann.

Wenn jedoch ein Informationssystem dem berechtigten Anspruch des Betroffenen nicht entspricht und sich dieser an die Kontrollinstanz wendet [40]), muß diese auch in Einzelinformationen einsehen können. Das ist außerdem im Rahmen der Programmüberwachung notwendig, da Programmtests mit den vorhandenen Informationen möglich sein müssen.

5.3.4.3. Programme und Datensicherungsmaßnahmen

Zur Durchführung von Programmtests und der Programmüberwachung ist ein Einsichtsrecht in Programme Voraussetzung. Diese müssen entsprechend

gestaltet sein. Darum sind auch hier nach den Bedürfnissen der Kontrollbehörde standardisierte Programmbeschreibungen vorzusehen, deren Übereinstimmung durch Stichproben (Testläufe) nachzuprüfen ist.

6. Strafnormen

Sämtliche DschVorschriften sind nur dann sinnvoll, wenn sie auch strafrechtlich abgesichert sind. Eine derartige Absicherung würde auch der Tatsache entsprechen, daß die meisten Verletzungen der Persönlichkeit, wie Geheimnisbruch, Ehr- und Verschwiegenheitsverletzung sowie Veruntreuung und bestimmte Indiskretionen, strafbewehrt sind; vgl. etwa §§ 169, 185 ff., 298 bis 300 StGB.

Das schutzwürdige Rechtsgut der freien Selbstbestimmung über Individualinformationen läßt sich in folgende Regelungskomplexe unterteilen, die durch Strafandrohung zu schützen sind:

— das rechtswidrige Speichern und Weitergeben von Individualinformationen,

— das Abgeben an Dritte, ohne selbst die Informationen zu verarbeiten,

— die Vernachlässigung von Datensicherungsmaßnahmen.

6.1. Datensicherungsmaßnahmen

Es sind zwei Fälle des Verstoßes gegen Datensicherungsmaßnahmen denkbar:

a) Die durch Gesetz oder als Auflagen der Kontrollinstanzvorgeschriebenen Maßnahmen werden nicht in vollem Umfang oder gar nicht erfüllt.

b) Jemand umgeht vorhandene Datensicherungsmaßnahmen, um sie sich oder anderen zugänglich zu machen oder sie ins System einzubringen.

Der Unterschied besteht also darin, daß es sich in Fall a) um die Verhinderung vorgeschriebener, in Fall b) um das Umgehen vorhandener Datensicherungsmaßnahmen handelt. Zu dem objektiven Tatbestandsmerkmal des Falles b) tritt noch die subjektive Komponente der Absicht, sich oder anderen die Informationen zugänglich zu machen oder sie ins System einzubringen. Damit soll ausgeschlossen werden, daß jemand bestraft wird, der Sicherungsmaßnahmen umgeht, ohne die dadurch erlangten Informationen rechtswidrig verwenden zu wollen. Datensicherungsmaßnahmen bezwecken nämlich den Schutz der Information [41]), sind dagegen kein Selbstzweck.

6.2. Unberechtigtes Erfassen und Speichern von Individualinformationen und das Zugänglichmachen gegenüber Dritten

Es sollen Tatbestände pönalisiert werden, die gegen DSchNormen verstoßen und direkt Auswirkungen auf den einzelnen zeitigen können. Die Erfüllung eines solchen Tatbestandes kann gleichzeitig einen Verstoß gegen Datensicherungsmaßnahmen beinhalten, jedoch muß das nicht immer der Fall sein. Gerade im letzteren Fall ergibt sich die Notwendigkeit solcher weitergehenden Vorschriften.
Beispiele:

— Der Inhaber/Benutzer eines IS oder einer der Angestellten geben unberechtigterweise Individualinformationen an Dritte weiter. Diese Weitergabe kann sowohl über Programm im Datenverband als auch durch Austausch einer Karteikarte geschehen.

— Ein Angestellter macht einem Dritten die Informationen auf Lochkarten oder einem Plattenspeicher zugänglich.

Verschwiegenheitspflicht

Die Norm statuiert damit auch die Verschwiegenheitspflicht der Angestellten des Informationssystems.

Die Strafbestimmungen müssen nach der Intention dieses Gutachtens konsequenterweise *auch nichtautomatisierte Informationsverarbeitung* erfassen. Das ist bisher, z. B. für Auskunfteien, nicht der Fall. Eine Ausgestaltung dieser Verschwiegenheitspflicht könnte entsprechend § 300 StGB erfolgen.

6.3. Strafrahmen

Der Strafrahmen sollte je nach Schwere des Verstoßes Freiheitsentzug von einem bis zu fünf Jahren vorsehen.

Für weniger gravierende Fälle, etwa Verstöße gegen Verfügungen der Kontrollinstanz, müßten angemessene Geldbußen vorgesehen werden. Angemessen sind sie dann, wenn sie in einer erheblichen Relation zum Jahresumsatz stehen.

[40]) vgl. § 6 Abs. 2 IPA-Entwurf
[41]) Steinmüller (1), 87

III. Informationssysteme zur internen zweckgebundenen Verarbeitung („Innerbetriebliche Informationssysteme") — Konsequenzen für den Gesetzgeber

Die unter diesen Begriff fallenden Informationssysteme weisen eine große Vielfalt auf.

Die internen zweckgebundenen Informationssysteme, im folgenden der Kürze halber nur „interne oder innerbetriebliche IS" genannt, spielen wahrscheinlich gesellschaftlich eine noch bedeutendere Rolle als die gewerblichen Informationssysteme [1]). Man bedenke nur, wie viele Berufssparten (Ärzte, Anwälte), Vereine und Verbände (Arbeitgeberverband, Gewerkschaften, Parteien) sich derartiger Systeme bedienen. Vor allem kommt kein Wirtschaftsunternehmen ohne ein internes Informationssystem aus.

In vielen Fällen — etwa im Verhältnis Arbeitgeber—Arbeitnehmer — hat der Betroffene eine relativ schwache Position. Er befindet sich in einem Abhängigkeitsverhältnis zum Arbeitgeber, verstärkt durch das Betriebs-Informationssystem. Das bedeutet, daß das Informationssystem nicht nur durch ein Personenmodell Macht über den einzelnen ausüben kann, sondern auch besonders durch Machtmittel, die sich aus dem besonderen Kontaktverhältnis zum Betroffenen ergeben. Solche Mittel sind etwa Gehaltsrückstufung, Versagen einer Beförderung, Kündigung; Versagen eines Versicherungsschutzes, faktischer Ausschluß aus Vereinen oder privaten Schulen; Weitergabe schwarzer Listen an andere Unternehmen, usf.

Hier nützt es dem einzelnen wenig, wenn er seine Rechte im wesentlichen selbst ausgestalten darf (durch das Erfordernis der Zustimmung zur Verarbeitung und die einzelnen eigenen Ansprüche), da in der Regel der sozial Mächtigere ihm den Verzicht auf seine Rechte abringen kann. Das bedeutet, daß die *Ansprüche des einzelnen nur im Rahmen der Normen ihre Wirkung entfalten können, die die Informationsverarbeitung einschränken, ohne daß der Betroffene auf die Beschränkung Einfluß nehmen kann.* Diese Auffassung entspricht der Betrachtungsweise, wie sie im Arbeitsrecht [2]) im Laufe der Jahre entwickelt hat.

Da den Arbeitgeber-Informationssystemen aufgrund der sozialpolitischen Bedeutung des Arbeitgeber-/Arbeitnehmer-Verhältnisses eine Sonderstellung zukommt, soll in den folgenden Ausführungen jeweils auf die damit verbundenen Fragen eingegangen werden.

[1]) Dies meint auch Simitis (2), 675, wenn er sagt, die spätindustrielle Gesellschaft kenne keine Privatheit mehr; sie breche die Privatsphäre durch ihre ökonomischen Strukturen auf und zerlege sie in eine Summe marktstrategisch wichtiger Daten.

[2]) vgl. Hueck - Nipperdey, 409

1. Gesetzliche Einschränkungen der Informationsverarbeitung

Das weitere Vorgehen erfolgt entsprechend dem 2. Unterabschnitt. Dabei werden die grundsätzlichen Erkenntnisse, die im Vorhergehenden gewonnen wurden, vorausgesetzt. Ausführlich erörtert werden nur die auftretenden Unterschiede, die sich aus den besonderen Voraussetzungen innerbetrieblicher Informationssysteme ergeben.

1.1. Ermittlung

Die Kriterien für die Feststellung der Regelungsbedürftigkeit der Informationsermittlung sind die gleichen wie im Bereich der gewerblichen Informationssysteme. Ausschlaggebend ist die Abwägung der geschützten Interessen der am tatsächlich bestehenden Verhältnis Beteiligten. Damit stellt sich auch hier die Frage, wann eine Interessenkollision eintritt und wie weit der Freiheitsbereich des Informationsverarbeitenden gegenüber der freien Selbstbestimmung des Betroffenen reichen kann.

Eine Besonderheit innerbetrieblicher Informationssysteme liegt, wie oben ausgeführt, darin, daß die Auswahl der verarbeitenden Informationen durch den Rahmen der Beziehungen zwischen den Beteiligten bestimmt ist. Indem etwa der einzelne zum Arzt geht und dort seine Personalien angibt, weil er die Notwendigkeit dazu erkennt, begibt er sich dieser Individualinformationen. Noch weitgehender sind die Auskünfte, die eine Krankenanstalt im Rahmen der Anamnese erhält. Auch dabei gibt der Patient freiwillig diese Informationen ab. Er setzt dabei jedoch stillschweigend voraus, daß seine Krankheitsgeschichte und alle weiteren Auskünfte für die bevorstehende Behandlung *notwendig* sind. Erst recht gilt das für — u. U. außerordentlich weitgehende — psychologische oder graphologische Tests und ihre Ergebnisse. Betroffener und Verarbeitender haben damit ausdrücklich oder konkludent eine Übereinkunft hinsichtlich der *notwendigen Informationen* geschlossen.

Die Ermittlung dieser Informationen — und damit auch die Auswahl — erfolgt also bereits im Hinblick auf den gemeinsamen *angestrebten Zweck,* also für einen eng begrenzten Benutzerkreis (pragmatische Ebene). Damit verbunden ist auch die Tatsache, daß derjenige, der die Informationen sammelt, direkt an der Person des Betroffenen interessiert ist. Wenn er die Information erhält, können sich von diesem Augenblick an Auswirkungen auf den Betroffenen ergeben.

Diese Tatsache wird wohl auf keinem Gebiet so deutlich wie im Arbeitgeber-/Arbeitnehmerverhältnis. Die Nachforschungen eines Vorgesetzten führen *unmittelbar* zu einer Beurteilung des Betroffenen.

Im Gegensatz zu gewerblichen Informationssystemen ergibt sich damit folgendes: Die Interessenkollision und die Geltendmachung des Rechts auf freie Selbstbestimmung des einzelnen werden bereits zum Zeitpunkt der Ermittlung akut. Durch Eintritt in das gegenseitige Kontaktverhältnis und die damit verbundene informationelle Öffnung nach außen begibt sich der Betroffene bereits eines Teils seiner Individualinformationen, nämlich derjenigen, die sein Partner im betreffenden Rahmen benötigt. Das hat zur Folge, daß der Inhaber des Informationssystems die notwendigen Informationen *auch ohne ausdrückliche Zustimmung des Betroffenen ermitteln kann.*

Wie bei gewerblichen Informationssystemen können ebenfalls die aus *allgemein zugänglichen Quellen* stammenden oder dort erhältlichen Informationen verarbeitet werden, ferner diejenigen, deren sich der Betroffene selber begeben hat, indem er sie einer unbestimmten Öffentlichkeit zugänglich machte, z. B. durch Angabe gegenüber einem biographischen Institut.

1.1.1.

Hinsichtlich der Frage, *ob sich der Betroffene* darüber hinaus *weiterer Individualinformationen durch Zustimmung begeben kann,* stellt sich ein besonderes Problem: In den meisten Fällen befindet sich der einzelne in einer *faktischen Zwangssituation.* Sein Gegenüber in dem Kontaktverhältnis ist ihm regelmäßig finanziell und wissensmäßig überlegen. Außerdem gibt es, bis auf die Fälle der Inanspruchnahme einer Dienstleistung, kaum eine Möglichkeit für den Betroffenen, einer solchen Situation zu entgehen, da er sich ihr immer wieder gegenübergestellt sieht. Auch diese Tatsache wird in einem Anstellungsverhältnis am deutlichsten. Der Arbeitnehmer sieht sich dem (den) Arbeitgeber(n) relativ hilflos gegenüber. Dem kann er sich nicht widersetzen; er muß sich den Wünschen beugen [3]).

Aus diesen Gründen kann eine über die notwendigen Informationen hinausgehende Verarbeitung auch mit Zustimmung *nicht möglich* sein.

1.1.2.

Ein weiteres Problem ist die *Festlegung des* zur Ermittlung *erlaubten Rahmens* von Informationen. Er kann nicht abstrakt bestimmt werden. So hängt z. B. die Art der benötigten Informationen für einen Anwalt vom jeweiligen Fall ab; ein Arbeitgeber braucht je nach Art der zu verrichtenden Arbeit unterschiedliche Informationen. Eine Regelung, die sämtliche denkbaren Fälle umfaßt, ist nicht möglich. Die Prüfung, ob in einem konkreten Fall der Rahmen der notwendigen Informationen überschritten ist, muß daher *den Gerichten überlassen* werden, wenn sich die Partner nicht einigen können.

Eine Ausnahme ergibt sich auf arbeitsrechtlichem Gebiet:

Wie bereits mehrmals angesprochen, bieten sich im Verhältnis Arbeitgeber/Arbeitnehmer die größten Probleme [4]).

Dem Betroffenen kann durch einmal bekanntgewordene, für ihn abträgliche Individualinformationen ein für allemal die Karriere verbaut sein [5]).

Die bereits erwähnte faktische Zwangssituation führt auf seiten des Arbeitnehmers häufig zum Nachgeben gegenüber dem Arbeitgeber [6]), so daß er „freiwillig, unfreiwillig" Informationen über den notwendigen Rahmen hinaus abgibt.

In dieser Situation ist der einzelne hilflos. Der langwierige und für ihn oft unsichere Rechtsweg ist ihm kaum zuzumuten, zumindest trägt er nicht seinem Rechtsschutzbedürfnis ausreichend Rechnung.

Daher ist für das Gebiet des Arbeitsrechts eine *Lösung durch das Betriebsverfassungs- oder Tarifvertragsrecht* anzustreben. Die von der Ermittlung Betroffenen eines Betriebes oder eines Betriebszweiges müssen mitwirken bei der Festlegung der notwendigen und damit erlaubten Informationen. Eine entsprechende Norm sollte in das Betriebsverfassungsrecht aufgenommen werden. Die Austragung der Auseinandersetzung könnte jedoch auch den Tarifvertragspartnern übertragen werden.

1.1.3.

Schließlich sind noch interne Informationssysteme zu erwähnen, die solche Informationen verarbeiten, welche *gemäß der* vorgenommenen Auslegung der *speziellen Grundrechte,* Artikel 4, 8, 19, grundsätzlich von privater Informationsverarbeitung *ausgeschlossen* sind [7]). Dabei handelt es sich um IS der Religionsgemeinschaften, der Gewerkschaften und ähnlicher Verbände sowie der politischen Parteien. Sie dürfen, soweit sie überhaupt zulässig sind (politische IS!), die für ihren Bereich notwendigen Informationen ebenfalls ohne ausdrückliche Zustimmung des Betroffenen ermitteln. Denn die stillschweigende Zustimmung ist zu vermuten und müßte ausdrücklich verweigert werden.

1.1.4.

Nach den oben dargelegten Kriterien wird die Erlaubnis bzw. das Verbot der Informationsermittlung

---

[3]) Da die deutschsprachige Literatur speziell zu dieser Problematik sehr spärlich ist, beziehen wir uns im folgenden hauptsächlich auf die Ausführungen bei Kamlah (1), 51 ff., 182 f.; er beschreibt zwar die amerikanische Situation, doch dürften die Fakten auch auf die deutsche Wirtschaft zutreffen, ebd., 52.

[4]) ebd., 51 ff.

[5]) Dies besonders angesichts der Tatsache — die jedoch vielfach geleugnet wird —, daß Informationen über den Arbeitnehmer von Arbeitgeber zu Arbeitgeber weitergereicht werden. Zu dem Problem erfolgen jedoch eingehende Erörterungen unten, 1.5.

[6]) Kamlah (1), 182

[7]) vgl. o. 1.1. und 1.2.1.

statuiert. Nicht jedoch werden *Art und Weise der Ermittlung* [8]) erfaßt. In gleichem Maße wie bei gewerblichen Informationssystemen sind auch hier die geschilderten „Entartungserscheinungen" der Ermittlung möglich. Für sie gelten grundsätzlich die a. a. O. gemachten Ausführungen.

1.2. Erfassung/Speicherung

Die Aufeinanderfolge der Informationsverarbeitungs-Phasen Ermittlung, Erfassung/Speicherung und Weitergabe haben zur Folge, daß die Regelung der früheren auch eine — zumindest weitgehende — Regelung der nachfolgenden Phase(n) bedeutet. Somit wird durch die Vorschriften hinsichtlich der Ermittlung auch die Erfassung bzw. Speicherung (Einbringen ins Informationssystem) erfaßt. Die Regelung soll darum, wie bei der öffentlichen Informationsverarbeitung, möglichst weit vorverlegt werden. Zwar kann nicht gesagt werden, daß die erlaubte Ermittlung auch die Erlaubnis von Erfassung und Speicherung notwendig impliziert, doch die zum Zeitpunkt der Ermittlung angesetzten Regelungen bewirken bereits, daß keine Informationen unerlaubt gespeichert werden dürfen. Dies wird dadurch erreicht, daß die mit der Ermittlung verbundene *Auswahl* der zur Erfassung vorgesehenen Informationen unter die DSchRegelungen fällt: Nur notwendige Informationen sollen durch die vorgesehene Einschränkung der Ermittlung erfaßt und gespeichert werden können.

Neue Konsequenzen für eine Regelung ergeben sich erst, wenn eine weitere Phase der Informationsverarbeitung Außenwirkung zeitigt. Das ist erst mit der Weitergabe der Fall.

Hier muß eine Beschränkung entsprechend der öffentlichen Informationsverarbeitung gefunden werden. Notwendig ist darum die Ermittlung der Minimal- und der (verhältnismäßigen) Unterstützungs-Informationen, die sich im Rahmen des Kontaktverhältnisses bewegen. (So wäre etwa die Speicherung von Informationen über die politische Betätigung von Chemiestudenten durch die BASF [im Hinblick auf künftige Mitarbeiter] aus mehr als einem Grunde rechtswidrig.)

Damit die Individualinformationen sich nicht unbegrenzte Zeit in einem Informationssystem befinden, müssen sie grundsätzlich *nach Ablauf von 10 Jahren* [9]) *gelöscht* werden. Diese Zeit muß ausreichen, den Inhaber des Systems von Rückfragen, Rückabwicklungen u. ä. abzusichern. Lag ein Arbeitsverhältnis vor, sind die Informationen ein Jahr nach dessen Beendigung zu löschen. Eine längerdauernde Speicherung ist nur im Rahmen von fortdauernden Rechtsbeziehungen (Wettbewerbsklausel, Schadenersatzansprüche) zu rechtfertigen. Die Löschung der Informationen kann im Gegensatz zu gewerblichen Informationssystemen hier deshalb verlangt werden, weil sie nach Beendigung des Verhältnisses normalerweise nicht mehr notwendig sind.

[8]) s. o. 3.1.1.

[9]) entspr. § 44 b HGB

1.3. Veränderung

Die denkbaren Fälle der Informationsveränderung sind die gleichen wie bei Weitergabe-Informationssystemen. Sie sind auch entsprechend zu beurteilen.

1.4. Löschung

Ein Recht *auf* Löschung (= gegen Speicherung) wurde bereits unter 1.2.1. erörtert.

Zum Recht *gegen* Löschung gilt dasselbe wie bei den gewerblichen Informationssystemen ausgeführt: Es ist ein Teilnahmerecht, da es einem *Recht auf Speicherung* entspricht und fällt daher nicht unter die Datenschutzproblematik.

1.5. Weitergabe

Oben wurde bereits ausgeführt, daß interne Informationssysteme durch die Benutzer- bzw. Zweckbestimmung der Informationen gekennzeichnet sind. Der Zweck wiederum bestimmt sich aus dem Rahmenverhältnis, das zwischen den Beteiligten besteht. *Die Informationsverarbeitung von internen Informationssystemen wird also ganz in den Dienst des gemeinsam verfolgten Zieles gestellt.*

Die Folge dieser Auffassung war, daß die Informationen nach Beendigung des Verhältnisses entweder nach einem kurzen oder längeren Zeitraum (7 bzw. 10 Jahre) gelöscht werden müssen. Wenn man diese Voraussetzungen akzeptiert, muß konsequenterweise statuiert werden, daß grundsätzlich die *Weitergabe von Individualinformationen aus innerbetrieblichen Informationssystemen an Dritte nicht erlaubt* sein darf. Wenn selbst der ehemalige Partner die Informationen nach Beendigung des Verhältnisses zu löschen hat, können sie erst recht nicht aus dem bestehenden Verhältnis heraus weitergegeben werden.

1.5.1.

Diese Schlußfolgerung stößt jedoch auf einige *Bedenken* hinsichtlich bestimmter Sonderfälle:

Es ist fraglich, ob ein Konzern (wie etwa Neckermann) die Informationen seiner Kunden nicht an das eigene, wenn auch organisatorisch unabhängige, Kreditinstitut weitergeben darf. Weiterhin gibt es den Fall, daß Unternehmen Lohn- u. a. Berechnungen von einer außenstehenden Stelle vornehmen lassen. Gleiches gilt für Ärzte, die ihre Abrechnungen von einer Zentrale erledigen lassen, für Steuerbevollmächtigte bei der DATEV usf. Die erwähnten Fälle unterscheiden sich von etwa der Informationsweitergabe unter Arbeitgebern dadurch, daß der Betroffene in der Regel von diesem Umstand weiß, wenn er sich in das betreffende Kontaktverhältnis begibt. In solchen Fällen muß die Einwilligung in das Verhältnis als vermutete Zustimmung zur Weitergabe aufgefaßt werden. Auf jeden Fall muß eine Abgabe von Informationen in der beschriebenen Weise unter den Vorbehalt der — zumindest konkludenten — Zustimmung des Be-

troffenen gestellt werden. Zustimmung ist leichter in Fällen anzunehmen, in denen nur Berechnungen anhand vorhandener Informationen durch einen Dienstleistungsbetrieb vorgenommen werden. Das betreffende Unternehmen ist nicht an dem Inhalt der Informationen interessiert. Insofern ist nur für ausreichende Diskretion des Personals zu sorgen, um dem Schutzinteresse des Betroffenen bezüglich seiner Individualinformationen Rechnung zu tragen. Dagegen kann die Abgabe von Informationen an Konzerntöchter oder Zweigbetriebe *nur unter ausdrücklicher Zustimmung* des Betroffenen geschehen [10]). Dabei kann es sich nämlich ohne weiteres um die Einbringung der Information in einen völlig anderen Rahmen handeln als er zwischen den Beteiligten ursprünglich bestanden hat. Dafür ist das Beispiel des konzerneigenen Kreditinstituts sehr anschaulich. Hier ist *nicht* anzunehmen, daß sich der Betroffene darüber im klaren ist, daß seine Individualinformationen bei Kreditaufnahme weitergegeben werden und welche Tragweite diesem Vorgang innewohnt.

1.5.2.

Während der *Verkauf ganzer Informationssysteme* bei gewerblichen Informationssystemen ein Problem darstellte, kann er bei der Regelung interner Informationssysteme unberücksichtigt bleiben.

Da die hier behandelten Informationssysteme als Hilfsmittel zu Optimierung innerbetrieblicher Vorgänge eingesetzt werden, ist ein Verkauf unabhängig vom Unternehmen kaum denkbar, jedenfalls aber — a maiore zur Weitergabe von Einzelinformationen — verboten. Wenn jedoch ein ganzes Unternehmen in andere Hände übergeht, ändert sich nichts an der Beziehung zwischen Informationssystemen und Individualinformation bzw. Betroffenem. Wenn Karteien oder Dateien unabhängig an Interessenten weitergegeben werden, handelt es sich um eine Menge von Einzelweitergaben, die entsprechend zu behandeln sind.

1.5.3.

Das Verbot der Weitergabe von Individualinformationen ohne Zustimmung des Betroffenen gilt insbesondere für Informationssysteme, die (als *Ausnahmefälle*) speziell grundrechtlich geschützte Informationen verarbeiten. Ihnen wurde das Recht zur Verarbeitung aufgrund der Tatsache zuerkannt, daß sie Informationen für ihren durch die gleichen Grundrechte geschützten Bereich benötigen. Von dieser Ausnahme kann jedoch die Weitergabe an Dritte, Außenstehende, nicht mehr gedeckt werden.

[10]) im Ergebnis wohl auch OLG Karlsruhe, Zivilsenat Freiburg, in: NJW 1971, 1042

[11]) Gros, G II

[12]) Entwurf vom 18. Dezember 1970, Bundesratsdrucksache Nr. 715/70

[13]) ebenso in § 37 Abs. 1 des IPA-Vorentwurfs; im IPA-Entwurf ist ein Einsichtsrecht jedoch nicht mehr enthalten

2. Erweiterter Rechtsschutz des einzelnen

Anders als bei den gewerblichen Informationssystemen ist ein innerbetriebliches Informationssystem in der Regel nur dann an Individualinformationen interessiert, wenn die Organisation oder das Unternehmen, zu dessen Optimierung das Informationssystem beitragen soll, in einer tatsächlichen oder rechtlichen Beziehung mit dem Betroffenen steht bzw. in eine solche eintreten will.

Als Beispiel seien hier nur die Personalkartei eines Arbeitgebers oder die Mitgliedskartei eines Fußballvereins genannt. Des weiteren ist auf die Ausführungen vor 1. zu verweisen. Die einzelnen Ansprüche, wie sie unter II. 4. ausgeführt wurden, bleiben im übrigen erhalten; es werden nur noch die sich zu Weitergabe-Informationssystemen ergebenden Modifizierungen erörtert.

2.1. Schadenersatz

Der Ersatz des Schadens, auch des immateriellen, ist selbst dann noch zu gewähren, wenn der Schaden durch die Verarbeitung von *notwendigen* Informationen verursacht wurde.

Beispiel: Ein Datum ist zur Berechnung einer Prämie notwendig. Anstatt „14. 10. 1939" wird jedoch ein falsches Datum verarbeitet und daraufhin die Prämie zu niedrig angesetzt. Der entstandene Schaden ist zu ersetzen.

2.2. Einsichts- und Auskunftsrechte

Diese Ansprüche dienen insbesondere dazu, dem einzelnen die Nachprüfung zu ermöglichen, ob wirklich nur die notwendigen Individualinformationen verarbeitet werden. Eine Besonderheit ergibt sich für das *Arbeitsrecht*. Die Stellung des einzelnen Arbeitnehmers bedarf wegen dessen Abhängigkeit vom Arbeitgeber verstärkten Schutzes durch die Vertreter der Arbeitnehmer. Bemerkenswerterweise besteht schon im derzeit geltenden Betriebsverfassungsgesetz ein *Recht des Betriebsrats* auf die Vorlage von Personalunterlagen der Arbeitnehmer und auf Einsicht in deren Personalakten im Rahmen seiner Aufgaben, § 54 Abs. b und § 54 Abs. 2 BetrVerfG [11]). Bislang fehlt allerdings ein allgemeines *Recht des einzelnen auf Einsicht in seine Personalakten*. Eine Änderung scheint sich hier jedoch abzuzeichnen: in den §§ 81 bis 84 des Regierungsentwurfs zur Neufassung des BetrVerfG [12]) ist unter anderem ein Recht auf Einsicht in die Personalakten zu finden [13]). Dies ist im Hinblick auf Artikel 2 Abs. 1 GG unumgänglich.

2.3. Anspruch auf Löschung

Der Löschungsanspruch ist hier wesentlich anders als bei den gewerblichen Informationssystemen auszugestalten. Bestehen bleibt nur, daß Individualinformationen, die aus allgemein zugänglichen Quellen stammen bzw. auch aus solchen erhältlich sind, *nicht* auf Verlangen des Betroffenen *gelöscht* werden müssen. Weiterhin steht dem einzelnen *kein Löschungsanspruch* bezüglich der notwendigen Infor-

mationen zu, solange das Kontaktverhältnis (im Rahmen dessen die Informationen verarbeitet werden) fortbesteht bzw. solange nicht die gesetzte Frist seit Beendigung der Rechtsbeziehungen zwischen einer Organisation, einem Unternehmen usw. und dem Betroffenen verstrichen ist.

Der einzelne hat lediglich *das Recht, die Löschung derjenigen Individualinformationen zu verlangen,* die keine notwendigen Informationen darstellen und nicht aus allgemein zugänglichen Quellen stammen, sofern er seine Zustimmung zur Speicherung nicht erteilt oder zurückgenommen hat.

2.4. Anspruch auf Berichtigung

Der Berichtigungsanspruch muß in vollem Umfange erhalten bleiben. Gerade wenn der einzelne dulden muß, daß gewisse Informationen ohne seine Zustimmung verarbeitet werden, muß er ein Recht darauf haben, falsche Informationen zu berichtigen.

2.5. Anspruch auf Ergänzung und Entzerrung

Für diesen Anspruch, der ja lediglich eine Art von Berichtigungsanspruch bezüglich richtiger Informationen darstellt (die allerdings im falschen oder verfälschenden Zusammenhang verarbeitet werden), gilt das schon unter 2.4. Gesagte. An dieser Stelle soll nochmals hervorgehoben werden, daß diese Berichtigungsansprüche dem einzelnen ein Recht auf Speicherung (man könnte auch sagen: Nicht-Löschung) geben. Ein solches Recht stellt im Grunde einen Anspruch auf wahre und vollständige Speicherung dar. Der Anspruch ist jedoch nur dann praktikabel, wenn seine Verwirklichung dem Betroffenen überlassen bleibt; nur er kann beurteilen, ob verzerrende oder entstellende Informationen über ihn vorliegen.

2.6. Unterlassungsanspruch

Gegenüber den Ausführungen unter II. 4.6. ergeben sich keine Unterschiede.

3. Öffentliche Kontrolle, Überwachung

3.1. Notwendigkeit und Ziel

Bei den gewerblichen Informationssystemen wurde die Notwendigkeit einer öffentlichen Kontrolle einerseits damit begründet, daß für den einzelnen nur sehr schwer ersichtlich sei, in welchen Zusammenhängen die einzelnen Informationen im System und insbesondere beim Systemverbund verarbeitet werden. Dieses Problem stellt sich bei innerbetrieblichen Informationssystemen in gleicher Weise. Der Betroffene kann bei den vielfältigen Verflechtungen innerhalb der Wirtschaft und der Wirtschaft mit dem Staat kaum mehr durchschauen, welchen Bereichen ein internes Informationssystem zugehörig ist; hier sei nur an das in diesem Unterabschnitt unter 1.5. erwähnte Konzernproblem erinnert.

Zum zweiten wurde die Notwendigkeit einer Kontrolle aus finanzieller Unterlegenheit des einzelnen gefolgert, die viele Prozesse gegen finanzkräftige Informationssysteme scheitern läßt. Zudem vermag ein Prozeß, da er nur im Nachhinein die Rechte des einzelnen bestätigen kann, für den konkreten Fall einzelne Verletzungen nicht zu verhindern. Bei internen Informationssystemen tritt nun noch verstärkend hinzu, daß durch die Druckmittel, die diese Informationssysteme als Träger sozialer Macht einsetzen können (Kündigung etc.), der einzelne an der Verfolgung seiner Rechte weitgehend gehindert werden kann.

Dies ist bei einer öffentlichen Kontrolle in weit geringerem Maße zu befürchten.

Die *Ziele* einer solchen Kontrolle sind die gleichen wie sie oben unter D. II., 5.1. aufgeführt wurden.

3.2. Kontrollinstanz als Voraussetzung für effektive Kontrolle

Für die Kontrolle innerbetrieblicher Informationssysteme durch eine öffentliche Kontrollinstanz ergeben sich besondere Schwierigkeiten bei der Frage, wie diese Instanz institutionalisiert werden soll. Die nähere Ausgestaltung der Kontrolle hängt wesentlich von der Antwort auf diese Frage ab.

3.2.1. Die Kontrollinstanz

Eine Kontrollinstanz für innerbetrieblichen Datenschutz kann ebenfalls grundsätzlich auf zwei Wegen institutionalisiert werden:

— die Kontrolle wird schon bestehenden Aufsichtsbehörden zugewiesen (Bankenaufsicht, Versicherungsaufsicht, Gewerbeaufsicht),

— die Kontrolle obliegt einer einheitlichen Institution.

Es erhebt sich nun folgendes Problem: kann man Teilbereiche eines schon unter Kontrolle stehenden Unternehmens oder einer Organisation etc. einer anderen Kontrollinstanz unterstellen? Kann etwa eine Bank neben der bestehenden Aufsicht durch das Bundesaufsichtsamt für Kreditwesen noch durch eine spezielle Kontrollinstanz für Datenschutz überwacht werden?

Im folgenden sollen zuerst Gründe angeführt werden, die für eine Verteilung der staatlichen Kontrolle von privaten IS auf schon bestehende Aufsichtsbehörden sprechen.

3.2.2. Gründe gegen eine einheitliche Kontrollinstanz

a) In der staatlichen Aufsicht über die Privatwirtschaft ist die Tendenz zu beobachten, einheitliche, zusammengehörige Wirtschaftsbereiche auch einer einheitlichen Kontrolle zu unterwerfen. So sollen etwa die Vorschriften des KWG für alle Kreditinstitute gelten [14]). Dies kommt in § 52 Abs. 2 KWG deutlich zum Ausdruck; Absatz 1 gewinnt erst durch diesen zweiten Absatz seine eigentliche Bedeutung. Das bedeutet, daß auch die Datenschutzkontrolle der Aufsichtsbehörde zuzuordnen wäre, die schon bislang die

Aufsicht über den betreffenden Wirtschaftszweig ausübt.

b) Die bestehende Aufsichtsbehörde kennt das zu kontrollierende Objekt infolge der ausgeübten Aufsicht schon und ist mit den besonderen Gegebenheiten — etwa bei Banken — bereits vertraut. Die Beamten beschäftigen sich ohnedies mit Aufsichtsmaßnahmen — wenn auch anderer Art — bezüglich der zu kontrollierenden Objekte.

c) Aufsichtsmaßnahmen gleichen einander grundsätzlich zum großen Teil; man denke an die Genehmigung. Bei verschiedenen Kontrollinstanzen würde u. U. eine Bank auf Grund der Bankenaufsicht und daneben auf Grund einer Datenschutzaufsicht der Zulassung zum Geschäftsbetrieb bedürfen. Eine Zuordnung der Datenschutzkontrolle zur Bankenaufsicht usw. würde hingegen nur eine einzige Genehmigung erfordern.

3.2.3. Gründe für eine einheitliche Kontrollinstanz

a) Die oben schon erwähnte Vorschrift des § 52 Abs. 1 KWG läßt mehrere Aufsichtsbehörden nebeneinander zu. Das gleiche ergibt sich aus § 139 g der Gewerbeordnung: Das Gewerbeaufsichtsamt darf Maßnahmen zur Durchführung von § 62 Abs. 1 HGB anordnen, die auch für Versicherungsunternehmen gelten, obwohl den Gewerbeaufsichtsämtern im übrigen die Aufsicht über Versicherungsunternehmen nicht zusteht. Zum anderen wird die Aufsicht, die sonst den Gewerbeaufsichtsämtern zusteht, von anderen Behörden ausgeübt, § 24 d Satz 3 GewO.

Das besagt, daß von einer Zuordnung aller Aufsichtsmaßnahmen zu den jeweils schon bestehenden Aufsichtsbehörden nicht die Rede sein kann.

b) Eine solche Zuordnung empfiehlt sich nur dann, wenn ein Wirtschaftsbereich unter *einem* einheitlichen Aspekt kontrolliert wird, der allein für diesen bestimmten Bereich von Bedeutung ist. Für die Bankaufsicht sind eben nur Bankgeschäfte, für die Versicherungsaufsicht nur Versicherungsgeschäfte von Belang. Für den Datenschutz kommt es jedoch auf die jeweiligen Geschäfte grundsätzlich nicht an (abgesehen vom Rahmen der notwendigen Informationen). Eine Trennung der Aufsicht, eine Aufteilung auf die verschiedenen bestehenden Aufsichtsbehörden ist deshalb nicht notwendig. Vielmehr macht gerade diese Eigenschaft der Datenschutzkontrolle eine einheitliche Kontrollinstanz für alle Informationssysteme möglich. Die Folge einer Aufteilung wäre eine Zersplitterung der Aufsicht auf viele einzelne Behörden, die der doch immer betonten Transparenz der öffentlichen Verwaltung für den Bürger gewiß nicht förderlich wäre.

c) Dieser Eindruck verstärkt sich, wenn man die Aufgabenstruktur bestehender Aufsichtsinstanzen näher betrachtet. Ziel der Banken- und Versicherungsaufsicht ist es, die Vermögenswerte der Bankgläubiger bzw. Versicherungsnehmer zu schützen und die volkswirtschaftliche Funktionsfähigkeit dieser Gewerbezweige zu erhalten [15]), dies ist in § 6 KWG ausdrücklich enthalten. Geschützt werden demnach lediglich wirtschaftliche, materielle Werte, nicht jedoch Werte, die außerhalb dieses wirtschaftlichen Rahmens anzusiedeln sind. Der Schutz der sog. Privatsphäre des einzelnen zählt also in keiner Weise zu den Zielen der bestehenden Aufsicht.

d) Aus dieser gänzlich anderen Zielsetzung wird auch deutlich, daß die personelle, technische etc. Organisation gar nicht geeignet sein kann, eine ordnungsgemäße Datenschutzkontrolle zu gewährleisten. Insofern kennt die Aufsichtsbehörde die zu kontrollierenden Objekte eben gerade nicht, sie müßte dazu eigens ausgestaltet und das Personal entsprechend geschult oder neu angestellt werden. Die verschiedene Zielsetzung erhellt auch, daß scheinbar gleiche Maßnahmen in Wahrheit doch nicht gleich sind: es kommt immer auf das damit verfolgte Ziel an. Sollten tatsächlich Überschneidungen auftreten, können sich die beteiligten Behörden diesbezüglich abstimmen, wie es auch im Bereich der Bankenaufsicht üblich ist.

e) Gegen eine Aufteilung der Datenschutzkontrolle spricht weiterhin, daß die einzelnen zuständigen Behörden einmal als Bundesoberbehörde [16]), einmal als Landesbehörde [17]) ausgestaltet sind. Eine einheitliche Behörde verdient den Vorzug, da auch die Kontrollmaterie einheitlich ist.

f) Ein letztes Argument für *eine* Aufsichtsbehörde ergibt sich aus der Überlegung, daß im Falle einer Aufteilung der Aufsicht diejenigen Informationssysteme *keiner Kontrolle* unterliegen würden, die bislang von keiner staatlichen Kontrolle erfaßt werden. Im Interesse des einzelnen muß jedoch auch hier eine öffentliche Kontrolle aus den oben unter 3.1. dieses Unterabschnittes genannten Gründen Platz greifen.

3.2.4. Entscheidung für eine einheitliche Kontrollinstanz

Die eben aufgeführten Argumente lassen es zumindest vorteilhafter, wenn nicht sogar geboten [18]) erscheinen, eine einheitliche Kontrollinstanz einzurichten. Bedenkenswert ist der Vorschlag des IPA-Entwurfs, eine *selbständige Bundesoberbehörde* zu errichten. Dadurch wäre eine einheitliche Kontrolle am besten gewährleistet. Gemäß Artikel 87 Abs. 3 Satz 1 ist dies möglich, sofern dem Bund in den betreffenden Angelegenheiten die Gesetzgebung zusteht [19]). Auf die nähere Ausgestaltung dieser Bundesbehörde kann hier nicht eingegangen werden, da dies den Rahmen des Gutachtens überschreiten würde.

---

[14]) vgl. den Ruland-Bericht, Drucksache 2563 der 3. Wahlperiode
[15]) vgl. für die Versicherungsaufsicht Boss, 15
[16]) § 5 I KWG
[17]) § 3 VAG
[18]) vgl. Simitis (2), 681
[19]) vgl. Gesetzgebungskompetenz

Vorzuziehen scheint jedoch die bereits zu den öffentlichen IS von Podlech vorgeschlagene organisatorische Lösung [20]). Im folgenden soll nur noch kurz darauf eingegangen werden, welche Punkte sich gegenüber der Aufsicht über Weitergabe-IS ändern.

a) Es wird sich nicht empfehlen, die Zulassung zum Geschäftsbetrieb für interne Informationssysteme getrennt von der Zulassung des eigentlichen Unternehmens bzw. der Organisation zu regeln. Es genügt, wenn bei der Zulassung etwa einer Bank das Aufsichtsamt für Kreditwesen die oben aufgeführten Zulassungsbedingungen berücksichtigt.

[20]) oben C. X.

b) Eine besondere Genehmigung für den Verkauf ganzer Informationssysteme ist, wie schon oben ausgeführt, nicht notwendig. Sie ist schlicht verboten.

Im übrigen behalten die Ausführungen zur öffentlichen Kontrolle der Weitergabe-Informationssysteme auch hier ihre Gültigkeit.

4. Strafnormen

Gegenüber den Ausführungen zu den gewerblichen Informationssystemen ergeben sich keine Änderungen.

Das Informationsrecht des Parlaments

Gliederung

Seite

C. Das Zusammenwirken von Parlament und Regierung im modernen Staat

D. Der Einfluß von Regierungsinformationssystemen auf den Entscheidungsprozeß in Regierung und Parlament

E. Das Verhältnis der parlamentarischen Informationsquellen zueinander

2. Teil

Juristische Untersuchung des Informationsaustausches zwischen Exekutive und Parlament

A. Vorbemerkung

B. Die herrschende juristische Doktrin

Einleitung

„Das Problem der Information des Parlaments ist ein Grundproblem des Staates und eine Lebensfrage für die Freiheit." Adolf Arndts [1]) leidenschaftlicher Appell an den Gesetzgeber des Jahres 1964, die Informationslage des Parlaments zu verbessern, hat auch heute nichts von seiner Gültigkeit verloren: Das Parlament, ohnehin von einem schier übermächtigen Apparat der Exekutive „an den Rand des politischen Zentrums" [2]) gedrückt, sieht sich durch die Einführung von Regierungs- und Verwaltungsinformationssystemen einer neuen Schwächung seiner ohnehin schon schwachen Position gegenüber.

Bis dahin mag noch ein weiter und mühevoller Weg zurückzulegen sein, gleichwohl ist der Gesetzgeber aufgerufen, schon jetzt seine besondere Aufmerksamkeit den Auswirkungen von Informationssystemen auf unser Verfassungsleben zu schenken. So begrüßenswert entsprechende Initiativen der Gesetzgeber [3]) in Bayern [4]), Hessen [5]) und Rheinland-Pfalz [6]) auch sein mögen, so sehr ist doch mit Simitis [7]) zu fragen, ob dort die spezifische Problematik erfaßt ist. Insbesondere erscheint es wenig angebracht, Fragen des Schutzes der sog. Privatsphäre und der Information des Parlaments unter dem Oberbegriff Datenschutz in ein und demselben Gesetz zu regeln [8]). Zutreffend ist das nur insoweit, als Datenschutz in der Tat die Kehrseite jeglicher Datenverarbeitung ist. Dabei ist jedoch zu unterscheiden zwischen Datenschutz im engeren Sinne, der sich mit der sog. Privacy-Problematik befaßt und Datenschutz im weiteren Sinne, der sich mit allen übrigen durch Datenverarbeitung hervorgerufenen Gefährdungen beschäftigt [9]). Letztlich ist die rechtliche Problematik beider Bereiche jedoch so verschieden, daß eine einheitliche Behandlung — jedenfalls für Zwecke des Gutachtens — „nur Verwirrung" stiften kann [10]). Aus diesem Grund ist es gerechtfertigt, beide Bereiche unabhängig voneinander zu behandeln. Das „Informationsrecht des Parlaments" wird daher hier entwickelt, ohne auf die Verknüpfung mit dem Datenschutz im engeren Sinne (Privacy-Problematik) näher einzugehen. Die Untersuchung des parlamentarischen Informationsrechts hat sich vor allem zwei hypothetische Fragen vorzulegen:

1. Welchen Einfluß haben Informationssysteme der Exekutive auf die parlamentarischen Funktionen?
2. In welcher Weise muß der Gesetzgeber den durch Informationssysteme bewirkten Veränderungen unseres Verfassungslebens Rechnung tragen?

Diese Fragestellung erfordert ein methodisches Vorgehen, das in einer breit angelegten Ist-Analyse zunächst die bestehenden informationellen Beziehungen zwischen Parlament und Exekutive untersucht. Sie bilden die Grundlage für die hypothetische Ist-Analyse (Frage 1) [11]) und den darauf zu entwickelnden Soll-Vorschlag (Frage 2) [12]).

[1]) (2), 292
[2]) Ellwein (4), 23
[3]) In Niedersachsen und Schleswig-Holstein hat die Exekutive von sich aus gehandelt, allerdings ohne das Problem der Information des Parlaments mitzuregeln; vgl. die „Dienstanweisung über den Schutz der Daten und ihre Geheimhaltung (Datengeheimnis) in der Datenzentrale Schleswig-Holstein vom 3. Februar 1970", abgedruckt in Kerkau, 100 ff. und die „Vorläufige Regelung des Datenschutzes in den Rechenzentralen des Landes", in: Niedersächsisches Ministerialblatt Nr. 46 vom 30. November 1970, S. 1326 f.
[4]) Gesetz über die Organisation der elektronischen Datenverarbeitung im Freistaat Bayern (Bay. EDVG) vom 12. Oktober 1970 (GVBl. S. 457).
[5]) Datenschutzgesetz vom 7. Oktober 1970 (GVBl. I S. 625)
[6]) Urantrag zum Entwurf eines Landesdatenschutzgesetzes vor mißbräuchlicher Datennutzung (Landesdatenschutzgesetz), Drucksache VI/2300
[7]) (2), 677 ff.
[8]) so auch Simitis (2), 678
[9]) s. o. zur Terminologie
[10]) Simitis (2), 677
[11]) s. u. 1. Teil, D.
[12]) s. u. 3. Teil

Gang der Untersuchung

Die Untersuchung beschränkt sich ausschließlich auf das Verhältnis Exekutive — Parlament: Zwar haben Veränderungen in diesem Verhältnis regelmäßig auch Auswirkungen auf andere Träger staatlicher Gewalt; so hat etwa die Judikative als Folge der faktischen Entmachtung des Parlaments einen Teil der diesem zugewiesenen Verwaltungskontrolle selbst übernommen. Doch handelt es sich hierbei im wesentlichen immer um Reaktionen auf veränderte Konstellationen im Verhältnis Exekutive — Parlament. Diese Tatsache rechtfertigt es, die Judikative — freilich nur für Zwecke des Gutachtens — aus der Untersuchung auszuklammern. Schließlich wird unter dem Stichwort Parlament hier nur der Bundestag behandelt. Insoweit wird unterstellt, daß das Informationsproblem für den Bundesrat wegen der engen funktionellen und personellen Verbindung von Bundesratsmitgliedern und Länderbürokratie verschieden gelagert ist.

Der einem Gutachten gesteckte Rahmen hatte des weiteren die Beschränkung zur Folge, daß im

wesentlichen nur das Verhältnis Regierung — Parlament in die Untersuchung einbezogen, dagegen die sonstige Exekutive ausgeklammert wurde. Diese Beschränkung rechtfertigt sich aus der Erwägung, daß Informationen innerhalb der Exekutive für den obersten Entscheidungsträger Regierung bereitgestellt werden müssen; Informationssysteme der Exekutive sind deswegen in erster Linie Regierungsinformationssysteme. Schließlich folgt sie aus dem Grundsatz der Alleinverantwortlichkeit der Regierung, der im wesentlichen keine unmittelbaren Beziehungen zwischen Parlament und Verwaltung zuläßt. Die Verwaltung ist nur insoweit in die Untersuchung miteinbezogen, als es für die Beweisführung unerläßlich war.

In einem ersten, vornehmlich politologischen und soziologischen Teil werden die derzeit herrschenden Informationsverhältnisse von Parlament und Exekutive analysiert. Es wird gezeigt, daß schon jetzt ein Informationsübergewicht von Regierung und Verwaltung besteht. Sodann wird nachgewiesen, daß sich dieses Übergewicht bei Einführung von Informationssystemen weiter zugunsten der Regierung bzw. Verwaltung verschieben wird. Im zweiten Teil wird die juristische Seite des Informationsaustausches zwischen Parlament und Regierung behandelt. Wir kommen zum Ergebnis, daß das geltende Recht und die herrschende Auslegung den Anforderungen schon jetzt kaum genügen, geschweige denn den besonderen, durch Informationssysteme erwachsenden Gefahren gerecht werden. Deshalb wird im weiteren Verlauf — freilich nur ansatzweise — eine neue Theorie des Informationsaustausches entwickelt. Diese Theorie ist Grundlage für die rechtspolitischen Vorschläge des dritten Teils.

1. Teil

Politologische Untersuchung der informationellen Situation von Parlament und Regierung

A. Die Informationsquellen des Parlaments

0. Terminologie [1])

Das Parlament wird in vielfacher Weise bei seiner parlamentarisch-politischen Tätigkeit unterstützt und mit Meinungen, Nachrichten, Stimmungen etc. beliefert.

Als *Informationsquelle* sei definiert jede Person, Einrichtung, Sammlung von Dokumenten, die dem Parlament Informationen oder Sachverstand zur Verfügung stellt.

Information wird hier in Anlehnung an Böhret [2]) in der Bedeutung von „zweckorientiertem Wissen" gebraucht. Diese Definition umfaßt danach nur die sog. pragmatische Dimension der Information [3]). Daß die Tragweite des noch immer sehr umstrittenen Begriffs nicht annähernd ausgeschöpft ist, kann für den Zweck der vorliegenden Untersuchung außer Betracht bleiben [4]).

Sachverstand sei hier jede Quelle, die aufgrund wissenschaftlicher Methoden wertende oder beschreibende Aussagen macht, er umfaßt also sowohl die wissenschaftliche Beratung wie Information [5]). Im übrigen wird auf die allgemeinen Ausführungen zur Terminologie verwiesen.

Für Zwecke der Untersuchung hat es sich als nützlich erwiesen, die Informationsquellen nach ihrer Herkunft zu unterscheiden [6]).

Interne Informationsquellen

Das sind alle Quellen, die sich das Parlament kraft seiner Autonomie selbst schaffen kann und die daher institutionell Teil der parlamentarischen Selbstverwaltung sind.

Externe Informationsquellen

Das sind alle Quellen, die institutionell außerhalb des Parlaments stehen.

1. Interne Informationsquellen

Die Internen Informationsquellen des Parlaments waren in den letzten Jahren häufig Gegenstand wissenschaftlicher Diskussion, so daß sich ein näheres Eingehen erübrigt. Daher wird im folgenden nur ein kursorischer Überblick gegeben [7]).

1.1. Parlamentarischer Hilfsdienst

Der Bund wie auch die meisten Bundesländer mit Ausnahme von Bayern, Bremen, Hamburg, Hessen, Saarland [8]) haben interne Hilfseinrichtungen für die Parlamente eingerichtet.

1.1.1. Parlamentarischer Hilfsdienst des Parlaments

Der parlamentarische Hilfsdienst des Bundestages ist rechtlich Bestandteil der Bundestagsverwaltung. Er gliedert sich in die Abteilungen Ausschußdienst und wissenschaftliche Abteilung [9]).

1.1.1.1. Der Ausschußdienst

Er besteht aus den Sekretariaten der Bundestagsausschüsse, wobei jedem Ausschuß ein sog. Ausschußdienst zur Verfügung steht.

Seine Aufgaben, die sich im einzelnen aus einem Schreiben des Bundestagspräsidenten an die Vorsitzenden der Bundestagsausschüsse [10]) ergeben, lassen sich wie folgt zusammenfassen:

— Unterstützung des Bundestagspräsidenten,

— Unterstützung der Ausschußvorsitzenden,

— büromäßige Vorarbeiten,

— Öffentlichkeitsarbeit,

— leichtere wissenschaftliche Tätigkeit.

---

[1]) Die Terminologie schließt sich eng an die Vorschläge Keller - Raupachs, 12 ff. an.

[2]) S. 141, der vor allem auf die Brauchbarkeit des Begriffs für ein politisches Informationssystem hinweist

[3]) näheres bei Steinmüller (1), 8; Wersig - Meyer - Uhlenried, 203

[4]) weiterführende Hinweise bei Wersing - Meyer - Uhlenried, 202; Steinmüller (1), 7; vgl. auch schon N. Wieners Ausführungen über Fortschritt und Entropie, 31 ff.

[5]) näheres bei Keller - Raupach, 14

[6]) Vgl. Keller - Raupach, 12: Die dort gegebene Unterscheidung ist zwar unscharf, aber für Arbeitszwecke durchaus geeignet. Daher wurde auch die durchaus problematische Einordnung der Hearings in die internen Informationsquellen übernommen.

[7]) weitere Einzelheiten in den Monographien von Schramm, Odewald und Keller - Raupach

[8]) Keller - Raupach, 19; im Saarland und in Bayern sind nicht einmal Ansätze vorhanden, Keller - Raupach, 23

[9]) guter Überblick bei Schäfer, 177 und Keller - Raupach, 154 ff.

[10]) abgedruckt bei Schramm, 112 f. und Keller - Raupach, 129 f.

1.1.1.2. Die wissenschaftliche Abteilung [11])

Die wissenschaftliche Abteilung bildet nach Schäfer [12]) die „Material- und Informationsbasis für alle Hilfsdienste des Bundestages". Er gliedert sich in die Referate [13])

— Bibliothek,
— Archiv,
— Gesetzesmaterialien,
— Presseauswertung,
— juristische Dokumentation,
— Fachdokumentation.

Die Aufgaben der wisenschaftlichen Abteilung lassen sich wie folgt umreißen [14]):

— Materialermittlung,
— Erschließung des bereitstehenden Materials,
— Literaturzusammenstellung, Bibliographie,
— Erstellung von Statistiken,
— Herstellung von Kontakten zu anderen wissenschaftlichen Einrichtungen.

1.1.2. Der Hilfsdienst der Fraktionen

Die Fraktionshilfsdienste haben keine feste organisierte Form; entsprechend ist der ihnen zugewiesene Aufgabenkatalog nicht genau zu ermitteln. Nach Untersuchungen von Keller—Raupach [15]) verrichteten sie im wesentlichen büromäßige Hilfsdienste, leisten Öffentlichkeitsarbeit und bieten eine Art von wissenschaftlichem Sachverstand an.

1.1.3. Leistungsfähigkeit der Hilfsdienste

Über die Leistungsfähigkeit der Hilfsdienste lassen sich generelle Aussagen nicht treffen. Zwar sind sie gewiß für die Parlamentarier eine wesentliche Hilfe, wie aus der Tatsache hervorgeht, daß der Hilfsdienst im Bund „recht rege in Anspruch genommen" [16]) und von den Abgeordneten positiv beurteilt wird [17]). Zu denken, ohne eigentlich beweiskräftig zu sein, gibt auch der Umstand, daß in Ländern mit relativ eingefahrenen Mehrheitsverhältnissen (Bayern, Hamburg, Hessen) die jeweilige Regierungsmehrheit Anträge der Opposition auf Einrichtung von Hilfsdiensten abgelehnt hat. Das mag, wie Keller—Raupach [18]) zutreffend bemerken, darauf zurückzuführen sein, daß eine Regierungsmehrheit, die nicht mit einem Wechsel der Mehrheitsverhältnisse zu rechnen braucht, kein großes Interesse an der Einrichtung derartiger Hilfsdienste hat, weil sie über den Regierungsapparat eher als die Opposition mit Informationen versorgt wird. Eine pikante Note erhält diese Feststellung obendrein dadurch, daß ausgerechnet Bayern und Hessen dem Parlament besondere Informationsrechte für Informationssysteme der Exekutive verschafft haben. Insgesamt ist der Tauglichkeit der Hilfsdienste im Hinblick auf die Beschaffung von Informationen mit Skepsis zu begegnen [19]). Die Bemühungen der Bundestagsverwaltung, in Zusammenarbeit mit der Studiengruppe für Systemforschung/Heidelberg [20]) automatische Dokumentationssysteme für den Bundestag zu entwickeln, mögen ein erster Anfang für die Verbesserung des parlamentarischen Apparats sein.

1.2. Persönliche Assistenten der Abgeordneten

Seit 1. April 1969 erhält jeder Abgeordnete des Deutschen Bundestages monatlich 1850 DM brutto für die Anstellung einer wissenschaftlichen Hilfskraft.

Die mit der Einführung der Abgeordneten-Assistenten verknüpften Hoffnungen haben sich nicht erfüllt: Die bisherigen Erfahrungen sind schlecht, die Assistenten bringen vornehmlich eine büromäßige Entlastung des einzelnen Abgeordneten und haben wegen der niedrigen Bezahlung nicht immer die erforderliche Qualifikation [21]).

Die Assistenten haben zur Verbesserung der Informationslage keinen wesentlichen Beitrag leisten können [22]).

1.3. Parlamentarische Hearings

Nach § 73 Abs. 2 der Geschäftsordnung des Bundestages können Ausschüsse durch besonderen Beschluß sog. Informationssitzungen einberufen, an denen Interessenvertreter, Auskunftspersonen und Sachverständige teilnehmen dürfen, eine Vorschrift, die auf das amerikanische Vorbild der Hearings zurückgeht [23]).

Hearings wollen in erster Linie den Veranstalter informieren, in zweiter Linie sollen sie den Interessierten Möglichkeiten der Einflußnahme eröffnen [24]), gleichsam den „Einfluß der Interessengruppen in die Publizität lenken" [25]). Der Informationseffekt der Hearings ist entgegen der Auffassung von Schramm [26]) und Schäfer [27]), die einen Ausbau dieses Instituts fordern, zweifelhaft: Die Hearings des amerikanischen Kongresses, die für die deutsche Regelung Pate gestanden haben, besitzen im amerikanischen Verfassungssystem eine andere Funktion [28]) und sind insbesondere deshalb so effektiv,

---

[11]) In welcher Weise der von Prof. Quaritsch geführte Gutachterstab des Bundestages mit dem wissenschaftlichen Dienst verbunden ist, ließ sich nach dem in Regensburg zugänglichen Material nicht ermitteln, vgl. dazu „Stern" vom 31. Januar 1971.
[12]) S. 183
[13]) insofern sind die Angaben bei Keller - Raupach, 183, ungenau, vgl. Schäfer, 183
[14]) näheres bei Keller - Raupach, S. 131 f.
[15]) S. 35
[16]) Keller - Raupach, 41
[17]) Keller - Raupach, 41
[18]) S. 44
[19]) ebenso wohl Keller - Raupach, 83
[20]) vgl. Meyer - Uhlenried
[21]) vgl. neuerdings: Der Spiegel, vom 3. Mai 1971, S. 36
[22]) so auch Keller - Raupach, 78
[23]) rechtsvergleichende Hinweise bei Frenkel, N. 943 ff.
[24]) Frenkel N. 945
[25]) E. Stein, zit. nach Schramm, 169
[26]) S. 169
[27]) S. 202
[28]) Das Verhältnis von Kongreß und Präsidenten ist durch eine strenge gewaltenteilige Organisation gekennzeichnet. Der Hauptteil der legislativen Arbeit wird von den Kongreßausschüssen geleistet, die eine ungleich stärkere Stellung haben als die Ausschüsse des Bundestages, vgl. näheres bei Keller - Raupach, 81, 86 ff.

weil sie nach einem dem Strafprozeß ähnlichen Verfahren ablaufen.

Hier dürfte schon die Publizität die Wahrhaftigkeit vieler Aussagen verhindern [29]). Im übrigen scheinen die Befürworter der Hearings von der auch von Keller-Raupach [30]) bekämpften Auffassung auszugehen, aus einer Vielzahl einseitiger Informationen lasse sich eine gleichsam in der Mitte liegende Information gewinnen.

1.4. Organisationen nach Art der Interparlamentarischen Arbeitsgemeinschaft (IPA)

Die 1953 gegründete IPA ist ein Zusammenschluß von Abgeordneten des Bundestages und der Länderparlamente. Sie gibt Stellungnahmen und Empfehlungen für den Gesetzgeber und versteht sich im übrigen als überparteilich.

Die IPA leistet sicher gute Dienste; zu nennen wären etwa die von der IPA herausgegebenen Gesetzestexte und in neuerer Zeit der Gesetzentwurf zum Schutz der Privatsphäre. Darüber hinaus bleibt ihr Einfluß gering, weil der satzungsmäßige Zwang zu parteipolitischer Neutralität viele Probleme neutralisiert [31]).

2. Externe Informationsquellen

2.1. Intermediäre Gewalten

Wegen des Wunsches der Verbände, ihre Ziele in den Gesetzen wiederzufinden, ist die Unterstützung für die Parlamentarier im Rahmen ihrer Verhältnisse jederzeit leicht verfügbar.

Wie schon oben unter 1.3. ausgeführt, ist der Wert der von Interessenvertretern gelieferten Informationen gering, soweit es sich nicht um bloße politische Standpunkte handelt: Die Verbandsinformationen sind in aller Regel einseitig und nicht vom Abgeordneten kontrollierbar. Auch die Parteien scheiden als Quelle von Informationen praktisch aus [32]).

2.2. Wissenschaftler- und Expertengremien

Über die Vergabe von Gutachten an Wissenschaftler und sonstige Experten durch das Parlament existieren — anders als für die Regierung — [33]) keine verläßlichen Angaben. Einen nennenswerten Einfluß haben die auch bisher inoffiziell und informell erstellten Gutachten auf die parlamentarische Informationssituation nicht nehmen können [34]).

2.3. Verwaltung und Regierung

2.3.1. Informationen nach Maßgabe von Rechtsbestimmungen

2.3.1.1. Auskünfte

Der Bundestag erhält bisher aufgrund folgender Rechtsnormen Auskünfte von der Regierung, d. h. die Tatsachenkenntnis wird von der Regierung vermittelt [35]):

— Artikel 43 GG (Zitierungsrecht, das übereinstimmend [36]) als Auskunftsrecht interpretiert wird)

— §§ 105 ff. GOBT (Große Anfrage)

— § 110 GOBT (Kleine Anfrage)

— § 111 GOBT (Mündliche Fragen in der Fragestunde)

— §§ 115, 116 GOBT (Auskunft über Ausführung von Bundestagsbeschlüssen)

Will man Keller - Raupach [37]) unter Hinweis auf Schäfer [38]) glauben, so handelt es sich bei den erwähnten Instituten „nach übereinstimmender Auffassung von politischer Wissenschaft und Praxis" eher — und in erster Linie — um Mittel zur Kontrolle der Regierung. Auf die Unhaltbarkeit dieser Auffassung wird später zurückzukommen sein.

2.3.1.2. Untersuchungen gemäß Artikel 44, 45 a GG

Diese unter dem Begriff Entqueterechte zusammengefaßten Informationsquellen bieten dem Parlament — im Gegensatz zu den Auskunftsrechten — die Möglichkeit, durch eigene parlamentarische Ermittlungstätigkeit Informationen von den Verwaltungsstellen zu holen [39]).

2.3.1.3. Befragung von Ministerialbeamten bei Ausschußberatungen

Die Teilnahme von Ministerialbeamten bei Ausschußsitzungen ist groß und zahlreich, wie Partsch [40]) berichtet. Genaue Angaben über die Art der von der Ministerialbürokratie gelieferten Informationen ließen sich nicht ermitteln.

2.3.1.4. Formulierungshilfe

Nach Keller - Raupach [41]) besteht „mindestens im Deutschen Bundestag eine gewisse gewohnheitsrechtliche Verpflichtung der Ressorts, den Fraktionen und Abgeordneten Formulierungshilfe bei ihren Vorlagen zu leisten".

2.3.2. Informelle Kontakte

Daß nach dem Abbau des Antagonismus von Exekutive und Parlament eine Vielzahl informeller Beziehungen zwischen beiden „Gewalten" besteht, bedarf keiner besonderen Erwähnung. Freilich ist es kein Geheimnis, daß die Ministerialbürokratie mit Hilfen behutsam umgeht, soweit es sich um Kontakte mit Oppositionspolitikern handelt.

---

[29]) Bedenken auch bei Keller - Raupach, 82
[30]) S. 81
[31]) in dieser Richtung auch Keller - Raupach, 83; a. A. aber Schramm, 163
[32]) Keller - Raupach, 76
[33]) vgl. etwa die bei Keller - Raupach, 69 FN 40 angeführte Literatur
[34]) vgl. auch die Polemik von Dichgans, 112 ff.
[35]) Ridder (1), Sp. 1170; vgl. im übrigen unten 3. Teil B. 1.
[36]) Statt aller Maunz - Dürig - Herzog, Artikel 43 N. 8
[37]) S. 66
[38]) S. 230 ff.
[39]) vgl. Steffani (2), 16 FN 1
[40]) (1), 84
[41]) S. 66 f.; so auch Höcherl in seiner Eigenschaft als Bundesminister, zit. nach Odewald 100 FN 226

2.3.3. Leistungsfähigkeit von Regierung und Verwaltung als Informationsquelle

Betrachtet man die vielfältigen — formellen wie informellen — Kontakte zwischen dem Parlament und der Regierung (Verwaltung), so scheinen sich dem Parlament dank der zweifellos großen Hilfsbereitschaft vielfältige und brauchbare Informationsquellen zu eröffnen.

Tatsächlich eignen sich die von der Exekutive erlangten Informationen nur bedingt für parlamentarische Zwecke: — keine Nachprüfbarkeit der Informationen.

Das Parlament hat zwar vielfältige Möglichkeiten, Auskünfte von der Regierung zu bekommen, jedoch keine Möglichkeit, die Informationen auf Vollständigkeit, Richtigkeit etc. zu überprüfen [42]). Da in der Fragestunde zudem eine Replik auf unbefriedigende Antworten des Ministers nicht möglich ist, hat sich nach Heinemann [43]) eine sog. „Rudeltaktik" entwikkelt, „derart, daß eine Reihe von Abgeordneten sich vorher zusammensetzen, um gedanklich durchzuspielen, welche ausweichenden oder verschleiernden Antworten ein Minister voraussichtlich geben kann, damit andere nachstoßen, wenn der erste Fragesteller ein Kontingent von nur zwei Fragen erschöpft hat".

— *Undurchschaubarkeit des Entscheidungsprozesses*

Das Parlament erfährt in aller Regel nur den endgültig formulierten Willen der Verwaltung. Auf dieser Linie liegt die Vorschrift des § 41 der Gemeinsamen Geschäftsordnung der Bundesministerien [44]), wonach Gesetzesvorlagen der Regierung selbst dann einheitlich im Parlament vertreten werden müssen, wenn etwa zwischen verschiedenen Ressorts Meinungsverschiedenheiten bestanden haben. Dem Parlament bleiben damit die für die eigene Entscheidung wesentlichen Bewertungsgrundlagen, Motive und Alternativprogramme verborgen [45]). Es bekommt also nur gefilterte Informationen.

— *Mängel exekutivischen Sachverstandes*

Es besteht kein Zweifel, daß das hochspezialisierte Fachwissen von Verwaltungsexperten und die mehr an übergreifenden Vorstellungen ausgerichteten Bedürfnisse der Parlamentarier in vielen Fällen nicht übereinstimmen. Inwieweit daraus der Vorwurf fachlicher Inkompetenz der Bürokratie abzuleiten ist, muß mit Keller — Raupach [46]) bezweifelt werden, in jedem Fall bedürfte das genauerer Untersuchungen. In diesem beschränkten Sinne mag auch Wittkämpers [47]) Bemerkung ihre Berechtigung haben, wonach das einseitige Verlassen auf die Sachkunde der Verwaltung zur Aushöhlung des Gewaltenteilungsprinzips führe.

— *Schwache Stellung der Opposition*

Die mangelhafte Versorgung mit Exekutivinformationen trifft vor allem die Opposition, da die Regierungsmehrheit weit mehr über den Sachverstand der Ministerialbürokratie verfügen kann [48]). Es ist daher nur folgerichtig, wenn die Auskunftsrechte, wie die Untersuchungen Schollers [49]) zeigen, vor allem von der Opposition in Anspruch genommen werden.

3. Vorschläge zur Verbesserung der Informationssituation des Parlaments

3.1. Parlamentsreform

Die Informationslage des Parlaments wird allgemein als unbefriedigend angesehen (vgl. etwa die Arbeiten von Schäfer, Odewald, Schramm, Keller-Raupach usw.). In der seit Jahren anhaltenden Debatte um die Parlamentsreform wird entsprechend immer wieder eine Verbesserung der parlamentarischen Informationsquellen gefordert.

Freilich weist die Diskussion keine hier erwähnenswerten Züge auf, sieht man einmal von der immer wiederkehrenden Forderung auf Schaffung eines Gesetzgebungshilfsdienstes [50]) und stärkerer Berücksichtigung wissenschaftlichen Sachverstandes ab [51]). Unter Gesetzgebungshilfsdienst soll dabei „eine Einrichtung zur Unterstützung der Abgeordneten in ihrer gesetzgeberischen Tätigkeit" [52]) verstanden werden. Zu bemerken bleibt noch, daß sich, wie Keller-Raupach [53]) zutreffend erkannt haben, zwei Richtungen der Diskussion feststellen lassen:

Die eine Richtung will das Gesamtparlament gegenüber der Regierung stärken, verbesserte Informationsquellen — wie etwa den Gesetzgebungshilfsdienst — entsprechend dem Gesamtparlament zuschlagen.

Die andere Richtung will vor allem die Stellung der Opposition gegenüber dem Block Regierung — Verwaltung — Regierungsmehrheit stärken; entsprechend legt sie den Schwerpunkt auf eine Stärkung des oppositionellen Apparats [54]). Ohne hier tiefer in die Diskussion eindringen zu wollen, kann festgestellt werden, daß die Debatte um die Parlamentsreform keine wesentlichen neuen Aspekte für das hier zu entscheidende Problem gebracht hat.

---

[42]) statt aller vgl. Gehrig, 295 und die in FN 248 Genannten
[43]) (1), E 57
[44]) besonderer Teil, abgedruckt bei Lechner - Hülshoff, 399 ff.
[45]) vgl. Odewald, 90 und die bei Keller - Raupach, 68 wiedergegebenen Zitate der Abgeordneten Müller-Link und Hirsch
[46]) S. 69
[47]) S. 177
[48]) Keller - Raupach, 50
[49]) vgl. insbesondere die Tabellen auf S. 410 ff.
[50]) Schäfer, 298; Keller - Raupach, 83; Odewald, 76 ff.; Schramm, 133 ff., der einen entsprechenden Verfassungsauftrag erkannt haben will; vgl. im übrigen oben 1.1.1.2.
[51]) so fordert Schäfer, 299, etwa die Einrichtung parlamentarisch-wissenschaftlicher Kommissionen
[52]) Schramm, 74
[53]) S. 92 f.
[54]) etwa Gehrig, 304 ff.

3.2. Die Datenschutzgesetze von Hessen und Rheinland-Pfalz; Bayerisches EDV-Gesetz [55])

Der Vollständigkeit halber soll hier kurz auf die Bemühungen der Bundesländer Hessen, Rheinland-Pfalz und Bayern [56]) eingegangen werden, dies schon deshalb, weil die entsprechenden Regelungen einem Bundesgesetzgeber als Vorbild dienen könnten.

3.2.1. Auskunftsrechte

Alle drei Gesetze (§ 1 Abs. 1 Bay. EDVG; § 6 I Hess. DSchG; § 4 Abs. 1 Rh-Pf. DSchG) geben den Länderparlamenten das Recht, von der Regierung bzw. der Verwaltung Auskünfte aufgrund der gespeicherten Daten zu verlangen (Rheinland-Pfalz: „erfaßten"). Man fragt sich, wie wohl derartige Formulierungen gemeint sein mögen und worin etwa der Unterschied zwischen der hessischen, bzw. bayerischen Normierung und dem rheinland-pfälzischen Gesetz bestehen mag. Auf die Gefährlichkeit derart vager Formulierungen ist breits an anderer Stelle [57]) hingewiesen worden. In jedem Fall fordern die Bestimmungen Auslegungsstreitigkeiten geradezu heraus: „Auskunft aufgrund der gespeicherten Daten". So könnte die Formulierung bedeuten, daß die Regierung bzw. sonstige Stellen für die Auskünfte *alle* verfügbaren gespeicherten Daten benutzen muß.

Auskunft könnte aber auch bedeuten Auswertung gerade durch Stellen der Exekutive. Dafür spricht die Formulierung des § 6 Abs. 1 Hess. DSchG, der Auskünfte von dem Vorhandensein von Auswertungsprogrammen abhängig macht. Schließlich wäre auch denkbar, daß die Auskunft erkennen lassen muß, aufgrund welcher Informationen (nicht Daten, wie die Gesetze fälschlicherweise formulieren) sie ergangen ist. Dann wäre ungeklärt, wie sich diese Auskunftsrechte zu den parlamentarischen Interpellationsrechten verhalten.

Nach allem läßt sich über den Wert der neugeschaffenen Auskunftsrechte solange keine Angabe machen, als nicht die genaue Bedeutung in der parlamentarischen Praxis erprobt ist. Dann läßt sich auch feststellen, ob die Landesgesetzgeber unterscheiden wollten zwischen einer Auskunft *aufgrund* und einer Auskunft *über* Daten.

3.2.2. Zugriffsrechte

Als einziges Gesetz statuiert Artikel 1 Abs. 2 des Bay. EDVG ein sog. *Zugriffsrecht:* „Der Landtag und der Senat haben Zugriff zu den gespeicherten Daten mit allgemeinem Informationsgehalt und mit planerischer Zielsetzung. Das Nähere wird durch Rechtsverordnung der Staatsregierung bestimmt, die der Zustimmung des Landtages bedarf."

Auch hier kann auf eine Kritik der Vorschrift verzichtet werden [58]). Zu fragen ist nur, was Daten „mit allgemeinem Informationsgehalt und planerischer Zielsetzung" wohl sein mögen. Diese Begriffe sind sowohl der klassischen Jurisprudenz wie der Rechtsinformatik fremd und zeugen nicht unbedingt vom Sachverstand des Gesetzgebers. Vielleicht geht sie auf die von der KGSt entwickelte Unterscheidung von Planung und Vollzug [59]) zurück, die ihrerseits von betriebswirtschaftlichen Vorstellungen beeinflußt ist. Der genaue Wert dieses Zugriffsrechts als parlamentarischer Informationsquelle kann erst dann eingeschätzt werden, wenn der Bayerische Verordnungsgeber den Auftrag des Artikels 1 Abs. 2 Bay. EDVG erfüllt hat.

4. Zusammenfassende Beurteilung der parlamentarischen Informationsquellen

4.1.

Die dem Parlament gegebenen Möglichkeiten zur Information sind — jedenfalls auf den ersten Blick — vielfach. Es bezieht Informationen über alle relevanten Bereiche der Wirklichkeit und von allen politisch relevanten Gruppen.

Freilich ist das Problem des Parlaments nicht ein Zuwenig, sondern ein Zuviel an Informationen. Das Parlament bekommt im wesentlichen keine zielgerichteten, entscheidungsrelevanten Informationen [60]). Oder anders: Das Parlament leidet an einem Überfluß an *DATEN* [61]) und einem Mangel an Informationen, eine Tatsache, die Keller-Raupach [62]) von einem „Paradoxon" sprechen läßt.

Die Informationsgewinnung des Bundestages ist mehr oder weniger zufällig und ermangelt der „auf den Empfangsmechanismus des Abgeordneten [63])" gerichteten Informationen.

4.2.

Das Parlament hat bisher noch keine Entscheidungshilfsmittel, d. h. Methoden, um Entscheidungen zu finden, entwickelt [z. B. brain-storming; Scenarios; Systemanalyse [64])]: Denn Informationen liefern noch nicht die Entscheidung [65]) selbst, sie bereiten sie vor.

Diesem Mangel entspricht die weit verbreitete Ansicht, es sei das „Kennzeichen der politischen Entscheidung, daß sie sich nicht aus Sachargumenten ableiten lasse" [66]). Dieser Auffassung kann nicht entschieden genug entgegengetreten werden; das soll aber hier nicht weiter vertieft werden [67]). Im Angesicht dieser Sachlage erscheint es klar, daß das Parlament nur noch am Rande des politischen Zentrums „Platz" [68]) hat.

---

[55]) Fundstellen s. o. in der Einleitung. Die dort erwähnten Regelungen Schleswig-Holsteins und Niedersachsens können hier außer Betracht bleiben.
[56]) In Nordrhein-Westfalen stehen möglicherweise ähnliche Regelungen bevor, vgl. Simitis (2), 677 FN 35.
[57]) Simitis (2), 679
[58]) dazu wieder Simitis (2), 679
[59]) vgl. dazu Steinmüller (1), 70 f.
[60]) zum Begriff „entscheidungsrelevant" vgl. Böhret, 141
[61]) vgl. im übrigen den Abschnitt über Terminologie
[62]) S. 65
[63]) Dichgans, 120
[64]) vgl. im übrigen die Übersicht bei Böhret, 66
[65]) zum Begriff s. u. 1. Teil, C. 3.2.1.
[66]) so Dichgans, 114
[67]) zur Kritik dieses nicht rationalen Modells der politischen Entscheidung vgl. auch Böhret, 33
[68]) Ellwein (4), 23

B. Die Informationsquellen der Regierung — Überblick

1. Die Darstellung der Informationsquellen

Im Gegensatz zu dem reichlichen Schrifttum über Informationsquellen des Parlaments ist die literarische Diskussion für den Bereich der Regierung im wesentlichen nicht über Ansätze hinausgekommen. Zwar gibt es zahlreiche Veröffentlichungen über den Bereich „wissenschaftliche Beratung der Politik" [1]). Zwar hat die Ankündigung des Bundesdatenbankprojektes [2]) insbesonders die Massenmedien zu „munteren Stellungnahmen" ermutigt. Es fehlt jedoch — soweit ersichtlich — bis heute ein systematischer Entwurf für die Entscheidungshilfsmittel der Regierung. Die Monographie von Böhret ist insoweit nur ein erster Anfang [3]). Diese Tatsache mag ihre Ursache darin haben, daß hinreichende Information nicht wie für das Parlament eine Frage des Überlebens ist, vielmehr zu den Dingen zählt, die sich von selbst verstehen. Zum anderen hat sich unter dem Primat der Verwaltungsrechtsdogmatik lange Zeit keine wissenschaftliche Lehre vom Regieren und Verwalten bilden können, ebenso wie die Politikwissenschaft das Problem vernachlässigt hat [4]).

Dieser Mangel tritt etwa exemplarisch in dem Lehrbuch Thiemes hervor: Er erwähnt als Informationsquelle das Schriftgut (Akten) [5]), bezieht die Anwendungsmöglichkeiten elektronischer Datenverarbeitung nur auf die Bearbeitung von Massenvorgängen [6]) und läßt die sich aus den Komponenten — Planung — Entscheidung — Information ergebende Problematik unerwähnt.

Nach allem muß es für den Rahmen dieser Untersuchung mit einem summarischen Überblick sein Bewenden haben. Die Regierung verfügt über folgende Informationsquellen:

— Verwaltung

„Die Verwaltung ist in wesentlichen Bereichen der eigene Informant" [7]).

— Beraterstäbe

Sonderabteilungen aus Beamten der Ministerien für besondere Aufgaben.

— Expertengremien

Jedes Ministerium läßt sich in wichtigen Fragen von Expertengremien und Sachverständigenkommissionen beraten [8]).

— Wissenschaft

Für wichtige und neuartige Fragen werden Gutachten in großer Zahl vergeben [9]).

— Eigene Forschungsinstitute

Beispiel ist die Gesellschaft für Mathematik und Datenverarbeitung (GMD) in Birlinghoven.

— Aufträge an Expertengremien

So wird das Justizdatenbankenprojekt in Zusammenarbeit mit der Frankfurter Beratungsfirma C-E-I-R abgewickelt [10]).

— vielfältige Kontakte mit Verbänden [11]).

2. Die Leistungsfähigkeit der Informationsquellen

Mit Ellwein [12]) gilt es festzustellen: „Niemand (ist) imstande, aufgrund rationeller Kriterien, zureichender empirischer Forschung und theoretischer Würdigung zu beurteilen, ob die Bundesregierung umfassend genug informiert ist und bei ihren Entscheidungen die möglichen Informationen genügend verarbeitet". Darauf kommt es jedoch für den vorliegenden Zusammenhang nicht an. Entscheidend kann insoweit nur sein, wie die Regierung (Verwaltung) im Verhältnis zum Parlament informiert ist. Insoweit besteht keinerlei Streit, daß das Parlament grundlegend schlechter informiert ist, ein Sachverhalt, der schon Max Weber [13]) zu dem Satz veranlaßte: „Der Reichstag ist verfassungsmäßig zur dilettantischen Dummheit verurteilt". Auch für die Beantwortung der dem Gutachten gestellten Fragen geht es einzig um das Verhältnis von exekutiven und legislativen Informationsquellen. Eine optimale Verhältnisbeschreibung findet sich bei Simitis [14]), der zur Charakterisierung den Ausdruck „Informationsgleichgewicht" verwendet. Freilich läßt sich dieses Ziel auch bei größten Anstrengungen nur schwer erreichen.

---

[1]) vgl. dazu etwa die bei Keller - Raupach, 69 FN 40 Genannten; vgl. auch neuerdings Friedrich

[2]) vgl. zuerst Bulletin des Presse- und Informationsamtes der Bundesregierung, Nr. 115, S. 990 vom 13. September 1968

[3]) Böhrets Untersuchung krankt jedoch daran, daß sie sich einseitig auf Ergebnisse der Wirtschaftswissenschaften stützt. Er hinterfragt nicht die Regierungstechniken nach ihren politisch-ökonomischen Implikationen — so richtig Narr, 8 FN 269 — und gibt somit einseitig der Effizienz der Technik den Vorrang vor anderen Prinzipien (z. B. Demokratie, Sozialstaatlichkeit).

[4]) zum ganzen vgl. Böhret, 11 f.; Ellwein, 9 ff.

[5]) Nr. 806

[6]) N. 786 ff.

[7]) Ellwein (2), 105 und FN 110

[8]) vgl. die umfassende, gleichwohl nicht vollständige Übersicht in Drucksache V/4585

[9]) näheres hierzu in der schon erwähnten Veröffentlichung von Friedrichs

[10]) näheres Projektgruppe Juristisches Informationssystem, 1

[11]) vgl. dazu Keller - Raupach, 69 f.

[12]) (3), 177 f.

[13]) S. 340 — freilich in etwas anderem Zusammenhang

[14]) (2), 674

C. Das Zusammenwirken von Parlament und Regierung im modernen Staat

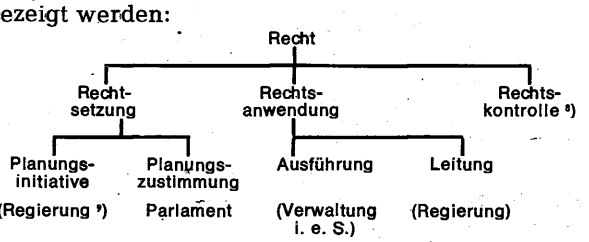
1. Die Verteilung der Funktionen

Für ein Gemeinwesen von auch nur bescheidenem Umfang ist es undenkbar, daß alle Funktionen an einer Stelle vereinigt werden [1]). Schon das Prinzip der Arbeitsteilung erfordert eine Verteilung der Aufgaben und eine arbeitsteilige Organisation [2]). Das Grundgesetz sieht dazu in Artikel 20 Abs. 2 eine Verteilung der Aufgaben auf die Funktionsträger Exekutive, Legislative und Judikative vor. Man hat lange geglaubt, im Grundsatz der Gewaltenteilung ein Prinzip gefunden zu haben, das brauchbare Kriterien für die Abgrenzung der Funktionsbereiche liefern kann. Diese Hoffnung hat sich nicht erfüllt wie insbesondere von der Tübinger Schule nachgewiesen wurde [3]). Mit Achterberg [4]) gilt: „Die Klärung der Funktioneninhalte (stellt) eine der wichtigsten Aufgaben der heutigen Staatsrechtswissenschaft dar".

Wenn daher im folgenden den einzelnen Funktionsträgern bestimmte Funktionen zugewiesen werden, so geschieht das unter ausdrücklichem Vorbehalt: Juristisch ist eine Abgrenzung bisher nicht gelungen, die etwa Planung [5]) und Initiative eindeutig der Regierung oder dem Parlament zuweisen würde. Um aber gleichwohl zu konkreten Ergebnissen zu kommen, scheint in Anlehnung an Ellwein [6]) jedenfalls für den Bereich der Regierung methodisch ein anderer Ansatz angebracht: Regierung erhält ihr Bezugssystem nicht aus der juristischen Staatsorganisation, sondern den öffentlichen Aufgaben, die die Regierung heute tatsächlich wahrzunehmen hat.

2. Modell einer Funktionsverteilung zwischen Exekutive und Parlament [7])

Sowohl Regierung wie Parlament ist die Grundfunktion „Gestaltung der sozialen Wirklichkeit" zugewiesen. Die arbeitsmäßige Verteilung dieser Funktion soll an Hand des folgenden Schemas aufgezeigt werden:



Das Schaubild zeigt deutlich, daß die Funktion Rechtsetzung auf Parlament *und* Regierung verteilt ist. Aus dieser Tatsache erklärt es sich unter anderem, daß juristische Abgrenzungsversuche von Regierung und Parlament bisher gescheitert sind. Planungsinitiative soll hier sein: Zielsetzung und Rechtsbestimmung; Planungszustimmung: die endgültige, letztinstanzliche Beschlußfassung.

Ausführung bezeichnet die innerhalb begrenzter Ermessenskompetenz gestaltete Rechtsanwendung im Einzelfall, Leitung die politische Anweisung und letztinstanzliche Befehlsgebung [10]). Da wie schon im Vorwort erwähnt — hier nur das Verhältnis Regierung — Parlament untersucht wird, beschränkt sich die folgende Analyse auf den Bereich der Rechtsetzung. Nach allem soll Regierung [11]) hier definiert werden als „die schöpferische Entscheidung, die politische Initiative und die zusammenfassende Leitung des Staatsganzen" [12]). Regieren läßt sich danach „als Planen, Entscheiden, Ingangsetzen, Anweisen und Beaufsichtigen" begreifen. [13]).

Im folgenden soll dieser dem Parlament wie der Regierung zugewiesene Bereich „Gestaltung der sozialen Wirklichkeit" besonders untersucht werden. Daß die rechtlichen Funktionen des Parlaments [14]), wie Kontrollfunktion, Ordnungsfunktion und Rückkopplungsfunktion [15]) dabei unberücksichtigt bleiben, rechtfertigt sich aus folgender Erwägung: Insbesondere die hier einschlägige Kontrollfunktion setzt die oben beschriebene Grundfunktion insoweit voraus, als sie darauf Einfluß nehmen will. Die getrennte Behandlung hat dann den Vorteil, daß sie Tendenzen und Veränderungen, die alle von dieser Grundfunktion abhängig sind, stärker hervortreten läßt.

3. Die Regierung als Planungsträger

Angesichts komplexer, mannigfacher und voneinander abhängiger Sachverhalte sieht sich jede Regie-

---

[1]) Forsthoff (1), 424
[2]) Hahn, 450
[3]) vgl. die Monographien von Jesch und Rupp
[4]) S. 231: vgl. auch Hinkamp, 35 ff.
[5]) zum Begriff vgl. unten 1. Teil C. 3
[6]) (2), S. 128 f.
[7]) In Anlehnung an Steffani (3), 331, der sich jedoch teilweise widerspricht. Im übrigen soll ausdrücklich darauf hingewiesen werden, daß es sich bei dem vorgestellten Modell um einen politologischen, nicht aber juristischen Ansatz handelt.
[8]) Die von der Judikative vorzunehmende Rechtskontrolle wird entsprechend dem im Vorwort Gesagten im Gutachten nicht behandelt.
[9]) Dabei wird das Initiativrecht des Bundestages nicht übersehen, vgl. Artikel 76 GG; siehe auch Steffani, a. a. O.
[10]) Näheres bei Stein, S. 79 ff.; Hesse (2), S. 196 ff.
[11]) gute Literaturübersicht zum Begriff und Wesen der Regierung bei Gehrig, 11 FN 27
[12]) Scheuner, 278
[13]) Ellwein (2), 128
[14]) vgl. insbesonders Steffani (2), 106 f.
[15]) vgl. Stein 75 ff.; Steins Begriff hat Ähnlichkeit mit der sog. lyrischen Funktion. Näheres bei Steffani (2) 14 FN 1; gegen die Eigenständigkeit dieser Kategorie wohl Ehmke (2), E 10

rung vor immer schwierigere Entscheidungssituationen gestellt; sie muß „sich auf zukünftig mögliche Situationen vorbereiten, darf Zufällen nicht hilflos gegenüberstehen und muß (lernen), die Konsequenzen ihrer Entscheidungen abzuwägen" [16]). Die Regierung hat die Aufgabe, die Zukunft berechenbar zu machen, sie muß planen [17]).

Planung, in weiten Kreisen noch ideologieverdächtig, ist inzwischen ein „ins allgemeine Bewußtsein aufsteigender Schlüsselbegriff" [18]) geworden. Ein moderner Staat kann es sich nicht mehr leisten, bei plötzlich eintretenden Krisen — wie etwa einer Währungskrise — handlungsunfähig zu sein. Er muß für diesen Fall sofort *Programme* — hier verwandt als „alternative Ziel-Mittelkombination [19]) — anbieten und dabei den ungeschriebenen Lehrsatz politischer Planung bedenken, wonach fast alle gesellschaftspolitischen Veränderungen voneinander abhängen. Planung heißt daher auch Ausschaltung des Zufalls und „systematischer Entwurf einer rationalen Ordnung" [20]). Auf das Verhältnis von Planungsprozeß und Entscheidung braucht hier nicht näher eingegangen zu werden. Schlagwortartig läßt sich sagen, daß Planung eine Art Antizipation der Entscheidung ist. [21])

Die schließlich ergehenden Planungsentscheidungen erfordern nach Ellwein [22]) ein Vierfaches:

1. Erkennen des Notwendigen,
2. Benennen der Regelungsmöglichkeiten,
3. Auswahl,
4. Beschluß (Bringen in die geeignete Form).

Diese Phasen sollen nun im folgenden näher betrachtet werden.

3.1. Erkennen des Notwendigen

Der Regierung ist die Aufgabe, „Gestaltung der sozialen Wirklichkeit" zugewiesen. Diese Aufgabe ist in bezug auf die soziale Wirklichkeit in keiner Weise begrenzt, sie hat also den gesamten Bereich sozialer Wirklichkeit zu erfassen. Nun kann freilich eine Regierung die soziale Wirklichkeit nicht einmal ansatzweise vollständig erkennen, weil sie zu komplex und kaum von Fachleuten durchschaubar ist. Gleichwohl besteht eine Beziehung zwischen Regierung und Wirklichkeit. *Diese Beziehung wird durch Informationen vermittelt.* Dies soll an einem Beispiel verdeutlicht werden:

Der Minister A erteilt einer zuständigen Stelle die — (generelle oder Einzel-)Anweisung, alle Veränderungen der Arbeitslosigkeit zu beobachten. Die Bundesanstalt für Arbeitsversicherung meldet die Zahlen 5 % in der X-Branche, 10 % in der Y-Branche. *Diese Zahlen sind nicht Wirklichkeit, sie repräsentieren Wirklichkeit:* Denn alle Informationen repräsentieren Wirklichkeit. Diese Zahlen werden dann zuständigen Stellen der Bürokratie zugeleitet, die Anmerkungen, Vorschläge, Ergänzungen machen, sich mit anderen Ministerien besprechen. Gemeldet wird der Regierung schließlich ein *Modell sozialer Wirklichkeit;* denn die Akte etwa, die der Minister erhält, ist das informationelle Abbild eines zu untersuchenden Originals (der abgebildeten Realität) für ein untersuchendes Subjekt (den Minister) [23]).

Dieses Modell ist verständlich nur aus der besonderen Entstehungssituation; sie umfaßt neben anderen:

— politische Weisungen des Ministers,

— generelle Dienstanweisungen,

— psychologische Besonderheiten der Hierarchie,

— Koordination,

— Absprachen mit Interessenträgern.

Mit anderen Worten, das Modell ist keineswegs „objektiv", sondern von den speziellen Verwendungszwecken des Entscheidungsträgers her definiert (pragmatische Dimension der Information und des Modells).

Dieses Modell wird die Wirklichkeit um so präziser wiedergeben, je besser die Instrumente zum Erkennen realer Vorgänge ausgebildet sind und je genauer sie in Informationen ausgedrückt und an den Entscheidungsträger weitergeleitet wird. Instrument dieser Art ist die gesamte öffentliche Verwaltung, deren Organisation im Zeitalter der Leistungsverwaltung den größten Teil gesellschaftlicher Realität erfaßt. Soweit diese Aufgaben von herkömmlichen Behörden nicht mehr erfüllt werden können, wurden Sonderverwaltungen gebildet, was zu dem von vielen beklagten Verlust der Einheit der Verwaltung [24]) geführt hat:

Es hat sich gezeigt, daß für eine neue Aufgabe, auch für die ausgefeilteste Form der Spezialisierung in einer Regierung immer Platz ist [25]).

Aus dieser Sicht wird verständlich, wenn formuliert wird, „fortlaufende Information (sei) die Grundlage für jede tätige Initiative auf allen Gebieten" [26]) oder „Information (gehöre) funktionell immer zum Regieren" [27]). Gemeint ist, daß über Wirklichkeit nicht ohne ein durch Informationen vermitteltes Realitätsmodell entschieden werden kann, oder besser, werden sollte.

Somit kann festgehalten werden:

1. Der Entscheidungsträger Regierung erhält aufgrund der Güte seiner Informationsquellen ein

[16]) Böhret, 1
[17]) vgl. Ellwein (2), 129
[18]) Kaiser (2), 7; Forsthoff (1), 3 setzt sogar den Begriff Verwaltung mit Gestaltung gleich.
[19]) Böhret, 53. Dieser Begriff stammt aus der Politologie und darf nicht mit dem Begriff verwechselt werden, wie er in der Datenverarbeitung verwandt wird.
[20]) Kaiser (2), 7
[21]) In dieser Richtung Grochla, Handwörterbuch der Organisation, Sp. 1305 f.
[22]) (2), 148
[23]) Steinmüller (1), 18
[24]) dazu vgl. Becker, 715; Osswald, 7; Thieme N. 445; Geib, 148 und Wolff, 94; Ellwein (3), 200
[25]) Partsch (1), 76/77
[26]) Nawiasky, 18
[27]) Kassimatis, 39; vgl. auch Fiedler (3), 555; Ellwein (3), 175

— im Vergleich zum Parlament — vollständigeres Realitätsmodell als Entscheidungsgrundlage.

2. Das Realitätsmodell ist von den Zwecken des Entscheidungsträgers her definiert.

3.2. Die Entscheidung selbst [28])

3.2.1. Allgemeines zum Entscheidungsbegriff

Die Regierung hat alle einlaufenden Realitätsmodelle zu überprüfen, zu verwerfen usw., sie hat sich letztinstanzlich zu entscheiden, sie ist der führende Entscheidungsträger [29]).

Als Entscheidung sei hier definiert jede bewußte und überlegte Wahl zwischen möglichen Verhaltensalternativen [30]). Dabei soll der Begriff auch dann erfüllt sein, wenn keine Wahl unter mehreren Möglichkeiten getroffen wird, vielmehr ein Zustand aufrecht erhalten bleiben soll [31]).

Die Komplexität des zu entscheidenden Gegenstandes und die Interdependenz der Lebensverhältnisse erfordert nun von der Entscheidung eine ganz bestimmte inhaltliche Qualifikation: Sie muß rational sein. Rational bezeichnet Böhret [32]) im Gegensatz zum intuitiven ein Verhalten, das überlegt, planvoll, begrifflich faßbar und intersubjektiv überprüfbar ist. Dieser Rationalitätsbegriff ist bedenklich, da Rationalität formal und wertneutral verstanden wird. Dem gleichen Fehler unterliegt etwa die Organisationssoziologin Mayntz [33]), die die Rationalitätskriterien nur auf die Art und Weise der Zielverfolgung, nicht auf den Inhalt der Ziele selbst bezieht. Demgegenüber wird hier vertreten, daß rational ein Verhalten nur dann ist, wenn für die Gesellschaft erwünschte Ziele verfolgt werden, wenn also die Wahl aus einem übergeordneten gesellschaftlichen Wertsystem abgeleitet wird [34]).

3.2.2. Entscheidung und Information

Wie bereits erwähnt, ist derzeit ein wissenschaftlicher Beweis darüber, ob die Regierungsentscheidungen die unter 3.2.1. geforderten Qualifikationen erfüllen, nicht möglich. Wahrscheinlich ist dies nicht der Fall.

Rückschließend von der Vielzahl von Informationsquellen, kann freilich behauptet werden:

1. Entscheidungen der Regierung geht eine derzeit annähernd optimale Alternativenbildung voraus.
2. Entscheidungen der Regierung werden nach bestimmten gesellschaftspolitischen Zielvorstellungen vorgenommen.

3.2.3. Rückwirkungen der Entscheidungen auf die Struktur der Verwaltung

Mit jeder Entscheidung ergreift die Regierung die Initiative zur Gestaltung sozialer Wirklichkeit, der planende Staat versucht sie steuernd in den *Griff zu bekommen.*

Jede veränderte Wirklichkeit stellt die Regierung zudem vor Probleme, die sie selbst und den ihr unterstehenden Apparat betreffen.

Jede Veränderung bedeutet potentiell eine neue Aufgabe; der Fall, daß Aufgaben wegfallen, dürfte wesentlich seltener eintreten. Die von der Exekutive als Gesamtheit zu bearbeitenden Aufgaben werden immer andersartiger, mannigfaltiger und komplizierter, seit sich der Eingriffs- zum Leistungsstaat gewandelt hat. Dieser Veränderung von Zielen und Aufgaben entspricht eine Veränderung der Verwaltung selbst. Einmal hat sich der hierarchische Apparat immer mehr ausgedehnt, zum anderen hat sich die organisatorische Struktur der Organisation [35]) verändert. Sie hat es verstanden, neue Ziele ständig in Struktur umzusetzen.

Ohne hier die besonderen Probleme und Gefahren [36]) erörtern zu wollen, kann festgehalten werden:

1. Zwischen Regierung und sozialer Wirklichkeit findet ein dauernder, sich aus Beobachtungen und Maßnahmen ergebender Kommunikationsprozeß [37]) statt.
2. In Verwaltung und Regierung findet ein dauernder struktureller Optimierungsprozeß statt. Sie ist daher bei allen Mängeln ein relativ gut an die Wirklichkeit angepaßtes dynamisches Gebilde.
3. Die Verwaltung weitet sich aufgrund komplexer werdender Verhältnisse immer weiter aus.

4. Das Zusammenwirken von Regierung und Parlament bei der Grundfunktion Gestaltung der sozialen Wirklichkeit

Die Regierung ist zur Durchsetzung des größten Teils ihrer Entscheidungen auf die Mithilfe des Parlaments angewiesen; das Parlament hat aufgrund seiner Zustimmungsfunktion Gesetze zu geben oder Ermächtigungen im Sinne des Artikels 80 Abs. 1 GG zu erlassen.

Wenn nun das Parlament in gleicher Weise wie die Regierung über die Initiative entscheiden wollte, hätte das zur Voraussetzung:

1. Das Parlament müßte ein eigenes Realitätsmodell haben.
2. Das Parlament müßte das der Initiative zugrunde gelegte Modell der Exekutive kennen.
3. Das Parlament müßte über die der Regierung zur Verfügung stehenden Alternativen verfügen.

---

[28]) allgemein zur Entscheidungstheorie vgl. Gäfgen, 26, 42 f.
[29]) Böhret, 14
[30]) Böhret, 16; vgl. auch Gäfgen, 26
[31]) vgl. Böhret, 17
[32]) Böhret, 26
[33]) etwa Mayntz, 19
[34]) vgl. den entsprechenden Rationalitätsbegriff bei Böhret, 42; insofern liegt ein Widerspruch zu dem auf S. 26 gegebenen Begriff vor
[35]) Mayntz, 147, definiert Organisation als zweckvoll gestaltetes Gebilde. Der Wert dieser Definition für juristische Zwecke erscheint zweifelhaft, da etwa ein Schuh auch als ein rationales Gebilde anzusehen ist.
[36]) einige Hinweise bei Böhret, 56
[37]) Definition bei Wersig - Meyer - Uhlenried, 200

4. Das Parlament müßte sich in seiner Organisations- und Entscheidungsstruktur den strukturellen Veränderungen der Exekutive angepaßt haben.

Dies alles ist nicht der Fall. Das Parlament bekommt aus seinen Informationsquellen kein vollständiges Modell der Realität, seine Informationen sind von vielfältigen Interessen überlagert, unscharf und unvollkommen; sie sind schlecht strukturiert; ihr Verwendungszweck ist nicht auf die Entscheidungsziele des Parlaments abgestimmt.

Das Parlament erfährt zwar die endgültig formulierte Entscheidung, jedoch nichts von dem vorausgehenden Entscheidungsprozeß. Die Gründe der Entscheidung bleiben somit weitgehend verborgen.

Das Parlament hat heute im wesentlichen die gleiche Struktur wie vor 100 Jahren. Seine personelle, die Organisations- und Entscheidungsstruktur ist den heutigen Aufgaben nicht mehr gewachsen. Es ist strukturell unangepaßt.

Diese ungleiche Gewichtung hat dazu geführt, daß bereits im dritten Bundestag 82 % [38]) aller Gesetze auf Initiative der Regierung zurückgingen. Das strukturell angepaßte Organ Regierung erledigt die Aufgaben mit, die das Parlament abgegeben hat. Diese starke Stellung der Regierung entspricht freilich einer inneren Logik des parlamentarischen Regierungssystems und wird jedenfalls von der jeweiligen Regierungsmehrheit auch nicht bestritten.

[38]) vgl. Ehmke (2), E. 20 FN 49,
vgl. aber die Angaben bei Ellwein (4), 83

D. Der Einfluß von Regierungsinformationssystemen auf den Entscheidungsprozeß in Regierung und Parlament

1. Allgemeines zum Begriff des Informationssystems

1.1. Mängel bisheriger Informationsquellen

Wir hatten oben gesehen, daß die Entscheidungen des Planungsträgers Regierung inhaltlich eine bestimmte Qualifikation erfüllen sollen, insbesondere soll den Entscheidungen tunlichst eine bewußte Wahl zwischen mehreren Möglichkeiten vorausgehen; vor allem soll sie nicht ohne Rücksicht auf alle möglichen Auswirkungen ergehen.

Davon ist auch ein dynamisches Gebilde wie die Regierung noch weit entfernt. Die immer komplexer werdende Wirklichkeit erschwert die Anfertigung von Realitätsmodellen. Veränderungen werden dem Entscheidungsträger zu spät gemeldet; zu großer Arbeitsanfall erschwert ausgewogene Entscheidungen. Auf diese Weise wird weitgehend verhindert, daß die Wünschbarkeit gesellschaftspolitischer Ziele in den Entscheidungsprozeß mit einbezogen wird:

Der Entscheidungsträger reagiert auf Veränderungen in der Regel zu spät und wählt zwischen zu wenig Alternativen aus. Planung als Vorwegnahme ist ihm bisher nicht ausreichend gelungen, weil für die für jede Entscheidung von Rang zu berücksichtigende konjunkturelle Entwicklung noch keine hinreichend präzisen Realitätsmodelle gefunden wurden [1]). Diese Mängel können erst dann beseitigt werden, wenn der Regierung ein ausgebautes Informationssystem zur Verfügung steht. Schon hier soll vor allzu optimistischen Erwartungen gewarnt werden: „Politik bedarf der Information, wird aber durch sie nicht ersetzt"; denn „nur wer weiß, was er will, weiß auch, welche Informationen er braucht" [2]).

1.2. Zum Wesen des Informationssystems

Über den Begriff des politischen Informationssystems bestehen weithin Unklarheiten; ebenso ist der eng damit zusammenhängende Begriff der Datenbank noch nicht restlos geklärt [3]). Für diesen Teil der Untersuchung genügt es festzustellen, daß das Regierungsinformationssystem — kurz Informationssystem genannt — im Kern Planungs- und Leitungsinformationssystem sein wird. Da es ein leistungsfähiges System dieser Art bisher noch nicht — auch nicht in den USA — gibt, soll hier nur gefragt werden, was ein derartiges System leisten kann und soll.

1.2.1. Leistungsfähigkeit eines Informationssystems

Entscheidungen beruhen auf Informationen oder Modellen über gegenwärtige und vergangenen Zustände, sowie Vorstellungen über zukünftige Veränderungen usw. [4]). Diese Modelle können der Regierung durch einen ständigen institutionalisierten Informationsfluß gemeldet werden, eben ein Informationssystem. Der Entscheidungsträger hat dann also jederzeit ein mehr oder weniger brauchbares Abbild der Entscheidungssituation.

Im einzelnen erfüllt es folgende Anforderungen [5]):

1. Soziopolitische Indikatoren [6])

   Der Begriff des Indikators baut auf dem hier verwandten Begriff der Information auf. Werden nun unter ganz bestimmten Aspekten zusammengefaßte Informationen „in ihrer inhalt-

[1]) Dies ist ein Grund, weshalb das sog. „Frühkoordinatensystem" des Bundeskanzleramtes nicht die gewünschten Erfolge zeigt, vgl. Der Spiegel 6 (1971), S. 28 ff.
[2]) Ellwein (3), 182
[3]) vgl. etwa Meincke, 67; Osswald, 53; Steinmüller (1), 77; Fiedler (3), 555
[4]) Böhret, 156
[5]) vgl. dazu Böhret, 156
[6]) zum Zusammenhang von Information — Daten und Indikatoren vgl. das Schaubild bei Böhret, 142

lichen Veränderung über die Zeit beobachtet, entstehen Indikatoren" [7]). *Die von den Indikatoren gelieferten Meßwerte repräsentieren dann ganz bestimmte Zustände oder Entwicklungen der Wirklichkeit.*

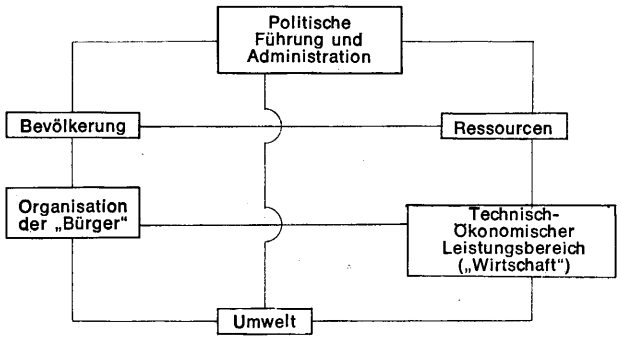
Beispiel [8]):

Der Indikator „Arbeitsmobilität" sei zusammengesetzt aus Informationen über Arbeitsplatzwechsel, Ausbildungsstand, Lohngefälle, Betriebs- und Regionbildung, Verkehrslage, Wohngelegenheit etc. Der Indikator faßt also eine bestimmte Kategorie von speziellen Informationen zusammen und liefert dem Entscheidungsträger eine allgemeine Information über den Gesamtzustand des Arbeitsmarktes.

Da es schon schwierig ist, die für eine Entscheidung relevanten Informationen zu finden, ist es um so mühseliger, aus diesen Informationen Indikatoren zusammenzustellen, die den Zustand des repräsentierten Wirklichkeitsbereichs hinreichend präzise wiedergeben. Solange soweit keine befriedigenden Lösungen gefunden sind, wird es kein leistungsfähiges Informationssystem für die Regierung geben.

2. Das System muß die Auswirkungen vorgenommener Aktionen melden.
3. Die Informationen müssen im richtigen Augenblick an die richtige Stelle kommen.
4. Das System muß permanent auskunftsbereit sein.
5. Der Informationsgehalt muß auf den Entscheidungsträger — also die Regierung — abgestimmt sein.
6. Die Informationen müssen ständig den aktuellen Stand wiedergeben.

1.2.2. Modell eines politischen Informationssystems [9])



Dieses Modell läßt sich — etwas vereinfachend — folgendermaßen erklären:

1. Die Orte, an denen Informationen entstehen, müssen ermittelt werden. Wegen der Vielzahl möglicher Stellen, die Informationen abgeben, muß darauf geachtet werden, daß das zu entwickelnde System überschaubar wird. *Eine Vielzahl derartiger Stellen muß daher zu großen Strukturelementen zusammengefaßt, aggregiert, werden.*

   (Hier durch die Kästchen dargestellt.)

2. Die Informationsströme zwischen den Strukturelementen oder Aggregaten müssen gemessen werden. Diese Informationsströme machen dann den jeweiligen Systemzustand sichtbar. *Die Informationen über Zustand und Veränderung der Aggregate seien Leistungen genannt.* Wie wir gesehen haben, wird der Inhalt dieser Informationsströme durch die Indikatoren repräsentiert.

Ein derart aufgebautes System kann zweierlei leisten:

1. Es bietet die jeweils benötigten Einzelinformationen.
2. Es liefert Vorschläge für Maßnahmen, wenn sich in den Informationsströmen Veränderungen ergeben haben.

2. Der Einfluß von Informationssystemen auf das Zusammenwirken von Regierung und Parlament

2.1. Allgemeines

Die bisher gesicherten Erkenntnisse über Informationssysteme sind gering. Selbst wenn es gelänge, in absehbarer Zeit ein Informationssystem in der Bundesrepublik zu errichten, sind erhebliche Schwierigkeiten zu erwarten (Schwächen des Ressortprinzips, Widerstände der Ministerialbürokratie, mangelnde Berechenbarkeit der konjunkturellen Entwicklung). Entsprechend sind bisher keine literarischen Stimmen bekanntgeworden, die sich wissenschaftlich mit der Problematik der Regierungsinformationssysteme in der Bundesrepublik auseinandersetzen. Das bedingt zweierlei:

— Mangels eigener Erfahrungen muß auf entsprechende Entwicklungen in den USA zurückgegriffen werden. Freilich ist zu betonen, daß das staatsrechtliche Verhältnis von Kongreß und Präsident nur sehr beschränkt für deutsche Verhältnisse anwendbar ist. Außerdem wurden die Erfahrungen auch dort nicht an einem Informationssystem, sondern dem sog. *Planning — Programming — Budgeting System (PPBS)* gewonnen [10]). Diese sind freilich insoweit vergleichbar, als das PPBS eine Art notwendige Vorstufe für ein Informationssystem und im übrigen gegenüber sonstigen Entscheidungshilfsmitteln umfassend ist [11]).

— Alle Fragestellungen sind hypothetisch und wissenschaftlich nicht im eigentlichen Sinne beweiskräftig. Freilich sprechen die Tatsachen für sich.

[7]) Böhret, 141
[8]) nach Böhret, 141
[9]) In Anlehnung an Böhret, 158 ff. Böhrets Buch stellt im wesentlichen die einzig einschlägige Veröffentlichung dar. Die zahlreich vorhandene Literatur über Management — Informationssysteme bedarf im Hinblick auf das Regierungsinformationssystem dringend einer wissenschaftlichen Aufarbeitung.
[10]) vgl. hierzu die kritischen Bemerkungen von Narr und Böhret, 174 ff.
[11]) Böhret, 226

2.2. Die am PPBS gewonnenen Erfahrungen

2.2.1. Für den Bereich der Exekutive

Nach Böhret [12]) lassen sich schon jetzt folgende Entwicklungen feststellen:

1. Die Exekutive der USA hat an Entscheidungsmacht gewonnen.
2. Sie hat ihren Handlungsspielraum wesentlich erweitern können, durch:
   — Ausweitung der Bürokratie
   — Zentralisierung von Entscheidungsmacht, wobei die Beurteilung insoweit nicht einheitlich ist [13]).
3. Sie hat ihre Argumentationsposition wesentlich verbessern können.
   Die vorgelegten, systemanalytisch ermittelten Programme sind von Kongreßausschüssen weniger „leicht als bisher *politisch* abzulehnen".
4. Die gleichzeitig von ihr eingeplanten Maßnahmen gegen die Abwehr parlamentarischen Widerstandes vermindern das Ablehnungsrisiko der vorgelegten Programme.
5. Sie gibt dem Kongreß nur unvollkommene Informationen, um seine Zustimmung mit hoher Wahrscheinlichkeit zu erhalten, und weist nicht auf alternative Möglichkeiten hin.
6. Die Exekutive ist wesentlich selbstsicherer geworden [14])
7. Der neugewonnene exekutive Sachverstand wird unkritisch anerkannt: Die Beweise der Sachgerechtigkeit der vorgelegten Programme werden scheinbar zwingender.

[12]) S. 240 ff.
[13]) Böhret, 236
[14]) Böhret, 247
[15]) Böhret, 249
[16]) S. 251

2.2.2. Für den Kongreß

1. Die Haltung der Abgeordneten zeichnet sich aus durch „Ignoranz, Argwohn, Unkenntnis, wenig sachliche Analyse" [15]).
2. Er fällt nur politische Entscheidungen, läßt entsprechend den gesellschaftlichen Nutzen von Programmen ggf. außer acht.
3. Er entdeckt politisch unerwünschte Programme nicht und stimmt schlechten ggf. aus Unkenntnis zu.
4. Die eingeplanten Reaktionen der Parlamentarier führen zu einer erheblichen Schwächung ihrer Politik.

2.2.3. Zusammenfassende Beurteilung

Zusammenfassend kann mit Böhret [16]) festgehalten werden:

1. Die Abwägung von Machtverlust und Machtzuwachs der Legislative bei der regierungsweiten Einführung des Planning — Programming — Budgeting Systems haben zu einer Stärkung der Exekutive geführt.
2. Bei einem weiter verbesserten Instrumentarium, insbesondere bei Einsatz eines auf Indikatoren aufbauenden Informationssystems, wird der Machtverlust des Parlaments weiter ansteigen.

Es besteht kein Anlaß, die Brauchbarkeit dieser Aussagen für bundesrepublikanische Verhältnisse zu verneinen. Dies um so mehr, als der amerikanische Kongreß wegen der streng gewaltenteiligen Staatsorganisation der USA eine wesentlich stärkere Stellung als das deutsche Parlament hat.

E. Das Verhältnis der Parlamentarischen Informationsquellen zueinander

Wir hatten gesehen, daß die Informationsquellen des Parlaments kein rationales für Entscheidungen relevantes Modell von Wirklichkeit liefern und daß das Parlament gegenüber den zu bewältigenden Aufgaben strukturell unangepaßt ist. Wenn das Parlament sich ein derartiges Modell durch eigene Maßnahmen und ohne Rückgriff auf Exekutivinformationen verschaffen könnte, wäre der dem Gutachten gestellten Problematik einiges von ihrer Brisanz genommen.

Die Frage lautet daher: Kann ein Parlamentarisches Informationssystem ohne von der Exekutive bereitzustellende Informationen auskommen?

Der Aufbau eines parlamentseigenen Informationssystems wurde bisher von Steinmüller [1]) und Böhret [2]) nachdrücklich gefordert. Aus einer von Böhret [3]) veranstalteten Meinungsumfrage geht hervor, daß etwa die Hälfte der US-Parlamentarier entsprechende Projekte unterstützen würde [4]). Freilich wären derartige Informationssysteme von vornherein mit einem großen Mangel behaftet: Das derzeit vorhandene Wissen läßt sich in Anlehnung an Ellwein [5]) etwas unscharf unterteilen:

1. *Das Apparatwissen* umfaßt alle Informationen, die in der der Regierung unterstehenden Bürokratie anfallen.
2. *Das Gesellschaftswissen* umfaßt alle Informationen, die in der Gesellschaft produziert und reproduziert werden und mit der diese auf die Umwelt reagiert.
3. *Das Wissen der Zeit* umfaßt Kenntnisse über wissenschaftliche und technologische Entwicklung, Verständnis der wesentlichen ideellen Auseinandersetzungen und ihres sozialen Bezuges.

[1]) (1), S. 67 f.
[2]) S. 259
[3]) a. a. O.
[4]) S. 259 FN 144
[5]) (3), 174 f.

So unscharf diese Aufzählung auch sein mag, so zeigt sie doch, daß es Informationen gibt, die *nur* in der Verwaltung anfallen und nirgends sonst. Diese Tatsache erklärt auch die Bedeutung, die der Integration im Einwohnerwesen [6]) beigemessen wird: Die Einwohnerdaten bilden die wichtigste Grundlage für Planungsinformationen, sie sind für die Bildung soziopolitischer Indikatoren unerläßliche Voraussetzung. Diese Informationen liefern die sonstigen Informationsquellen mit Sicherheit auch dann nicht, wenn das Parlament über ein eigenes Informationssystem verfügt. Es ist daher zutreffend, wenn sowohl ein eigenes Parlamentarisches Informationssystem (PAIS) als auch parlamentarische Zugriffsrechte gefordert werden [7]) [8]), wobei freilich das PAIS dem allgemeinen staatlichen Informationssystem als Subsystem zu integrieren ist.

Freilich soll die Problematik einer derartigen Forderung nicht übersehen werden: Exekutiv-Informationen liefern in jedem Fall ein informationelles Abbild, das an den Bedürfnissen des Entscheidungsträgers Regierung ausgerichtet ist [9]). Die Lösung dieses Problems wird Techniker und Politiker zukünftig vor schwere Aufgaben stellen.

[6]) vgl. dazu das Buch von Meincke
[7]) Steinmüller (1), S. 67; auch (2), S. 8 f.
[8]) In dieser Richtung sind wohl auch die bei Böhret, 171 abgedruckten Vorschläge des Kongreßmitgliedes R. Mc Clory zu verstehen.
[9]) ebd. (1), S. 67; vgl. auch Simitis (2), 674 und Deutsch, 54 ff.

2. Teil

Juristische Untersuchung des Informationsaustausches zwischen Exekutive und Parlament

A. Vorbemerkung

In diesem Abschnitt soll untersucht werden, in welcher Weise unser Rechtssystem den im ersten Abschnitt geschilderten tatsächlichen Verhältnissen Rechnung trägt und in welcher Weise es auf die durch die Einführung von Informationssystemen zu erwartenden Veränderungen vorbereitet ist. Schließlich soll gezeigt werden, wie Schwächen der derzeit herrschenden Meinung überwunden werden können.

Das Grundgesetz und sonstige Rechtsnormen regeln den Faktor Information, soweit er das Verhältnis Exekutive — Parlament betrifft, nicht ausdrücklich; freilich kennt das Grundgesetz an verschiedenen Stellen Vorschriften, die das Problem behandeln. Diese sollen nunmehr untersucht werden.

B. Die herrschende juristische Doktrin

1. Das allgemeine Informationsrecht des Parlaments

Nach v. Mangoldt — Klein [1]) soll es sich hierbei um „das über bloße Empfehlungen und Ersuchen hinausgehende und als solches anzuerkennende Auskunfts- und Informationsrecht des Bundestages gegenüber der Bundesregierung hinsichtlich innen- und außenpolitischer Fragen" handeln.

Diese Meinung ist vereinzelt geblieben und wird — soweit ersichtlich — sonst nicht vertreten. Zwar könnte, so wird argumentiert [2]), das Parlament als solches versuchen, die Regierung mit politischen Mitteln zu zwingen, ihm die gewünschten Informationen herauszugeben. Einen Rechtsanspruch habe es jedoch nicht. Beispielhaft für die insoweit einmütige Auffassung ist eine Entscheidung des Hessischen Staatsgerichtshofes vom 24. November 1966 [3]): „Die Verfassung legt der Regierung keine Rechtspflicht auf, über alle Vorgänge erschöpfend Auskunft zu erteilen, wenn die Regierung auch jederzeit Erklärungen abgeben kann". Ein allgemeines parlamentarisches Informationsrecht wird also von Rechtsprechung und Literatur nicht anerkannt.

[1]) S. 872; vgl. auch S. 1195
[2]) Düwel, 132
[3]) in DÖV 67, 55

2. Die Interpellationsrechte [4])

2.1. Terminologie

Als Interpellationsrechte werden hier alle Rechte verstanden, die die Regierung verpflichten, auf Fragen von Parlamentariern Rede und Antwort zu stehen [5]). Interpellationsrechte können also nicht mit

[4]) Die Abgrenzung der Interpellationsrechte vom allgemeinen Informationsrecht ist unklar. v. Mangoldt-Klein, a. a. O., gehen offensichtlich davon aus, daß das allgemeine Informationsrecht weiter geht als die Interpellationsrechte.
[5]) so auch Maunz - Dürig - Herzog, Artikel 43 N. 1; Gehrig, 292 FN 233

dem Zitierungsrecht des Artikels 43 GG und entsprechenden Rechten der Geschäftsordnung gleichgesetzt werden. Diesem Fehler unterliegt auch die im übrigen sehr ungenaue Dissertation Sauers [6]), der so Maunz zum Befürworter einer Auffassung macht, die er ausdrücklich nicht vertritt [7]). Bezogen auf die vermittelten Informationen kann schlagwortartig formuliert werden: *Interpellationsrechte geben Tatsachenkenntnis durch Vermittlung der Regierung* [8]).

2.2. Das sogenannte Zitierungsrecht der Regierung, Aritkel 43 GG

Der Bundestag und seine Ausschüsse können die Anwesenheit der Regierung verlangen, Artikel 43 Abs. 1 GG. Anwesenheit bedeutet nicht „stummes Dasitzen, sondern die Pflicht auf Fragen zu antworten" [9]).

Artikel 43 Abs. 1 GG begründet nach einmütiger Meinung [10]) eine Informationspflicht der Regierung. Es besteht weiter Einmütigkeit, daß die Antwortpflicht nur eine formelle ist. Es liegt im Belieben des Regierungsmitgliedes, welche Antwort es geben will, ggf. kann es die Antwort sogar mit „plausibler Begründung" verweigern, etwa wenn Belange der Bundesrepublik Deutschland gefährdet sind [11]).

2.3. Die sogenannten Interpellationsrechte der Geschäftsordnung des Bundestages

Darunter werden hier gefaßt:

— Große Anfragen, §§ 105 ff.
(Verlangen von 30 Bundestagsmitgliedern)

— Kleine Anfragen, § 110
(Mitglieder in Fraktionsstärke)

— Mündliche Anfragen, § 111
jeder einzelne Abgeordnete ist zur Frage berechtigt. Beantwortung erfolgt in der monatlichen Fragestunde.

— Auskunftserteilung über die Ausführung von Bundestagsbeschlüssen, § 115 f.

Die geschäftsordnungsmäßigen Fragerechte zeitigen gegenüber den Rechten des Artikels 43 GG folgende Besonderheiten:

Die Bundesregierung ist zur Beantwortung der gestellten Fragen rechtlich nicht verpflichtet [12]). Die Geschäftsordnung des Bundestages als autonome Satzung des Organs Parlament könne, so wird von der h. M. argumentiert, eine Informationspflicht der Regierung nicht begründen. Artikel 43 GG erfordere insoweit einen Beschluß des Bundestages, die Fragerechte der Geschäftsordnung §§ 105 ff. seien aber als Minderheiten„rechte" ausgestaltet. Die davon zu unterscheidende Frage, daß die Regierung in aller Regel die Antwort nicht verweigern wird, ist für die normative Betrachtung ohne Belang [13]). Anzumerken bleibt noch, daß die Verfassungen von Hamburg (Artikel 24), Bremen (Artikel 98) und dem Saarland (Artikel 78 Abs. 2) den der Geschäftsordnung des Bundestages entsprechenden Interpellationsrechten Verfassungsrang gegeben haben.

Weiterhin besteht Einmütigkeit [14]), daß die Bundesregierung Umfang und Art der Informationen nach ihrem Belieben bestimmen kann. Eine Gewähr für die Richtigkeit der Information ist somit rechtlich nicht gegeben [15]).

3. Das Enqueterecht des Artikels 44 GG

3.1. Terminologie

Das Enqueterecht ist „das dem Parlament zustehende Recht, Tatsachen und Vorgänge festzustellen, deren Kenntnis zur Ausübung der parlamentarischen Funktionen erforderlich ist" [16]). Der wesentliche Unterschied zu den Interpellationsrechten besteht darin, daß hier *Tatsachenkenntnis durch eigene parlamentarische Ermittlungstätigkeit* erreicht wird, während dort Tatsachen nur durch die Regierung vermittelt werden [17]). Insofern bilden sie die einzige Möglichkeit, die Verwaltung ohne Zwischenschaltung der Regierung zu kontrollieren.

3.2. Umfang und Grenzen der Untersuchungsbefugnis

Der Umfang des Rechts wird allgemein durch die auf Zweig [18]) zurückgehende „Korollartheorie" bestimmt. Sie besagt: Das Ermittlungsrecht steht dem Parlament zu, wird aber durch den Ausschuß ausgeübt [19]). Der Untersuchungsausschuß kann keinen selbständigen, vom Willen des Parlaments unabhängigen Wirkungskreis haben, die Übertragung besonderer Rechte sei kein Beweis für die Unabhängigkeit [20]).

---

[6]) S. 27; vgl. auch K. F. Arndt, 112; Scholler, 407 f.
[7]) in Maunz - Dürig - Herzog, Artikel 44 N. 32
[8]) vgl. Steffani (3), 16 FN 1
[9]) Anschütz, Artikel 33 N. 1
[10]) Gehrig, 292 f.; Trossmann, 151; v. Mangoldt - Klein, 937; Drexelius - Weber, Artikel 23 N. 3; Schäfer, 231; etwas anders wohl Frenkel N. 614; unklar Düwel, 132
[11]) ganz h. M.: Maunz - Dürig - Herzog, Artikel 43 N. 8; Frenkel N. 614; v. Mangoldt - Klein, 937; Trossmann, 151: „Nur die generelle Verweigerung ist unzulässig"; vgl. auch Ehmke (2), E 32
[12]) ganz h. M.: Frenkel N. 613, 682; Gehrig, 295; Ritzel - Koch, § 106 N. 1 a; Lechner - Hülshoff, § 106 N. 1; Stein, 68 ff.; K. F. Arndt, 112; vgl. auch schon für das Recht der WRV Perels, 459; Marschall v. Bieberstein, 536 FN 94 und für das Deutsche Reich Hatschek (1), 106 a. A. v. Mangoldt - Klein, 1195; Sauer 40 f.; Scholler, 407 f. und Trossmann, 151, nach dem eine generelle Informationspflicht bestehen soll, im Einzelfall könne die Bundesregierung jedoch von der Beantwortung absehen.
[13]) Ellwein, (1), 233
[14]) insoweit auch v. Mangoldt - Klein, a. a. O.
[15]) vgl. Gehrig, 295 FN 248
[16]) Zweig, 265
[17]) Steffani (3), 16 FN 1; Ridder (1), Sp. 1170
[18]) S. 267; vgl. auch Partsch (2), 467
[19]) Steffani (3), 13
[20]) Lammers, 461, skeptisch Partsch (2), 461

Der Umfang des Untersuchungsrechts ergibt sich danach aus:

1. der Allgemeinen Parlamentskompetenz

   Der Untersuchungsausschuß ist Werkzeug des Parlaments und in seiner Existenz vom Willen des Parlaments abhängig. In der Entscheidung über Inhalt und Ziel der Untersuchungen ist der Ausschuß daher gänzlich auf das Parlament angewiesen [21]).

2. Zweck und Ziel des Untersuchungsinstituts

   Ganz allgemein haben Untersuchungsausschüsse den Zweck, „Tatsachen und Vorgänge zu untersuchen, deren Kenntnis zur Ausübung der parlamentarischen Funktionen erforderlich ist" [22]), „kurz: sie haben der Vorbereitung von Beschlüssen des Parlaments zu dienen" [23]).

3.3. Einzelfragen

Eine ausführliche Erörterung des Enqueterechts würde den Rahmen der vorliegenden Untersuchung sprengen. Es genügt hier die Darstellung einiger Einzelfragen, die umstritten sind, solange es ein Enqueterecht gibt (vgl. Artikel 34 WRV). Auch die Verhandlungen des 45. Deutschen Juristentages haben insoweit keine Klarheit bringen können.

3.3.1. Beweiserhebungen

Strittig [24]) ist nach wie vor die Wendung des Artikels 44 Abs. 2 GG „Auf Beweiserhebungen finden die Vorschriften der Strafprozeßordnung sinngemäß Anwendung".

[21]) Steffani (3), 85
[22]) Zweig, 263
[23]) Steffani (3), 86
[24]) gute Übersicht über den Streitstand bei Düwel, 133 f.
[25]) Dafür ist die h. M.: Maunz - Dürig - Herzog Artikel 44 N. 57 und FN 4, m. w. N.; Bonner Kommentar, Artikel 44 N. 8; Ehmke (1), 418 f.; Keßler, 323 f.; Steffani (2), 173; vgl. auch schon M. Weber, 340 f.; a. A., aber mit völlig unzureichender Begründung Düwel, 137; siehe noch für die Zeit der WRV: Koellreuther, 858; Lammers, 473; Anschütz Artikel 34 N. 8.
[26]) E 173 Nr. 9
[27]) Maunz - Dürig - Herzog, Artikel 44 N. 17; Lechner - Hülshoff, § 63 N. 3; Hamann - Lenz, Artikel 44 N. B 2; Schäfer, 288; Keßler, 324; Partsch (3), 14, Gehrig, 287; gute rechtsvergleichende Übersicht bei Frenkel, N. 876 ff.; soweit ersichtlich a. A. nur Steffani (1), 173; vgl. auch Ehmke (2), E 32, 36
[28]) Entscheidung vom 22. Januar 1922, in: RGZ 104, 423 ff.; ständige Rechtsprechung, vgl. auch die Entscheidung des vorläufigen Staatsgerichtshofes vom 12. Juli 1921, in: Lammers - Simons, 879 ff. (Besprechung bei Poetzsch, 210 ff.); Bay. VGHE vom 30. November 1955, in: VGHE 8, II. Teil, 103; Hess. StGH, Urteil vom 24. November 1966, in: DÖV 67, 51 ff.
[29]) v. Mangoldt - Klein, S. 956; Lechner - Hüllshof, § 63 GOBT, N. 4; dazu Maunz - Dürig - Herzog, Artikel 45 a N. 8
[30]) Maunz - Dürig - Herzog, Artikel 44 N. 17; Sauer, 58; vgl. schon Lammers, 466; a. A. wohl nur Steffani (1), 473; Ehmke (2), E 32, 36
[31]) in DÖV 67, 56
[32]) vgl. Hatschek (1), 105 f.; Gehrig, S. 61

Über die hier interessierende Frage, ob die Auskunft oder Akteneinsicht gemäß § 54, bzw. § 96 StPO unter Berufung auf ein überwiegendes öffentliches Interesse verweigert werden darf, konnte bisher keine Einmütigkeit erzielt werden [25]).

Nach wohl herrschender Meinung sind die §§ 54, 96 StPO entgegen Artikel 44 Abs. 2 GG unanwendbar, wobei wohl, wie die Beschlüsse des 45. Deutschen Juristentages zeigen [26]), Ausnahmen zu machen sind, wenn „Gründe der Staatssicherheit es gebieten".

3.3.2. Dauerhafte Untersuchungsausschüsse

Ungeklärt ist weiter, ob die dauerhafte Einsetzung von Ausschüssen zur ständigen Information und fortlaufenden Kontrolle der Verwaltung möglich ist.

Die ganz h. M. [27]) hält derartige Ausschüsse im Anschluß an ein Urteil des Staatsgerichtshofes für das Deutsche Reich [28]) für verfassungswidrig.

Als einzig zulässiger dauerhafter Untersuchungsausschuß wird die Vorschrift des Artikels 45 a GG angesehen. [29])

3.3.3. Ex-Post-Kontrolle

Ungeklärt ist weiter, wie sich das Enqueterecht zum Initiativrecht der Bundesregierung verhält. Allgemein [30]) nimmt man an, daß Untersuchungen in der Regel nur als Ergebniskontrolle ex-post vorgenommen werden dürfen. Exemplarisch für diese Auffassung ist ein Urteil des Hessischen Staatsgerichtshofes [31]). Das Gericht argumentiert:

Kontrollmaßnahmen, die geeignet seien, Initiativen der Regierung zu beschränken, die Vorbereitung in eine bestimmte Richtung zu lenken, zu hemmen oder zu stören, seien unzulässig. „Das Mittel der parlamentarischen Untersuchung darf dann nicht verwandt werden, wenn auch nur die Gefahr besteht, daß das Handeln der Regierung im Initiativbereich durch die Erhebungen eines Untersuchungsausschusses beeinträchtigt werden könnte".

4. Kritische Anmerkungen zur herrschenden Auffassung

Auffällig ist zunächst die Einmütigkeit, mit der dem Parlament Informationen verweigert werden, obwohl das Parlament, wie ausgeführt, seine Aufgaben gar nicht ohne Exekutivinformationen erfüllen kann. Das dürfte daran liegen, daß die angeführten Rechtsfragen nicht im Brennpunkt juristischen Interesses liegen. Das führt zu einer kasuistischen Problemsicht, die zu den entscheidenden Kernfragen nicht mehr vorstößt. Das hat seinen Grund weiter darin, daß der Charakter der vorgeführten Rechtsinstitute als Informationsrechte völlig verkümmert und denaturiert ist:

Historisch sind die Interpellationsrechte etwa ganz eindeutig als Mittel der Information entstanden [32]); gleichwohl begreift man sie in der Hauptsache als

Kontrollrechte [33]) und meint, wie etwa Sauer [34]), „die Information (sei) nur Durchgangszweck". Die maßgebliche Bedeutung der Information für die Bedeutung heutiger Informationsstrukturen muß so unerkannt bleiben [35]).

Die gleiche Entwicklung ist bei der Auslegung des Enqueterechts zu verzeichnen [36]). Ursprünglich auch und ausdrücklich auf parlamentarische Information angelegt [37]), hat sie durch Max Weber [38]), den „Vater des modernen Enqueterechts", eine Richtung bekommen, die ausschließlich den Aspekt der Verwaltungskontrolle betonte [39]). Damit hat das parlamentarische Untersuchungsrecht „eine Wendung genommen, die es für die Informationsbeschaffung (praktisch) ungeeignet macht" [40]). Schon das Wort *Untersuchungs*ausschuß legt sich einseitig auf Mißstandsuntersuchungen fest, wo es doch ebensosehr und in erster Linie um die Erhebung von Tatsachen geht [41]). Die historische Wurzel des Enqueterechts als Zeichen des Mißtrauens des Parlaments gegenüber der Exekutive [42]) vermag daran nichts zu ändern.

Dieser einseitigen Sicht steht ein Mangel an theoretischer Begründung im übrigen gegenüber. Da wird die Zulässigkeit von dauerhaften Untersuchungsausschüssen unter Berufung auf das Gewaltenteilungsprinzip abgelehnt, ohne daß auch nur die Frage gestellt wird, ob in einem parlamentarischen Regierungssystem derartige Argumente zulässig sind [43]). Durchweg fehlen Begründungen, die etwa erklären könnten, warum die Exekutive — außer im Falle des Artikels 44 GG — den Parlamentariern nur die Informationen zu geben braucht, die sie ihr geben will.

Die Sicht der vorgestellten herrschenden Meinung vermag durchweg nicht zu befriedigen. Sie führt die Diskussion mit fast den gleichen Argumenten, die schon unter der Geltung der Reichsverfassung von 1871 und der Weimarer Reichsverfassung gebraucht wurden. Sie wird in keiner Weise den veränderten Informationsstrukturen einer moderen Verwaltung gerecht und ist überdies in entscheidenden Fragen — wie bei den Untersuchungsausschüssen gezeigt — kontrovers. Damit bietet sie nur wenig Ansatzpunkte, die den Wandlungen der Regierungsform und den durch den Einsatz von Informationssystemen drohenden Gefahren gerecht werden könnten. Daher ist ein neuer theoretischer Ansatz erforderlich, der im folgenden in Grundzügen vorgeführt werden soll. Denn noch immer gilt die polemische Formulierung A. Arndts [44]) aus dem Jahre 1964 zu Recht:

„Ein Parlament im Atomzeitalter nicht anders zu informieren und arbeiten zu lassen als im Zeitalter der Postkutsche, ist für Volk und Staat lebensgefährlich".

Aus diesem Grund ist daher auch immer wieder gefordert worden, das Untersuchungsrecht „mehr unter den allgemeinen Gesichtspunkten einer guten, vollständigen und eigenständigen Information zu stellen" [45]).

[33]) Keller-Raupach, 66; Schäfer, 230 ff.; vgl. aber die differenzierende Betrachtung von Frenkel N. 570
[34]) S. 14
[35]) vgl. auch die in anderem Zusammenhang gefallene Kritik von Simitis (2), 677
[36]) vgl. auch E. Kaufmann, 319
[37]) vgl. etwa Steffani (1), 160 und passim
[38]) S. 340 ff.
[39]) Ehmke (2), E 9; Steffani (1), 77
[40]) Schäfer, 299
[41]) vgl. schon Zweig, 281 f.; Steffani (1), 13
[42]) Steffani (2), 163
[43]) vgl. Ehmke (2), E 32 f.
[44]) (2), 290
[45]) v. Heydebreck, E 66; Arndt, 290

C. Versuch einer Theoriebildung für den Informationsaustausch zwischen Parlament und Exekutive

0. Vorbemerkung

Die Regelung des Informationsaustausches und die Auslegung durch die h. M. ist schon jetzt unbefriedigend [1]). Um so mehr wird das bei dem Aufbau von Informationssystemen der Fall sein. Für eine Theorie, die diese neueren technischen Mittel in die Überlegungen mit einbezieht, lassen sich vorerst nur einige allgemeine Anforderungen aufstellen:

„Die Rechtsordnung kann ihre Aufgabe nur durch eine zukunftsorientierte Interpretation ihrer gegenwartsbezogenen Normen erfüllen", wie Simitis [2]) plastisch formuliert, andernfalls laufe sie Gefahr, der Entwicklung hinterher zu hinken [3]). Sie muß sich also „dem technischen Fortschritt öffnen, will sie mehr sein als nur ein System zur Aufrechterhaltung überkommener Strukturen" [4]). Sie hat die Chancen moderner Informationsverarbeitung zu nutzen, ohne die Effizienz nach Art von Bilderstürmern zu beseitigen. Sie hat also um- und mitzudenken. Das von Wieacker [5]) beklagte „futurologische Pathos" derartiger Auffassungen muß und soll dabei in Kauf genommen werden.

[1]) deswegen würden schon immer neue Regelungen gefordert, vgl. etwa A. Arndt (2); 292; Ehmke (2), E 35
[2]) (2), 673
[3]) Simitis (2), 677
[4]) Steinmüller (1), 3
[5]) S. 286; er spricht vom „futurologischen Pathos der Informationstheorie"

1. Parlamentarisches Regierungssystem und Information des Parlaments

Die Bundesrepublik Deutschland hat ein parlamentarisches Regierungssystem. Das ist freilich nicht unbestritten. Loewenstein [6]) etwa bezeichnet die Bundesrepublik Deutschland als „demo-autoritär" zumindest während der Dauer einer Legislaturperiode. Die politische Führung — obwohl demokratisch in der Entstehung — sei autoritär [7]) und regiere ohne jede Begrenzung durch die Wählerschaft. Dieser Klassifizierungsversuch erscheint ebensowenig fruchtbar wie der Hinweis, die Bundesrepublik Deutschland sei eine Mischform aus englischem und amerikanischem Regierungssystem [8]). Rechtsfolgen können aus derartigen Klassifizierungen nur dann abgeleitet werden, wenn feststeht, daß diese Klassifizierung auch heute zutrifft.

Richtig ist nur, daß das parlamentarische System in Deutschland historisch eine bewußte Abkehr von der Monarchie darstellt, die dem zu Macht gekommenen liberalen Bürgertum auch die noch verbliebenen exekutiven Freiräume überantworten sollte. Insofern beantwortet das parlamentarische System die Frage der Regierungsform, d. h., welche unmittelbaren Staatsorgane an der Willensbildung mitwirken [9]), der Idee nach dahin, *daß der Staat vom Parlament regiert wird.*

Dieses Bild läßt sich auch für die Bestimmungen des Grundgesetzes nachweisen. So hat es die Regierung durch vielfältige Auskunfts- und Informationsrechte, Mitwirkungs- und Kontrollrechte (Mißtrauensvotum, Ministerverantwortlichkeit) an den Willen des Parlaments gebunden und gemäß Artikel 20 Abs. 2 GG die staatlichen Funktionen auf verschiedene Funktionsträger verteilt mit dem Ziel, durch ein kunstvolles System von Aufgabengliederungen, Mitwirkungspflichten der Staatsorgane usw. ein Gleichgewicht, sog. „system of check and balance", der gesellschaftlichen und politischen Kräfte herbeizuführen [10]).

[6]) S. 93 f.
[7]) zum Begriff vgl. Loewenstein, 53
[8]) vgl. etwa Keller — Raupach, 90 f.
[9]) Küchenhoff, 189
[10]) näheres bei Loewenstein, 127 ff.; eine gute Übersicht über das Balancesystem befindet sich bei Ermacora, II, (1) 616 ff.
[11]) (1), 213
[12]) zu den Konsequenzen für unser heutiges Verfassungssystem, vgl. Ellwein (4), 54 ff.
[13]) vgl Stein, 26 f.; Odewald, 74 f.; Gehrig, 94
[14]) vgl. v. Heydebrek, E 68; Keller-Raupach, 42, vgl. aber S. 94; und die bei Odewald, 74 in FN 38 und 39 Genannten
[15]) so v. Heydebrek, a. a. O.
[16]) Auch der Sturz der Regierung Erhard bildet insoweit keine Ausnahme.
[17]) (2), 30 ff.
[18]) vgl. Keller-Raupach, 94
[19]) statt aller Gehrig, 94
[20]) vgl etwa die z. T. widersprüchlichen Ausführungen von Gehrig, 94, 101 f., 128 f., 168, 243, 247 f.
[21]) (1), 218
[22]) S. 101

Es besteht kein Zweifel, daß ein derart relativ statisches Modell nicht in der Lage ist, die Dynamik gesellschaftlicher Prozesse und ihre schließliche Integraton in den Rechtsprozeß zu erklären: Das parlamentarische System derart juristisch behandeln zu wollen, hieße „Wasser mit einem Sieb aufzufangen", wie U. Scheuner [11]) schon 1927 formuliert hat.

1.1. Der Dualismus von Exekutive und Parlament

Eine dualistische Gegenüberstellung von Parlament und Exekutive mag im Zeitalter des bürgerlichen Konstitutionalismus noch sinnvoll gewesen sein, als sich im Bürgertum (verkörpert im Parlament) und dem Monarchen (verkörpert durch die Exekutive) zwei reale politische Kräfte gegenüberstanden [12]) und die Gesellschaft durch wenige, nicht plurale Gruppeninteressen gekennzeichnet war. Dieses Spannungsverhältnis ist heute wegen der funktionellen Identität von Regierung und Regierungsmehrheit aufgehoben [13]).

Andererseits [14]) wird argumentiert, das traditionelle Spannungsverhältnis sei erhalten geblieben, nur spiele sich dann die Auseinandersetzung nicht öffentlich, sondern in den Zimmern der Fraktionskreise ab [15]). Gerade dieses Argument beweist die Richtigkeit der hier vertretenen Auffassung. In jedem Fall tritt der Block Regierung — Verwaltung — Regierungsmehrheit mit einem einheitlich formulierten Willen an die Öffentlichkeit. Man könnte den Befürwortern der Dualismus-Theorie nur dann zustimmen, wenn bewiesen wäre, daß die Regierungsfraktion einen Willen unabhängig von der Regierungsmehrheit zu bilden imstande ist, wenn sie etwa geschlossen gegen Regierungsvorlagen stimmt und die Mittel der parlamentarischen Kontrolle gegen den Willen der Regierung ausübt, etwa den Bundeskanzler durch konstruktives Mißtrauensvotum abwählt [16]). Dies alles ist nicht der Fall, im Gegenteil, die Waffen des Parlaments sind stumpf geworden. Nicht regiert das Parlament die Regierung, was W. Weber [17]) noch von der „Entmachtung der Exekutive" sprechen ließ, sondern „die Regierung regiert das Parlament". Es wäre daher im höchsten Maße unrealistisch, wieder eine „Suprematie" des Parlaments gegenüber der Regierung fordern zu wollen [18]). Ein solches Spannungsverhältnis kann daher heute allenfalls noch zwischen dem Block Regierung — Verwaltung — Regierungsmehrheit und der Opposition gesehen werden [19]). Trotzdem wäre es falsch zu sagen, die Funktionen des Gesamtparlaments seien auf die parlamentarische Opposition übergegangen [20]), eine Meinung, die Ellwein [21]) etwas zu polemisch als „Ammenmärchen" bekämpft.

Richtig daran ist, daß die Chancen der Opposition, eigene alternative Vorstellungen durchzusetzen und Kontrollmaßnahmen Konsequenzen für die Regierungsmehrheit folgen zu lassen, denkbar gering sind. Wenn Gehrigs [22]) Bemerkungen, eine tatkräftige Opposition bewirke „Mäßigung und Toleranz" der Regierung, gleichwohl zutreffend ist, so hat das freilich andere Gründe. Es wird bewirkt durch den

Pluralismus oligarchischer Gruppen [23]), im folgenden auch intermediäre Gewalten genannt.

1.2. Der Pluralismus intermediärer Gewalten

Die Träger realer Macht, im konstitutionellen System noch interessenmäßig unterscheidbar, haben sich in einer Gesellschaft, die durch eine Vielzahl pluraler Gruppeninteressen gekennzeichnet ist, gewandelt. An ihre Stelle sind die sog. intermediären Gewalten getreten [24]), die alle auf den Staat einwirken. Als wesentliche sind hier zu nennen:

— die Interessengruppen (Verbände wie Gewerkschaften, Arbeitgeberverband etc.),

— die öffentliche Meinung (Massenkommunikationsmittel),

— die Parteien (Regierungs-, Oppositionsparteien),

— desintegrierte Gruppierungen (außerparlamentarische Opposition).

Das Funktionieren eines derart pluralen Gruppenprozesses läßt sich wie folgt erklären:

Über Artikel 38 läßt das Grundgesetz eine Vielzahl von Bürgern an der staatlichen Willensbildung teilhaben. Dabei erweisen sich die Parteien als notwendig einerseits, um *formal* einen kollektiven Willen zu bilden [25]), andererseits, um *materiell* aus der Vielzahl vorhandener Wertvorstellungen, Meinungen und Interessen im Wege des Kompromisses eine Entscheidung zu fällen [26]). Die mit einer Vielzahl von Verbands- und Interessenvertretern durchsetzten Parteien beherrschen das Parlament und stellen dort die Regierung oder die Opposition. Das Parlament spiegelt damit einen großen Teil der in der Gesellschaft verbreiteten Interessenlagen wider. Der Opposition kommt nun in diesem Prozeß eine ganz besondere Funktion zu. Diese besteht nicht so sehr in Kontrolle und Überzeugung des politischen Gegners, der die Regierungsmehrheit stellt, als vielmehr darin, die Öffentlichkeit über Vorgänge im Regierungslager zu informieren. *Die Opposition ist also Mittler von Öffentlichkeit.* Eine intakte öffentliche Meinung, die von Massenkommunikationsmitteln mit gesteuert wird, kann Regierung und Parlamentsmehrheit, die für die Wiederwahl auf das Wählertum angewiesen sind, viel nachhaltiger kontrollieren, als es heute einer potentiell machtlosen Opposition gelingt. Sie kann das freilich nur, wenn der Zugang zu Informationen und den Nachrichtenmitteln auf alle Machtträger und Gruppen gleichmäßig verteilt ist [27]). Eine ähnliche Funktion wie die öffentliche Meinung haben desintegrierte Gruppierungen wie etwa die APO übernommen. Ihre mit „Penetranz" [28]) vorgetragene Forderung nach gesellschaftlicher Innovationsfähigkeit hat Veränderungen hervorgebracht, die vor Jahren noch niemand für möglich gehalten hätte.

Nach allem ist die sog. Kontrollfunktion des Parlaments heute de facto erloschen. Freilich bestehen durchaus berechtigte Hoffnungen, daß die Kontrollfunktion wieder aufleben kann: Durch die Einrichtung von Regierungsinformationssystemen können erstmals die Voraussetzungen für eine wirksame Kontrolle geschaffen werden [29]).

Ein derart mit der Realität erklärtes Verfassungsgeschehen, sieht sich schon heute folgenden noch nicht befriedigend gelösten Fragen gegenüber:

— Die ständige Rückkopplung staatlichen Geschehens über Verbände, Parteien und Gruppierungen gibt ein verzerrtes Bild sozialer Wirklichkeit wieder, weil bestimmte Interessen — wie etwa die der Kapitaleigner — überrepräsentiert sind — eine Feststellung, die an die Aussagen von Karl Marx erinnert [30]).

— Diese Rückkopplung hat einmal zur Voraussetzung, daß sie sich ungesteuert und ungehindert entwickeln kann, wenn sich also wirklich eine Meinung bilden kann, die etwa die Regierungsmehrheit zum Einlenken bewegen kann. Daß die Chancen der Beeinflussung durch die je regierende Mehrheit ungleich größer sind, bedarf keiner besonderen Erörterung [31]). Weiter muß sich der Staat dem Rückkoppelungsprozeß öffnen, er muß ein durch Informationen vermitteltes Modell seiner Tätigkeit geben. Verfassungsmäßiger *Empfänger dieses Modells kann nach allem nur die Opposition als Mittler von Öffentlichkeit sein.*

— Wegen des Vordringens technokratischen Sachverstandes wird der Staatsapparat zwar transparenter, für Outsider aber immer undurchschaubarer. Die Staatsführung muß sich daher — schon aus Effektivitätserwägungen — gegenüber Verselbständigungstendenzen [32]) der Bürokratie absichern.

1.3. Konsequenzen für den Informationsaustausch

Das Gleichgewicht in einem parlamentarischen System wird durch das Zusammenspiel pluraler Gruppen bewirkt. Es hat sich weiter gezeigt, daß die Opposition als wichtiger Mittler für diese Gruppen (soweit sie nicht ohnehin von den Regierungsparteien repräsentiert und entsprechend auch informiert werden) insofern fungiert, als sie Empfänger von durch Informationen vermittelten Realitätsmodellen sein kann. *Daher macht das parlamentarische System die Ausgestaltung von Rechten, die*

---

[23]) dieser Ausdruck geht auf W. Weber (3), 195 zurück

[24]) vgl. hierzu die fünf Komponenten der Gewaltenteilungslehre Steffanis (2), 305 ff.

[25]) formale Integrationsfunktion der Parteien, Gehrig, 108 f.

[26]) „materielle Integrationsfunktion" der Parteien, Gehrig, 109

[27]) vgl. Loewenstein, 16

[28]) zu der Bedeutung von Penetranz im heutigen Verfassungsleben vgl. den vorzüglichen Aufsatz von L. Phillips, Recht und Information (erscheint demnächst in dem von A. Kaufmann herausgegebenen Band „Rechtstheorie")

[29]) Stein, 74

[30]) in diesem Sinne auch Böhret, 148

[31]) eindrucksvolle Beispiele bei Gehrig, 174 ff.

[32]) vgl. die bei Böhret, 55 ff. aufgezeigten Gesetzmäßigkeiten

den Informationsaustausch zwischen Exekutive und Parlament betreffen, als Oppositionsrechte unbedingt erforderlich. Es erfordert eine von der Regierung vollständig und richtig informierte Opposition [33]). Daher ist der Meinung von Scholler [34]) und Sauer [35]) und v. Mangoldt-Klein [36]) voll und ganz zuzustimmen, die in den Fragerechten der §§ 105 ff. der Geschäftsordnung des Bundestages Rechte sehen, die die Regierung zur Antwort verpflichten. Wenn das schon erwähnte Bay. EDVG in § 1 Abs. 2 Zugriffsrechte nur dem Parlament als ganzem gewähren will, so verträgt sich das nicht mit den Grundsätzen eines modernen parlamentarischen Systems.

Ehmkes [37]) Argumente gegen ein derartiges Ergebnis vermögen nicht zu überzeugen. Er sagt, die politische Logik des parlamentarischen Systems liege in der Chance des Regierungswechsels, nicht in der Ersetzung des Mehrheits- durch das Minderheitsprinzip. Daher sei es nicht möglich das parlamentarische Untersuchungsrecht — dieses Argument ist darüber hinaus verwendbar — im Ergebnis auf die Opposition zu übertragen. Wie groß diese Chance aber ohne ausreichende Information ist, sagt Ehmke nicht. Außerdem ist die Gefahr irreversibler, d. h. durch den Regierungswechsel nicht mehr verhinderbarer Entscheidungen in einer dynamischen Gesellschaft zu groß geworden. Minderheitenrechte sind (für parlamentarische Untersuchungsausschüsse) „eine Waffe des Kampfes der rechts- und linksradikalen Parteien im Kampf gegen die Weimarer Republik" gewesen [38]). Ehmke verkennt damit die Rolle der modernen Parteien. Mag in der Weimarer Verfassung ein mehr an Informationen von „umstürzlerischen Parteien" noch bedeutet haben, daß der Staat sich selbst „in die Hände seiner Todfeinde" begibt [39]), so trifft das auf unsere demokratischen Parteien sicher nicht zu: „Je mehr ein Staat sich der Demokratie nähert, um so mehr wird er (Informationsrechte) [40]) als Minderheitenrechte ausbilden" [41]). Bleibt festzuhalten:

Information des Parlaments heißt vor allem Information der Opposition. Informationsrechte des Parlaments gegenüber der Regierung müssen als Minderheitenrechte ausgestaltet sein.

[33]) vgl schon Heinemann (1), E. 54 f.; Gehrig, 301
[34]) S. 407 f.
[35]) S. 40 f.
[36]) S. 1195
[37]) (2), 45 — freilich im Zusammenhang mit dem Enqueterecht gefallen
[38]) Ehmke (2), E 9
[39]) Koellreuther, 858; in dieser Richtung auch noch Düwel, 137 f.
[40]) siehe dazu oben 2. Teil C. 1.2.
[41]) so schon Hatschek (2), 657 für Interpellationsrechte
[42]) vgl. etwa Steffani (2), 14
[43]) gegen die Eigenständigkeit dieser Funktion zutreffend Ehmke (2), E 10
[44]) S. 308
[45]) zum folgenden vgl. Steffani (2), 108
[46]) Steffani (2), 108; Ehmke (2), E 21; Böhret, 259 f.; und die bei Keller-Raupach, 93 FN 136 zitierten.
[47]) (1), 88
[48]) zum Ganzen vgl. Bäumlin (2) und Leibholz (1)
[49]) Das ist die zentrale Aussage Gehrigs, 83 und passim.

2. Die Aufgaben der Opposition im parlamentarischen System

Als parlamentarische Funktionen werden allgemein genannt [42]):

— Gesetzgebungsfunktion (einschl. Budgetrecht),
— Kontrollfunktion (Einsetzung, Abberufung und ständige Kontrolle der Regierung),
— Sicherung und Aufrechterhaltung der innerparlamentarischen Ordnung,
— die politische Integration (sog. „lyrische Funktion"! [43])),
— die Wahlfunktion.

Für unseren Zusammenhang genügt ein genaueres Eingehen auf die Gesetzgebungs- und die Kontrollfunktion.

2.1. Die Gesetzgebungsfunktion

Aus den Darlegungen des ersten Abschnitts ist hervorgegangen, daß die Zustimmungsfunktion formell zwar beim Parlament verblieben, materiell aber im wesentlichen auf die Regierung übergegangen ist. Max Webers [44]) Bezeichnung des Parlaments „als Bewilligungsapparat der Bürokratie" hat insoweit weiter seine Berechtigung [45]). Geschichtlich ist diese Entwicklung eine Folge des Übergangs von der konstitutionellen Monarchie zum parlamentarischen Regierungssystem. Das Parlament fand sich angesichts komplexer werdender Umweltverhältnisse bereit, den Hauptteil der gesetzgeberischen Arbeit der strukturell besser geeigneten Bürokratie zu überlassen, dies aber unter der Voraussetzung, daß das Tun der Regierung weiter fest in seinen Händen liegt. *Der Verlagerung von Aufgaben sollte ein wirksamer Kontrollapparat gegenüberstehen.* Wie gesagt, die Waffen des Parlaments sind insoweit stumpf geworden.

Es ist unrealistisch und politisch undurchsetzbar, die verlorengegangene Initiative des Parlaments wiedergewinnen zu wollen [46]). Das würde in jedem Fall eine Art parlamentarischer Gegenbürokratie erforderlich machen, die Partsch [47]) mit dem schlagenden Argument verwirft: „Wollte man jedem Referat der Ministerialbürokratie einen einzigen Fachmann entgegenstellen, so bräuchte man deren 1000."

Von den Konsequenzen, die aus dieser Entwicklung zu ziehen sind, ist anschließend zu handeln. In jedem Fall ist es wünschenswert, daß die Funktionen des Parlaments soweit wie möglich gestärkt werden.

2.2. Die Kontrollfunktion [48])

2.2.1. Begriff und Wesen der Kontrolle

Mit Verschwinden des Dualismus von Monarch (Exekutive) und Bürgertum (Parlament) ist die Kontrollfunktion — wenn überhaupt — so doch nur auf die Opposition übergegangen [49]). Kontrolle, in ihrem

ursprünglichen Sinn gleichbedeutend mit Kritik [50]), wird heute darüber hinaus verstanden als Beeinflussung und im gewissen Sinne Beherrschung der Regierung [51]). Dieser Sprachgebrauch erscheint aus zweierlei Gründen unzulänglich. Einmal werden die meisten Veränderungen der Regierungspolitik nicht durch die Opposition bewirkt, vielmehr nimmt als Folge vielfältiger Rückkopplungen das Regierungslager Korrekturen an sich selbst vor (Beispiel: Meinungsumfrage bringt veränderte Regierungspolitik). Zum anderen verkennt eine derartige Begriffsbildung das für heutige Verhältnisse entscheidende Moment: den Faktor Information. Es wird gesagt, „die Information (sei) nur Durchgangszweck" [52]) und führe zum eigentlichen Zweck der Kontrolle, der Beschneidung und Begrenzung der Macht [53]) der Exekutive. Worin aber dieser „eigentliche" Kontrollzweck bestehen soll und wie er realisiert wird, wird nicht gesagt.

Auch auf die Gefahr hin, hier Plattheiten zu wiederholen, sei an Bacons Sentenz „Wissen ist Macht" erinnert, die übertragen bedeutet, daß derjenige an Macht verliert, der sich seines Wissens begibt [54]). Macht wird heute vor allem auch durch Information repräsentiert; nur wer diese Informationen auch kennt, ist in der Lage, Gegenmaßnahmen zu entwerfen.

Die Verwendung des Worts Kontrolle verschleiert deshalb, daß es nicht so sehr um oppositionelle Kritik des Regierungskurses, als vielmehr primär um Offenbarung eben dieses Kurses geht. Daß Regierungen entsprechend wenig interessiert sind, Wissen freizugeben, versteht sich nachgerade von selbst [55]). *Deshalb ist die Opposition verfassungsmäßiger Mittler von Öffentlichkeit für Öffentlichkeit* [56]). Kontrolle darf nach allem nicht instrumental verstanden werden. Sie ist zu beziehen auf Entscheidungsprozesse und -strukturen in Verwaltung und Regierung.

Kontrollfunktion des Parlaments heißt heute Offenlegung der Entscheidungsprozesse in Regierung und Verwaltung [57]).

2.2.2. Arten der Kontrolle

Typen der Verwaltungskontrolle, die speziell auf die Entscheidungsprozesse der Exekutive bezogen sind, sind bisher noch nicht entwickelt; die geltenden Institute sind, wie Simitis zutreffend bemerkt, in aller Regel auf andere Informationsstrukturen zugeschnitten. „Sie stellen Reaktionen auf ein Instrumentarium dar, das mit der elektronischen Datenverarbeitung überhaupt nicht verglichen werden kann" [58]). Die umfangreiche und wissenschaftlich bisher nicht bewältigte Problematik kann hier nicht erschöpfend behandelt werden. Im folgenden sollen gleichwohl einige Hinweise gegeben werden. Entscheidungsprozesse könnten in folgenden Aspekten oppositioneller Kontrolle unterliegen:

1. Kontrolle von politischen Ziel- und Wertentscheidungen (Prioritätensetzung),
2. Kontrolle der Entscheidungsfindungsprozesse (Kontrolle der Alternativauswahl),
3. Kontrolle der Exekutivprogramme (Kontrolle entsprechend vorgegebener Zielentscheidungen und Informationsmengen),
4. Kontrolle der Entscheidungsstrukturen (Offenlegung der Verantwortlichkeit für jeweilige Entscheidungen),
5. Insichkontrolle (Kontrolle gegen Verselbständigungstendenzen der Bürokratie).

Dieser theoretische Ansatz ist gewiß vorläufig und allenfalls dann realisierbar, wenn arbeitsfähige Informationssysteme bestehen. Er wird durch elektronische Datenverarbeitung überhaupt möglich [59]). Es ist aber unrealistisch zu glauben, man könnte die über Informationssysteme Verfügenden kontrollieren, ohne die Kontrollmittel den neuartigen Informationsstrukturen anzupassen.

Die spezifische Problematik dieser Kontrollmittel soll im folgenden kurz angerissen werden. Dabei beschränken wir uns auf die unter 1. bis 3. erwähnten Mittel, da sie unter dem Gesichtspunkt des Gutachtens besonders wichtig sind.

2.2.2.1. Kontrolle von politischen Ziel- und Wertentscheidungen und des Entscheidungsfindungsprozesses

Kontrolle politischer Zielentscheidung ist nur dann sinnvoll, wenn offengelegt wird, warum die Regierung sich gerade für dieses Ziel entschieden und die Prioritäten anderer Ziele verneint hat; wenn fest steht, welche Alternativen sie aus welchen Gründen verneint hat; wenn sie sagt — was bei Informationssystemen möglich sein wird —, welche gesellschaftlichen Auswirkungen die Entscheidung hat, also aufgrund welcher Informationen ihre Entscheidung ergangen ist. All das erfordert einen ungehinderten und dauernden Zugang zum Informationssystem der Regierung. Diesen Anforderungen genügen die derzeitigen Informationsrechte — jedenfalls in der herrschenden Auslegung — nicht! Sie gestatten es der Exekutive, frei über die Informationen zu verfügen und verhindern damit für die Zukunft jedwede wirksame Kontrolle. Das weitere Festhalten an dieser Auffassung kann für unsere parlamentarische Demokratie lebensgefährlich werden. Diese Auffassung ist daher aufzugeben. Richtig kann danach nur eine Meinung sein, die der informationsgebenden Stelle der Exekutive auch und gerade im Hinblick auf die Art der Informationen eine Rechtspflicht auferlegt. Die derzeit fehlende Realisierbarkeit kann für ein erst zu schaffendes Gesetz kein Hindernis sein. Als erste praktische Auswirkung dieser Auffassung ist die Vorschrift des § 41 der Gemeinsamen Geschäftsordnung der Bundesministerien, besonderer Teil aufzugeben und neuzeitlichen Gegebenheiten anzupassen.

---

[50]) Gehrig, 3
[51]) zu den verschiedenen Bedeutungen von Kontrolle vgl. Gehrig, 3 ff.
[52]) Sauer, 14
[53]) eine Definition für Macht findet sich bei Gehrig, 20; Hinkamp, 32 f.
[54]) vgl. auch Gehrig, 303 FN 299
[55]) das hat schon M. Weber, 341 beklagt
[56]) so auch Stein, 75
[57]) bescheidene Ansätze finden sich bei Gehrig, 11 ff.
[58]) (2), 677
[59]) so auch Böhret, 148

2.2.2.2. Kontrolle der Exekutivprogramme

Das Parlament, also die Opposition, muß jederzeit wissen, welche Informationen aus welchem Grund und zu welchem Ziel in Regierungsinformationssystemen gespeichert sind. Sie muß deshalb auf die dort gespeicherten Informationen zugreifen können. Dabei sind Beschränkungen gleich welcher Art unangebracht.

2.2.3. Parlamentarisches Informationssystem (PAIS)

Die schon oben gestellte Forderung nach einem PAIS ergibt sich daraus, daß eine Kontrollinstanz, die sich nicht mit den (an eine moderne Regierung gestellten) Anforderungen parallel entwickelt und immer neu erkennt, was eigentlich vorrangig kontrolliert werden muß, die Aufgabe nicht mehr erfüllen können wird [60]). *„Die Maßnahmen und Verfahrensweisen der Kontrollinstanz (müssen) sich deshalb an die fortgeschrittenen Methoden der Entscheidungsbildung innerhalb der Regierung angleichen."*

Fraglich und bisher ungelöst ist freilich die Frage, wie ein PAIS aussehen könnte [61]). Einerseits bekommt es von der Exekutive nur Informationen, die auf ihre Verwendungszwecke zugeschnitten sind. Zum anderen würde die innere Logik des parlamentarischen Systems erfordern, daß die Opposition und nicht die Mehrheit des Parlaments den Verwendungszweck bestimmt. Das ist politisch schwer durchsetzbar und bei einem Regierungswechsel sehr problematisch. Schließlich steht nicht fest, welche Informationen das Parlament (Opposition) eigentlich braucht und ob insoweit eine Konsequenz aus der Tatsache zu ziehen ist, daß die Gesetzgebungsfunktion auf die Bürokratie übergegangen ist.

3. Rechtsdogmatische Einwände — Überblick

3.1. Der Grundsatz der Gewaltenteilung

3.1.1. Begriff und Wesen der Gewaltenteilung

Nach W. Kägi [62]) gibt es zu Montesquieus Gewaltenteilungsschema so viele Interpretationen wie Interpreten. So ist „die Gewaltenteilung zu einer Diskussionswaffe (geworden), die dem, der sie zuerst anwendet, einen bedeutenden Vorteil verschafft oder gegnerische Argumente gar zum verstummen bringt. Das vor allem, wenn die Einrichtung einer neuen staatlichen Einrichtung bekämpft werden soll, deren Ort im Gefüge der Gewalten noch unbestimmt ist" [63]). Wiewohl eine Art „Heilige Kuh des Deutschen Staatsrechts", ist *DIE* Gewaltenteilung kaum als Argument für oder gegen etwas zu verwenden [64]). Trotzdem gilt *DIE* Gewaltenteilung als *DAS* tragende Organisationsprinzip des Grundgesetzes [65]). Am ehesten noch könnte man die Meinungen folgendermaßen unterteilen:

3.1.1.1. Die Meinung des Bundesverfassungsgerichts [66])

Nach dieser Meinung ist Artikel 20 Abs. 2 GG sedes materiae des Gewaltenteilungsprinzips [67]). Der Inhalt des Prinzips wird in folgender Unterscheidung erblickt:

— *Gewaltentrennung*
  — Unterscheidung der Funktionen Rechtsetzung, Vollziehung und Rechtsprechung
  — Verbot, Funktionen wahrzunehmen, die einer anderen Gewalt zugewiesen sind.

— *Gewaltenbalancierung*

  gegenseitige Kontrolle und Hemmung der Gewalten. In dieser Bedeutung erscheint das Prinzip als Mittel der Aufteilung und Mäßigung der Staatsgewalt [68]).

Bezogen auf das hier zu erörternde Verhältnis von Regierung und Parlament betrifft das Prinzip vor allem die Kontrollfunktion. Es hat dann einen

— *negativen Kontrollaspekt*

  Freiheit des Parlaments vor Regierungseinfluß (funktionelle und personelle Unabhängigkeit),

— *positiven Kontrollaspekt* [69])

  Sämtliche Kontrollmittel des Parlaments gegenüber der Regierung.

Diese Meinung hat Schwierigkeiten wegen der vielfältigen Überschneidungen der Gewalten. Sie argumentiert [70]) daher, zwar sei der Gewaltenteilungsgrundsatz nirgends rein verwirklicht und werde an vielen Stellen durchbrochen, doch sei der Einbruch in den „Kernbereich" einer anderen Gewalt in jedem Falle verfassungswidrig. Die Frage, wie dieser sog. Kernbereich zu definieren sei, bleibt unbeantwortet.

3.1.1.2. Eine weit verbreitete Literaturmeinung [71])

Nach diesen Autoren hat Gewaltenteilung zumindest eine Doppelbedeutung. Einmal sei sie ein politisches Prinzip, das der Machtmäßigung diene, zum anderen ein Organisationsprinzip und Prinzip der Arbeitsteilung [72]). In dieser zweiten Bedeutung ließe sich das Prinzip wie folgt umreißen: *Gewaltenteilung als Prinzip der Funktions- und Aufgabenklarheit und der funktionsgerechten Organisationsstruktur* [73]). Die Meinungen der verschiedenen Autoren

---

[60]) Böhret, 259

[61]) Auch die bisherigen Vorschläge (vgl. Steinmüller (1), 67 f.; (2), 8 f.) helfen nicht so recht weiter, da sie nicht scharf genug zwischen Kontroll- und Gesetzgebungsfunktion des Parlaments unterscheiden; allerdings geben sie die Richtung an, in die die Überlegungen zu gehen haben.

[62]) Zit. nach Frenkel, N. 8

[63]) Frenkel, N. 8

[64]) Frenkel, N. 102 und N. 830 für parlamentarische Untersuchungsausschüsse

[65]) so etwa Hesse (2), 200

[66]) vgl. BVerfGE 2, 13; 3, 247; 5, 199; 9, 279

[67]) Hinkamp, 44 meint etwa in dieser Vorschrift Montesquieus Schema wiedererkennen zu können.

[68]) Hesse (2), 192

[69]) vgl. Loewenstein, 192

[70]) vgl. etwa BVerfGE 18, 59

[71]) vgl. insbesondere Hesse (2), 192 ff.; Küster, 9; Bäumlin (1), 94 ff., insb. 96; Loewenstein, 32; wohl auch Forsthoff (2), 30; ähnlich Lang, 233; Frenkel, N. 78; vgl. im übrigen die bei Gehrig, 211 FN 31 genannten Autoren; vgl. auch Odewald, 71

[72]) Exemplarisch für diese Auffassung ist Hesse (2), 195 ff.

[73]) Küster, 9

unterscheiden sich danach, je nachdem, ob sie dem politischen Aspekt (Freiheitssicherung) oder dem organisatorischen Aspekt (Leistungsfähigkeit, Effektivität) den Vorrang geben [74]). Diese Meinung hat immerhin für sich, daß sie verfassungs*rechtlich* die strukturellen Veränderungen innerhalb des Staatsapparats gut erklären kann, dies unter Zuhilfenahme neuerer organisationssoziologischer Untersuchungen [75]). Auch sie gibt aber keine Kriterien dafür an, wieweit sich die Staatsorganisation entsprechend Effektivitätsgesichtspunkten entwickeln darf, um nicht mit Verfassungsprinzipien zu kollidieren.

3.2.1. Der unlösbare Widerspruch zwischen Gewaltenteilung und parlamentarischem Regierungssystem

Die traditionellen Gewaltenteilungslehren gehen von folgenden — unlösbaren — Widersprüchen aus:

1. Sie setzen Funktion und Funktionsträger im wesentlichen gleich.

Sowohl Parlament wie Exekutive ist die Funktion „Gestaltung der sozialen Wirklichkeit" überwiesen und der Schwerpunkt der realen Handhabung dieser Funktion hat sich weitgehend auf die strukturell besser angepaßte Exekutive verlagert. Eine überzeugende inhaltliche Abgrenzung der Funktionen ist bis heute nicht gelungen. Insoweit wartet hier „eine der wichtigsten Aufgaben (auf die) heutige Staatsrechtswissenschaft" [76]).

2. Sie setzen Funktionsträger und Träger realer Macht im wesentlichen gleich.

Will man Steffani [77]) glauben, so besagt Montesquieus Grundansicht, daß ein politisches Organ ein anderes nur dann wirksam beschränken kann, wenn es selbst eine politische Kraft mit Autorität und sozialem Einfluß vertritt, die sich anderen Kräften gegenüber behaupten kann. Diese Bedingung ist heute schon wegen der funktionellen Identität von Regierung und Regierungsmehrheit nicht mehr erfüllt. *In einem parlamentarischen System kann das Gesamtparlament die parlamentarischen Funktionen nicht wahrnehmen. „Das Montesquieusche Gewaltenteilungsschema ist daher nicht mehr verwendbar"* [78]).

Auch die Vertreter der traditionellen Gewaltenteilungslehren haben freilich die Widersprüche ihrer Lehre erkannt und führen deshalb oftmals beredte Klage über das sog. Auseinanderklaffen von Verfassungsrecht und Verfassungswirklichkeit [79]), ohne freilich die Konsequenz zu sehen, daß unser Grundgesetz veraltet sei [80]). Sie übersehen dabei, worauf Stein [81]) zutreffend hinweist, daß „unter der Decke dieser veralteten Gewaltenteilungstheorien längst ein neues Verfassungsrecht herangewachsen (ist), das den heutigen Realitäten Rechnung trägt und ihnen ein erhebliches Maß an freiheitlicher Effektivität abringt".

Dieses Maß „freiheitlicher Effektivität" wird heute lediglich durch das oben [82]) problematisierte Gleichgewicht intermediärer Gewalten gesichert.

3.1.3. Gewaltenteilung und parlamentarische Informationsrechte

Gegen Informationsrechte, die über die bestehenden Interpellations- und Enqueterechte hinausgehen, könnte man etwa folgende dogmatische Einwände erheben:

1. Informationsrechte, die eine Offenlegung des Entscheidungsprozesses fordern, dringen in den Kernbereich der Regierung ein und seien daher verfassungswidrig.
2. Informationsrechte mit ständigem Zugriff zu Regierungsinformationen dringen in den Initiativbereich der Regierung ein und sind also verfassungswidrig, in gleicher Weise sei die dauerhafte Kontrolle unzulässig. Dies ergebe sich schon aus der Spezialregelung des Artikels 45 a GG.
3. Der dauernde Zugriff zu Regierungsinformationssystemen sei materiell nichts anderes als direkte Ermittlungstätigkeit bei der Verwaltung. Diese sei aber ausdrücklich nur im Fall des Artikels 44, 45 a GG zulässig. Im übrigen verstoße er gegen das Gewaltenteilungsprinzip.

3.1.3.1. Gewaltenteilung und Initiativrecht

Am schlagkräftigsten müßte sich für die Gegner der hier vertretenen Auffassung das Argument erweisen, Informationsrechte mit ständigem Zugriff zu Regierungsinformationssystemen seien geeignet, das Initiativrecht der Regierung aufs empfindlichste zu beeinträchtigen [83]). Kontrolle sei nur als „ex-post-Kontrolle" möglich. Demgegenüber wird hier vertreten, daß *grundsätzlich alle* Entscheidungsprozesse dem Kontrollträger Opposition potentiell offenstehen müssen. Zwischen diesen beiden Extremen wird sich die Diskussion bewegen müssen. Da sie bisher überhaupt noch nicht in Gang gekommen ist, können hier lediglich einige Hinweise gegeben werden:

Bei dem einzigen im Hinblick auf Informationen wirksamen Kontrollmittel des Artikel 44 GG wird überwiegend [84]) behauptet, Informationen und damit Kontrolle seien nur ex post möglich. In der Konsequenz schließt dieses Argument wirksame Kontrolle überhaupt aus. Heißt Kontrolle wirklich nur nachträgliche Zurkenntnisnahme von Mißständen, so wird das, was Sinn von Kontrolle auch sein muß, nicht verhindert: Falsche und irreversible Entscheidungen der Regierung. So sind etwa in der

[74]) entschieden für den Vorrang des politischen Prinzips etwa Frenkel, N. 78
[75]) vgl. dazu Mayntz
[76]) Achterberg, 231
[77]) (3), 325
[78]) Diese Meinung scheint in der neueren staatsrechtlichen Literatur im Vordringen begriffen; vgl. Stein, 23 ff.; Gehrig, 228 f.; für den Zusammenhang mit Informationsrechten besonders wichtig Ehmke (2), E 35; vgl. auch den bei Odewald, 72 FN 20 wiedergegebenen Meinungsstreit.
[79]) Beispielhaft Hinkamp, 51 ff.
[80]) zu diesem Argument Stein, 30; Hesse (2), 192 f.
[81]) S. 30
[82]) 2. Abschnitt C. 1.2.
[83]) vgl. zu diesem Argument Hess StGH in DÖV 1967, S. 56
[84]) vgl. oben 2. Teil, B. 3.3.3.

Bundesrepublik Deutschland Milliarden für Rüstungssysteme (HS 30-Schützenpanzer, Starfighter) ausgegeben worden, ohne daß die vorhersehbare Problematik mit einer Öffentlichkeit, sei es der parlamentarischen, sei es einer sonstigen Öffentlichkeit, ernsthaft diskutiert worden wäre. Die endliche Bekanntgabe solcher Entscheidungen nützt niemand etwas, wenn sie nur einmal gefallen ist. Was not tut, ist nicht so sehr eine grundlegende Änderung unserer Rechtssysteme, was not tut ist ein grundlegender Umdenkungsprozeß von Regierung und Verwaltung. Sie müssen lernen, ihr Wissen nicht als „Herrschaftswissen", sondern als „Verwaltungswissen" [85]) zu begreifen, das allen nützt und daher auch grundsätzlich allen offenstehen muß. Letztlich wird das dogmatisch nur möglich sein, wenn es gelingt, den Faktor Information aus dem organisatorischen Schema der Gewalten gleichsam herauszulösen.

3.1.3.2. Gewaltenteilung und Geheimhaltung

Eng mit dem Problem des Initiativrechts hängt zusammen die Frage der Geheimhaltung.

Um hier nicht mißverstanden zu werden, gilt es mit Arndt [86]) festzuhalten, daß kein Staat ohne Geheimhaltung auskommen kann. Nur gilt es zu differenzieren. Die bisherigen EDV- und Datenschutzgesetze (Artikel 1 Abs. 1 Bay. EDVG; § 6 i. V. m. § 5 Abs. 2 HessDSchG; § 5 i. V. m. § 4 Rhld.-Pf.-DSchG) haben geglaubt, einen Weg einschlagen zu können, der es bei einem globalen Hinweis auf die Geheimhaltungsvorschriften beläßt. Das Hessische Gesetz macht da immerhin eine Ausnahme. Dem kann nicht scharf genug entgegengetreten werden. *Es gibt im Prinzip weder ein öffentliches Interesse noch gar eine Geheimhaltungsvorschrift, die dem parlamentarischen Informationsverlangen entgegengehalten werden kann* [87]). Jede andere Meinung muß darauf hinauslaufen, der Opposition zu verweigern, was der Regierungsmehrheit längst bekannt ist. Ein Regierungssystem, das seine Informationssysteme mit einem Schleier von Geheimhaltung umgibt, schaufelt sich selbst das Grab.

Was not tut, ist eine Theorie, die das Geheimnisproblem systematisch nach den Prinzipien der Verfassung zu ordnen unternimmt [88]). Eine solche Theorie existiert bisher nicht und kann auch hier nicht entwickelt werden. Dies trifft zu, obwohl M. Weber [89]) schon 1918 darauf hngewiesen hat, daß das wichtigste „Machtmittel des Beamtentums die Verwandlung des Dienstwissens in ein Geheimwissen durch den berüchtigten Begriff des Dienstgeheimnisses" bilde. Letztlich sei es lediglich ein Mittel, die Verwaltung gegen Kontrolle zu sichern. In Fragen des Enqueterechts ist der Weimarer Verfassungsgeber den Vorschlägen M. Webers voll und ganz gefolgt — was in bezug auf Informationsrechte ein wenig zu bedauern ist. Auch der Bonner Verfassungsgesetzgeber sollte seine Vorschläge beherzigen und die Problematik — bei aller weiter notwendigen Geheimhaltung — nicht wie die vorgestellten Landesgesetze verschleiern. Die einzig nennenswerte Monographie über das Amtsgeheimnis [90]) wird ihm bei der Lösung nicht recht weiterhelfen können. Sie vertritt in unserem Zusammenhang Auffassungen, die weder der Stellung einer modernen Opposition, noch den Anforderungen einer parlamentarischen Demokratie auch nur annähernd gerecht werden. Sie ist insoweit unbrauchbar.

Nach allem kann die Problematik des Amtsgeheimnisses hier mit Anspruch auf Wissenschaftlichkeit nicht entschieden werden. Es muß mit diesen Hinweisen sein Bewenden haben.

3.2. Der Grundsatz der Alleinverantwortlichkeit der Regierung

Dieser Grundsatz besagt, daß allein die Regierung und nicht etwa die Verwaltung dem Parlament politisch verantwortlich ist [91]). Verantwortlichkeit heißt, daß die Regierung für ihre Handlungen mit dem Amt einstehen muß. Dieser Grundsatz ist keine notwendige Folge der Gewaltenteilung [92]).

Man könnte nun folgendermaßen argumentieren: Die Informationen, die das Parlament (die Opposition) per Informationsrecht aus dem Informationssystem bekommt, seien in Wahrheit nichts anderes, als die Informationen, die heute nur in den Akten stünden. Akteneinsicht sei aber ausdrücklich nur im Fall der Artikel 44, 45 a GG zulässig. Also sei ein Informationsrecht, das zum direkten Zugriff auf Exekutivinformationen berechtige, verfassungswidrig. Diese Auffassung übersieht einmal, daß der Verfassungsgeber die neuen durch Informationssysteme geschaffenen Informationssysteme weder hat vergessen können, noch ausdrücklich ausschließen wollen. Insoweit könnte auch eine subjektive Verfassungsauslegung nicht weiterhelfen [93]). Zum anderen kann „Alleinverantwortlichkeit der Regierung vernünftigerweise nicht bedeuten, daß (die Regierung) auch allein Herr sein solle über die Informationen, die das Geltendmachen einer Verantwortung durch das Parlament überhaupt erst ermöglichen" [94]).

Schließlich kann dieses Argument gegenüber Informationsersuchen der Opposition schon deshalb nicht durchschlagen, weil die Verantwortlichkeit allein durch ein Mehrheitsvotum des Gesamtparlaments geltend gemacht werden kann. Der Block Regierung — Regierungsmehrheit — Verwaltung hätte es damit in der Hand, Informationen unter Berufung auf Rechte zu verweigern, die der Opposition und nicht ihr selbst zustehen.

---

[85]) Ellwein (3), 181
[86]) (1), 2040
[87]) vgl. die Literatur, die zur Anwendbarkeit des § 96 StPO im Rahmen Artikel 44 Abs. 2 GG ergangen ist: Arndt (2), 292; Bonner Kommentar Artikel 44 N. 8; Keßler, 323; Ehmke (1), 419; vgl. auch These 9 der Beschlüsse des 45. DJT, E 173 und oben 2. Teil B. 3.3.1.
[88]) so auch Arndt (1), 2040
[89]) S. 341
[90]) Düwel, 136 ff.
[91]) vgl. Frenkel N. 430; 439; die Sonderstellung der parlamentarischen Untersuchungsausschüsse wurde bereits erwähnt, vgl. oben 2. Teil, B. 3.1.
[92]) so auch Frenkel N. 928
[93]) dagegen BVerfGE 1, 312
[94]) Frenkel N. 928

3. Teil

Vorschläge an den Gesetzgeber

A. Grundsätzliche Bemerkungen

Die vorliegende Untersuchung hat gezeigt, daß viele grundlegende Probleme des hier zu bearbeitenden Themas noch nicht gelöst sind und auch ohne gesonderte Untersuchungen, die jede für sich den Umfang dieses Gutachtens annehmen würden, nicht gelöst werden können.

Dazu gehören insbesondere:

1. Der Bedarf des Parlaments, bzw. der Opposition an Informationen, bezogen jeweils auf die parlamentarischen Funktionen [1]).
2. Probleme, die sich aus der frühzeitigen Empfängerstrukturierung der Exekutivinformationen für den Benützer ergeben [2]).
3. Systematisierung und Dogmatisierung der oppositionellen Kontrollinstrumente auf dem Boden neuer Informationsstrukturen [3]).
4. Systematischer Entwurf des Amtsgeheimnisses im Verhältnis Parlament und Exekutive [4]).
5. Technische usw. Lösungen für den Datenverbund Parlament-Exekutive.

Der Gesetzgeber sollte sich jedenfalls bei diesen für ihn lebenswichtigen Fragen frühzeitig, d. h. umgehend wissenschaftlichen Sachverstandes versichern.

Dies erscheint um so dringlicher, als die Wissenschaft den Gesetzgeber bisher mit Vorschlägen für dieses schwierige Gebiet weitgehend im Stich gelassen hat [5]). Er wird zu bedenken haben, daß das Problem des Informationsaustausches zwischen Exekutive und Parlament umstritten ist, solange es existiert. Er wird sich daher bemühen müssen, die Neuregelung der Informationsrechte in der Verfassung abzusichern.

[1]) s. o. 1. Teil E; 2. Teil C. 2.
[2]) s. o. 1. Teil E; 2. Teil C. 2.2.3.
[3]) s. o. 2. Teil C. 2.2.3.
[4]) s. o. 2. Teil C. 3.1.3.2.
[5]) von unseren Vorschlägen einmal abgesehen

B. Die Vorschläge im einzelnen

1. Art der Berechtigung

Dem Parlament sind umfassende Informationsrechte für alle die Informationen zur Verfügung zu stellen, die für Entscheidungen der Regierung Berücksichtigung finden. Insofern ist also das exekutive und gubernative „Informationsverhalten" offenzulegen. Darüber hinaus sind dem Parlament alle die Informationen zur Verfügung zu stellen, die es zur Wahrnehmung seiner Funktionen benötigt, also etwa Kontrollinformationen, Planungsinformationen usw. Hier ist der Ort von Informationsrechten.

Die Informationsrechte sind zu unterscheiden in:

— Zugriffsrechte,

— Auskunftsrechte.

[6]) das sind etwa: Landtagspräsident, die Fraktionen, der Ältestenrat, Ausschüsse, einzelne Abgeordnete

[7]) Das hier geforderte Auskunftsrecht ist also weiter als die bisher bestehenden Auskunftsrechte, vgl. oben 1. Teil A 2.3.1.1. Gleichwohl empfiehlt es sich, den Begriff beizubehalten, zumal er auch in den EDV-Gesetzen von Hessen, Bayern und Rheinland-Pfalz verwandt wird.

Zugriffsrecht:

Das Recht parlamentarischer Stellen [6]), bei der Exekutive (Regierung und Verwaltung) anfallende Informationen ohne ihre Vermittlung durch Benutzung von Exekutivinformationssystemen zu ermitteln.

Auskunftsrecht:

Das Recht parlamentarischer Stellen, von der Regierung zu erwartende oder gefällte Wertentscheidungen und die dazu zu benützenden oder benützten Informationen bei Bedarf mit Hilfe der jeweiligen Informationssysteme zu erfahren [7]). Politische Entscheidungen verlangen Auskunft des Politischverantwortlichen. Derartige Auskünfte kann nur die Regierung, nicht eine sonstige Stelle der Exekutive liefern. In einer weiteren Regelung ist sicherzustellen, daß auch solche Stellen — privaten oder öffentlichen Rechts — in die Auskunftsverpflichtung miteinbezogen werden, die die Regierung bei ihren Vorhaben nur unterstützen.

Diese Rechte sollten tunlichst in der Verfassung abgesichert werden, was etwa durch eine ent-

sprechende Änderung des Artikels 43 GG geschehen könnte (Gesetzesvorbehalt).

2. Berechtigte

Das Gesetz muß in jedem Fall sicherstellen, daß die Informationsrechte als Rechte der parlamentarischen Opposition ausgestaltet werden. Dabei muß die Opposition mindestens Fraktionsstärke besitzen.

Diese Berechtigung, sowie die oben geforderten Auskunfts- und Zugriffsrechte sind an die Stelle des jetzigen Artikels 43 GG in das Grundgesetz einzufügen.

3. Art der von den Informationsrechten erfaßten Informationen

Im Grundsatz sind im Parlament alle der Regierung verfügbaren Informationen zugänglich zu machen. Das gilt auch für Individualdaten [8]).

Die Berufung auf Geheimhaltungsvorschriften ist grundsätzlich unzulässig. Soweit Geheimhaltung weiter erforderlich ist, kann diese durch nichtöffentliche Sitzung der Bundestagsausschüsse gewahrt werden. Zweifelsfälle sind dem Bundesverfassungsgericht zur Entscheidung vorzulegen.

4. Sonstige Vorschriften

— Das Informationssystem hat ausreichend Programme zur Wahrnehmung der parlamentarischen Informationsrechte zur Verfügung zu stellen.

— Für die Zugriffsrechte muß dem Parlament ausreichend Rechenzeit eingeräumt werden. Dazu sind bestimmte Bearbeitungsprioritäten festzulegen.

— Das Bedienungspersonal muß für Zwecke des Parlaments zur Verfügung stehen. Insoweit sind die Zugriffs- und Auskunftsberechtigten direkt zu Weisungen berechtigt.

Letztlich werden alle hier aufgestellten Forderungen nur dann zu einer Verbesserung der informationellen Situation des Parlaments führen, wenn folgende Bedingungen erfüllt sind:

1. Das Parlament benötigt ein eigenes parlamentarisches Informationssystem (PAIS), das als Subsystem in das allgemeine staatliche Informationssystem integriert ist [9]).
2. Die Organisationsstruktur des Parlaments muß entscheidend verbessert werden.

---

[8]) näheres zur Terminologie unten im Teil C. des Gutachtens

[9]) vgl. zu dieser Forderung neuerdings wieder Steinmüller (3) in einer Untersuchung über die bayerischen Verhältnisse

Anlage 2

Datenschutz im Spiegel der anglo-amerikanischen Literatur

Ein Überblick über Vorschläge zur Datenschutzgesetzgebung

von

Dr. Ruprecht B. Kamlah, Erlangen

Der nachstehende Überblick über Vorschläge zur Datenschutzgesetzgebung berücksichtigt amerikanische und englische Quellen, die der Verfasser im Rahmen eines Forschungsauftrages für das Bundesministerium des Innern in der Zeit von November 1970 bis September 1971 ausgewertet hat. Da die einschlägigen Veröffentlichungen in für Europäer häufig schwer zugänglichen Publikationsorganen zu erscheinen pflegen, kann es sein, daß manches noch nicht berücksichtigt ist, was der Verfasser nur in den USA entsprechend schnell hätte erhalten können. Da der Verfasser sich aber seit 1967 — teils in den USA — mit den Problemen des Datenschutzes befaßt hat, kann er doch mit einiger Zuversicht davon ausgehen, daß er das Wesentliche erfaßt hat.

In den Abschnitten B und C hat Herr Rechtsreferendar Ewald Weschky aus Nürnberg mitgearbeitet. Ich möchte es nicht versäumen, ihm dafür — und für seine Tätigkeit beim Exzerpieren eines großen Teils der Literatur — zu danken.

Erlangen, den 14. Oktober 1971

Ruprecht Kamlah

Vorbemerkung

Seit den Hearings über das von der amerikanischen Regierung geplante „National Data Center" oder die „National Data Bank" [1]) ist in den Vereinigten Staaten die öffentliche Diskussion über die Implikationen der automatischen Datenverarbeitung (ADV oder EDV) nicht mehr verstummt. Im Mittelpunkt der Diskussion stand und steht das „right of privacy", das in vielen Beziehungen dem deutschen allgemeinen Persönlichkeitsrecht entspricht [2]). Bedeutende amerikanische Autoren haben das ehrwürdige „right of privacy", wie es von Warren und Brandeis [3]) entdeckt wurde, mit den neuen technologischen Entwicklungen konfrontiert [4]). Sie kommen so gut wie einhellig zu dem Ergebnis, daß eine unkontrollierte Entwicklung der ADV, angewandt auf personenbezogene Daten, zwangsläufig eine totale Datenüberwachung durch den Staat und die private Wirtschaft herbeiführt, die die Vision George Orwells von 1984 nicht nur erreicht, sondern vermutlich sogar übertrifft [5]).

Den Plänen des Bureau of the Budget und des Bureau of the Census zur Errichtung einer statistischen Datenbank — nichts anderes sollte das National Data Center sein — schlug daher großes Mißtrauen der Öffentlichkeit entgegen. In den o. g. Hearings fand dieses Mißtrauen seinen Niederschlag. Hier soll nicht die Genesis der Pläne für ein National Data Center bis zum bitteren Ende beschrieben werden [6]). Tatsache ist, daß der amerikanische Kongreß der Regierung nicht einmal die Errichtung einer rein statistischen Datenbank gestattet hat, da die Befürchtungen, die man hatte, auch nach den beiden umfangreichen Hearings im Kongreß und im Senat nicht zerstreut werden konnten. Nach den drei Expertisen von Richard Ruggles [7]), Edgar S. Dunn und Dr. Carl Kaysen [8]), die alle die Pläne des Bureau of the Budget im Ergebnis — jedoch mit abnehmendem Nachdruck — befürworteten [9]), waren die Bedenken nicht ausgeräumt. Vielmehr wurde immer deutlicher, daß sich eine moderne statistische Datenbank unvermeidlich zu einer Sammlung von beliebig verknüpfbaren Einzelangaben entwickeln werde [10]). Die Abrufbarkeit von personenbezogenen Daten in Form von Dossiers konnte nicht ausgeschlossen werden. Es bleibt dem Personal des statistischen Amtes möglich, Einzelfragen über Personen der Datenbank zu entnehmen. Denn es ist, wie der Zeuge Raymond T. Bowmann vor dem Gallagher-Committee aussagte [11]), nicht möglich und auch nicht sinnvoll, personenbezogene Daten ohne irgendeine Form von Identitätsmerkmal zu speichern, wenn auch die Herstellung persönlicher Dossiers sicher nicht das Ziel einer statistischen Datenbank ist [12]). Dies stimmte mit dem Kaysen-Report überein, der bestätigte, daß die Geheimhaltung personenbezogener Daten stets vom Personal der statistischen Datenbank abhängen werde [13]).

Dies gab den Ausschlag für den Kongreß, der Regierung Einhalt zu gebieten, bis angemessene Vorschläge zur gesetzlichen Sicherung der Privatsphäre vorhanden sind [14]). Im April 1968 wurden die Pläne des Bureau of the Budget vorerst abgeblasen [15]).

Jedoch hat diese Entscheidung die Sorgen der Öffentlichkeit und der Wissenschaft nicht beendet. Miller bezeichnet sie als einen Pyrrhus-Sieg, denn die Datenverwaltung strebt auch ohne eine statistische Datenbank der Vollkommenheit entgegen [16]). Der dezentralisierte Datenaustausch im automatischen

---

[1]) The Computer and Invasion of Privacy, Hearings before a Subcommittee of the House Committee on Government Operations, 89th Cong. 2d Sess. 1966, House-Hearings; Computer Privacy, Hearings before the Subcommittee on Administrative Practice and Procedure of the Senate Committee on the Judiciary, 90th Cong. 1st Sess. 1967, Senate-Hearings.

[2]) Vgl. hierzu Kamlah, „Right of Privacy", Köln 1969 — in deutscher Sprache.

[3]) 4 Harv. L. Rev. 193 (1890/91)

[4]) Arthur R. Miller, Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society, 67 Mich. L. Rev. 1091 bis 1244 (1969); Alan F. Westin, Privacy and Freedom, New York 1967, 2. Aufl. 1970; ders.: Science, Privacy and Freedom: Issues and Proposals for the 1970's, 66 Col. L. Rev. 1003 (1966); Malcolm Warner — Michael Stone, The Data Bank Society; Organizations, Computers and Social Freedom, London 1970, um nur die wohl bekanntesten Werke zu nennen.

[5]) Warner-Stone, a. a. O., p. 13 seq; Miller, 67 Mich. L. Rev. 1107, 1128; Westin, Workshop on the Data Bank Society, London, Nov. 1970, (workshop), Anhang; vgl. auch Kamlah, Right of Privacy, a. a. O., S. 37 ff.

[6]) Vgl. hierzu besonders Privacy and the National Data Bank Concept, thirtyfifth Report to the House by the Committee on Government Operations, Nr. 1842, 90th Cong. 2d Sess. 1968, im Folgenden „35th Report".

[7]) Ruggles Report — in Auftrag gegeben vom Bureau of the Budget, abgedruckt in den House-Hearings, p. 195.

[8]) Dunn-Report, ebenfalls im Auftrag des Bureau of the Budget hergestellt, abgedruckt ebd., p. 254; Kaysen-Report, Senate-Hearings, p. 25.

[9]) 35th Report, a. a. O., p. 4; vgl. auch die Darstellung von Robert L. Chartrand, The Federal Data Center: Proposals and Reactions, 1968 L.a.C.T. Oct. p. 12 seq.

[10]) Vgl. auch R. J. Miller, Computers and the Law of Privacy, Detamation, Sept. 1968, p. 50; Warner-Stone, a. a. O., p. 88.

[11]) House Hearings, pp. 52 seq.

[12]) Vgl. auch Note, Privacy and Efficient Government, Proposals for a National Data Center, 82 Harv. L. Rev. 400, 414 (1968).

[13]) 35th Report, p. 15; Warner-Stone, a. a. O., p. 88.

[14]) 35th Report, p. 6, III A; Gallagher, Congressional Record, Aug. 18, 1966, abgedr. in Congress-Hearings, p. 311.

[15]) Vgl. Russel Pipe, Privacy; Establishing Restrictions on Government Inquiry, 18 Am.U.L. Rev. 516, 538 (1969); Miller, 67 Mich.L.Rev. 1132.

[16]) Miller, ebd., p. 1139; ebenso Pipe, 18. Am. U.L.Rev. 540; Warner-Stone, a. a. O., p. 88.

Datenverbund wird früher oder später eine zentrale statistische Datenbank überflüssig machen [17]), ja ist im Grunde genommen noch viel gefährlicher als ein allumfassendes National Data Center [18]).

Der Ruf nach dem Gesetzgeber ertönte daher nur um so lauter. Es gibt kaum eine Veröffentlichung, in der er nicht zu vernehmen ist [19]). Auch in England wurde fast gleichzeitig erkannt, wie notwendig Gesetzgebung zum Schutze der Privatsphäre ist [20]). Daneben wirft ein Licht auf die Bedeutung des Problems das 2 Millionen DM Forschungsprojekt des Computer Science and Engineering Board of the National Academy of Sciences; Leitung Alan F. Westin [21]). Lediglich über die Art und den Umfang der notwendigen Gesetzgebung bestehen unterschiedliche Auffassungen [22]).

Die unterschiedlichen Auffassungen betreffen jedoch mehr den Umfang der Gesetzgebung als den grundsätzlichen Inhalt [23]). Als Alternativen werden vorgeschlagen berufs-ethische Regeln für den neuen Beruf der Programmierer [24]) oder Verwaltungsvorschriften, die natürlich in erster Linie den Staat erfassen, die aber auch von der Industrie, z. B. von den Kreditauskunfteien eingeführt werden können [25]).

Nicht einmal die Credit Bureau Policies, geschweige denn andere Verfahrensregeln der Kreditauskunfteien, deren Ziel es war, strengere gesetzliche Regeln vor ihrer Entstehung zu unterlaufen und aufzuhalten [26]), werden als echter Ersatz für ein Eingreifen des Gesetzgebers angesehen [27]). Sie sollen — je nach dem Umfang notwendiger Gesetzgebung — die erforderlichen Ergänzungen der teuflischen Details liefern [28]).

Es kann daher festgehalten werden, daß der Ruf nach dem Gesetzgeber so gut wie einhellig ist [29]). Es kommt darauf an, aus den vielen Vorschlägen die auszuwählen, die brauchbar sind [30]).

---

[17]) Pipe, ebd.

[18]) Miller, 67 Mich.L.Rev. 1136.

[19]) Hier sollen nur die dem Verfasser bekanntgewordenen Konferenzen zum Thema genannt werden: Conference on Privacy, Chicago Feb. 1968; Computers: Privacy and Freedom of Information, Conference, Kingston, Ontario, Canada; Workshop on the Data Bank Society, London 1970.

[20]) Privacy and the Law, A Report by Justice, London 1970, p. 27; Workshop, a. a. O.

[21]) Vgl. auch Gallagher, Technology and Society: A Conflict of Interest? Congressional Record Apr. 1, 1969.

[22]) Vgl. Computers: Privacy and Freedom of Information, Summary Conclusions Reached at Kingston, Ontario Conference, May 21 bis 24, 1970, „Kingston-Summaries".

[23]) Vgl. Kingston-Summaries, Legislation and Regulations: comprehensive — Bikini-type-legislation.

[24]) Niblett, Digital Information and the Privacy Problem, OECD-Papier 27. November 1970, p. 14, unveröffentlicht; ders., Workshop on the Data Bank Society, Paper 1; Miller, 67 Mich.L.Rev. 1217; Hunnings, Neville-March, Workshop on the Data Bank Society, Paper 10; Watson, Technology and Privacy, Rede vor dem Commonwealth Club of California; D'Agapeyeff, Workshop, Anhang; Senate-Hearings, p. 119, Testimony; Karst, The Files, Legal Controls over the Accuracy and Accessibility of Stored Personal Data, 51 L.a.C.P., p. 342 seq., 362 seq.; Ruebenhausen-Brim, Privacy and Behavioral Research, 65 Col.L.Rev. 1184; Hargreaves (IBM), The Responsibility of Industry, Workshop, Anhang; Michael, 33 Wash.L.Rev. 279.

[25]) Niblett, OECD Papier, p. 22; Associated Credit Bureaus of America, Inc., (ACB), Code of Ethics, Credit-Hearings 1968, infra, p. 152, 154 seq.; Credit Bureau Policies to Protect Consumer Privacy, 1969 (ACB); Miller, 67 Mich. L.Rev. 1236; Code of Ethics and Operating Rules of CDC, Credit-Hearings 1970, infra, p. 163.

[26]) Gallagher, Statement, Hearings on „Fair Credit Reporting" before the Subcommittee on Consumer Affairs of the House-Committee on Banking and Currency, 91st. Cong., 2d. Sess. 1970, im Folgenden: Credit Hearings 1970, p. 29.

[27]) Die Kreditauskunfteien haben S. 823 (1969) unterstützt, um durch den Gesetzgeber nicht zuletzt auch gleiche Bedingungen für den Wettbewerb zu haben. Darüber hinaus haben sie das Ziel des S. 823 aber auch sehr verwässert. Vgl. Miller, Credit-Hearings 70, p. 188.

[28]) Miller, 67 Mich.L.Rev. 1232. Vgl. die Entwürfe zu einem Fair Credit Reporting Act S. 823, H.R. 6071, H.R. 1634 (1970), die alle flankierende Ausführungsvorschriften verlangen. Ebenso der Baker-Entwurf, „Data Surveillance Bill", Bill 150, House of Commons 1969, der in Sec. 8 dem Registerführer den Erlaß von Ausführungsvorschriften überträgt.

[29]) Pipe, 18 Am.U.L.Rev. 545; Miller, 67 Mich.L.Rev. 1232; Jacob, Privacy and the Law, 1969 L.a.C.T. Oct., p. 24; Privacy and the Law, a. a. O., p. 31 seq., 34.

[30]) Miller, ebd.

Vorschläge zur Gesetzgebung

A. Die Verrechtlichungstendenz

Während das Common Law bisher nur einen Schutz gegen Veröffentlichungen persönlicher Daten oder gegen das unbefugte Eindringen in die Privatsphäre durch verschiedene Abhör- und sonstige Überwachungstechniken gewährleistete [31]), haben die heute auftauchenden Probleme des Schutzes der Privatsphäre im Computerzeitalter die Rechtswissenschaft in eine neue Phase der Erörterungen versetzt [32]). Es wurde notwendig, neben der Untersuchung bekannter Verletzungsformen des Eindringens durch Abhörgeräte und der Veröffentlichung auch die Frage zu stellen, wann persönliche Daten allgemein ermittelt und — ohne Veröffentlichung — weitergeleitet werden dürfen [33]). Man kann von einer Tendenz sprechen, die dahin geht, die Verwendung personenbezogener Daten weiter zu verrechtlichen [34]). Dies ist im einzelnen näher zu belegen.

1. Rechtsgrundlage für das Sammeln und Einspeichern von Daten

In fast allen Publikationen wird gefordert, daß bereits dem Datenhunger der zu erwartenden Speicherkapazitäten Grenzen zu setzen sind, indem schon heute die Ermittlungsmethoden und -gewohnheiten der Staatsbehörden und der Wirtschaft überdacht werden. Der Bürger soll nur das allernotwendigste aus seiner Privatsphäre preisgeben müssen [35]). Die Berechtigung, Daten zu ermitteln und einzuspeichern, soll sich nach Vorschriften oder Richtlinien richten, die strenge Maßstäbe an die Notwendigkeit der Daten für die einspeichernde Behörde anlegen und das Bedürfnis des Betroffenen, die Daten nicht preiszugeben, an der Art der Daten, insbesondere am Grad ihrer Privatheit messen [36]). Für die Bemühungen in dieser Richtung ist ein Gesetzesvorschlag beispielhaft, der sich der Einstellungsfragebögen annimmt, die Stellensuchenden vorgelegt werden. Nur was unmittelbar mit der in Aussicht genommenen Stellung des Bewerbers zu tun hat, darf untersucht werden [37]).

Vor dem Versuch, bestimmte Bereiche der Privatsphäre abstrakt abzugrenzen oder Arten von Daten zu bestimmen, die überhaupt nicht gespeichert werden dürfen, machen die meisten Autoren halt oder bezeichnen das Unterfangen als aussichtslos [38]).

Die rechtliche Folge aus diesen Forderungen ist, daß für das Ermitteln und Speichern von Daten eine im Einzelfall näher zu bestimmende Rechtsgrundlage gefordert werden muß [39]). Dies kommt nicht stets mit gleicher Deutlichkeit zum Ausdruck [40]), da die verfassungsrechtlichen Reflexionen der meisten Autoren nicht sehr tiefschürfend sind, kann jedoch nicht anders sein, da viele Autoren, die sich mit dem Thema beschäftigen, keine Verfassungsrechtler sind [41]). Sehr aufschlußreich sind hier die Ausfüh-

---

[31]) Vgl. statt aller Prosser, Right of Privacy, 48 Cal.L.Rev. 383 ff. (1960) und zur Entwicklung des „right of privacy" in den USA Kamlah, Right of Privacy, a. a. O., S. 57 ff., Gutachten des Max-Planck-Instituts für ausländisches und internationales Privatrecht, der zivilrechtliche Persönlichkeits- und Ehrenschutz, Tübingen 1960, S. 257; v. Hippel, Persönlichkeitsschutz und Pressefreiheit im amerikanischen und deutschen Recht, RabelsZ 1969, 276.

[32]) Privacy and the Law, a. a. O., p. 31; Kamlah, a. a. O., S. 78.

[33]) Vgl. die Verletzungsform des Eindringens und der Indiskretion, Kamlah, a. a. O., S. 105, 120.

[34]) Privacy and the Law, a. a. O., p. 31 seq.; Westin, Political and Legal Dimensions of the Computer Data Bank Issue: Some Forecasts from the American Experience, Workshop, Anhang, behauptet, diese Tendenz wäre auch ohne den Computer aufgekommen. Vgl. neuerdings S. 975 (1971), § 552 a Freedom of Information Act, Sec. (a) (2); H.R. 854 (1971) Congressional Record H. 2947 (1971); seit 19. Juli 1971 in erweiterter Fassung: Amendment No. 261 of the Citizens' Privacy Act, S. 975, Cong. Record S. 11353.

[35]) 35th Report, p. 3, p. 12; Campbell, Computers and Freedom, 1969, Law and Computer Technology, June, p. 3; Jacob, Joseph, Some Legislative Proposals for the Proper Regulation of Data-Banks, Workshop on the Data Bank Society, Paper 11, p. 6; Senator Ervin, Bill S. 1791, 91st Cong., 1st Sess. (1969); Miller, Statement, Senate Hearings. p. 77; ders., 67 Atlantic 53—57; ders., A Transparent Society, N. Y. Herald Tribune, 6. 8. 69; Note, 82 Harv.L.Rev. 417 (1968). Besonders Pipe, 18 Am.U.L.Rev. 517: Control over input.

[36]) Ontario Law Reform Commission, Report on Protection of Privacy in Ontario (Ryan-Report), Ontario, Canada, 1968, p. 79; Pipe, a. a. O., p. 517; Miller, Testimony, Senate Hearings, p. 70 unten; § 164 (c) des H.R. 6071, Fair Credit Reporting Act.

[37]) S. 1438, Bill to protect the civilian employees . . ., April 1, 1971, Congr. Record, Senate, S. 4227 seq.

[38]) So z. B. Pipe, 18 Am.U.L.Rev. 542.

[39]) Westin, Legal Safeguards to Insure Privacy in a Computer Society, 10 ACM 536 (1967).

[40]) Meist wird nur eine gesetzliche Beschränkung der Datensammlung gefordert. Vgl. Miller, Statement, Senate Hearings, p. 77.

[41]) Der Gesetzesvorschlag von Senator Ervin, H.R. 7214, 91st Cong., 1st. Sess. (1969), weist überdeutlich in diese Richtung. Miller, 67 Mich.L.Rev. 1234 bezeichnet den Vorschlag als eine neuartige Lösung, der er im Prinzip zustimmt, p. 1235, jedoch mit der Einschränkung, daß man den Gesetzgeber nicht in die Details hinabzwingen darf. Vgl. auch Report on Protection of Privacy in Ontario; Ryan-Report, p. 73, twenty point proposal Nr. 4/5, p. 77, p. 79, besonders p. 81: Das Sammeln und die Weitergabe von Daten ist prima facie eine Verletzung der Privatsphäre. Ferner auch Campbell, Computers and Freedom, 69 L.a.C.T. June, p. 3.

rungen von Reich, der als Verfassungsrechtler die wesentlichen Punkte präzise zu formulieren versteht [42]). Das Verfassungsrecht gebe lediglich einen minimalen Schutz auf allen Gebieten, der durch den Gesetzgeber zu konkretisieren, niemals aber zu beschneiden sei [43]). Das Eindringen in persönliche Daten könne man sich daher nur auf einer gesetzlichen Grundlage vorstellen [44]).

2. Rechtsgrundlage für die Weitergabe von Daten

a) Reich hat auch sicher als einer der ersten in den USA generell eine Rechtsgrundlage für die Weitergabe von persönlichen Daten gefordert, auch dann, wenn die Daten bereits einmal zulässigerweise ermittelt wurden [45]). Dies ist ein Unterfall des Vorgangs der Indiskretion [46]), der am anschaulichsten als „Entfremdung" bezeichnet werden kann, da Daten — zu einem bestimmten Zweck ermittelt — durch die Weitergabe neuen, anderen Zwecken zugeführt werden, für die sie ursprünglich nicht bestimmt waren [47]). Durch die Computertechnik wird der Datenaustausch unendlich erleichtert [48]). In Anbetracht dessen — daß nämlich der Betroffene die Kontrolle über seine Daten verliert — gewinnt die Verrechtlichung der Indiskretion besondere Bedeutung. Man beginnt, für jede Weitergabe persönlicher Daten im Rahmen einer Datenverwaltung — natürlich muß der „Klatsch" außer Betracht bleiben — eine Rechtsgrundlage zu verlangen [49]). Die allgemein verbreitete Auffassung, daß die Entnahme von Daten aus einer „Datenbank" — eine Form der Indiskretion — ein rechtserheblicher Vorgang ist, kommt auch darin zum Ausdruck, daß viele für diese Form der Datenweitergabe die Einwilligung des Betroffenen als Grundsatz fordern [50]) oder sonstige Kontrolle, wie den später zu behandelnden Anspruch auf Auskunft über die Datenverwendung und die damit verbundene Protokollierungspflicht [51]).

Dementsprechend haben die Entwürfe zu Gesetzen über die Kreditagenturen auch das berechtigte Interesse der Kreditwirtschaft an Kreditauskünften anerkannt, jedoch nur in genau bestimmten Fällen [52]). Umgekehrt bestimmt der „credit data reporting act" [53]), unter welchen Voraussetzungen Staats- und Verwaltungsbehörden Auskünfte von Kreditagenturen einholen dürfen. Ein neuerer Gesetzentwurf schlägt vor, die bisher geübte Praxis der Staatsverwaltung einzustellen, daß Adressenlisten an Direktwerbungsunternehmen verkauft wurden, sozusagen „Massenindiskretion" [54]), ein Übel, das auch schon vorher beklagt und bekämpft wurde [55]) und auch bei uns vorkam [56]).

Natürlich ist man sich in den USA darüber im klaren, daß man eine Verrechtlichung der Datenverwendung nicht von heute auf morgen wird erreichen können [57]). Dies führt jedoch nicht dazu, die Forderung nach größerer Transparenz fallen zu lassen. Niemand ist wohl bei dem Gedanken, Daten unkontrolliert fließen zu sehen. Seien es nun Gesetze, Schutzprogramme oder berufs-ethische Regeln, die die Privatsphäre schützen, der Schutz ist erforderlich und soll so gesetzlich sein wie möglich.

b) An dieser Stelle sei noch bemerkt, daß eine Datenweitergabe auch dann normiert sein soll, wenn sie innerhalb einer Staatsverwaltung erfolgt [58]). Behörden oder Stellen einer öffentlichen Körperschaft sind in bezug auf den Datenaustausch zu trennen [59]). Der Streit um die National Data Bank konnte nur auf der Prämisse entstehen, daß Vorgänge des Datenaustausches innerhalb der Staatsverwaltung nicht als Interna anzusehen sind, sondern vielmehr Außenwirkung haben, also Eingriffe in das Right of Privacy darstellen [60]). Würde man solchen Datenaustausch frei zulassen, wäre die Entfremdungsregel praktisch aufgehoben, die sogar von sehr ge-

---

[42]) Reich, Statement, House-Hearings, p. 22 seq.
[43]) P. 31.
[44]) P. 31, 32.
[45]) Reich, ebd.
[46]) Kamlah, Right of Privacy, S. 116.
[47]) Kamlah, a. a. O., S. 131, ausführlich zum Begriff der „Entfremdung"; vgl. auch Jacob, Privacy and the Law, 1969, L.a.C.T. Oct. p. 20; Miller, Statement, Credit-Hearings 1970, p. 188.
[48]) Michael, Speculations on the Relation of the Computer to Individual Freedom and the Right to Privacy, 33 Wash.L.Rev. 273 (1964); Miller, 67 Mich.L.Rev. 1109.
[49]) Strömhohn, Right of Privacy and Rights of the Personality, Stockholm 1967, p. 108 andeutungsweise; Ryan-Report, p. 82; Jacob, Privacy and the Law, 1969, L.a.C.T. Oct., p. 23; Gallagher, Statement, Credit-Hearings 1970, p. 49: „due process of law"; Note, 82 Harv.L.Rev. 415; Pipe, 18 Am.U.L.Rev. 541; Miller, 67 Mich.L.Rev. 1170.
[50]) Westin, Legal Safeguards to Insure Privacy in a Computer Society, 10 ACM 533, 536 (1967); Ryan-Report, p. 82: Einwilligung ist der Grundsatz; Karst, 31 L.a.C.P. 344; N.Y.Gen.Bus.Law § 373; S. 975 (Amendment No. 261) 5 U.S.C. § 552 a (2).
[51]) Vgl. Data Surveillance Bill (1969), Lord Windlesham, MP Baker, § 4 Abs. 2; S. 975 (1971), § 552 a (a) (2), Freedom of Information Act; H.R. 854, Congressional Record H. 2947 (1971), Apr.; Ryan-Report, p. 83; Miller, Statement, Senate-Hearings, p. 78, erwähnt auch verwaltungstechnische Zugriffskontrollen, die eine vorherige Bestimmung der Zugriffsberechtigten nicht überflüssig machen. Daher fordert er gründliche Voruntersuchungen.
[52]) Vgl. Sec. 12, Sec. 34, H.R. 16340; § 164 (c) H.R. 6071; § 602, § 604, S. 823.
[53]) N.Y. General Business Law, § 373.
[54]) H.R. 8903, Horton, Congr. Record H. 6679, July 13, 1971.
[55]) Half a Million Junk Mail each Year, Gallagher, Congr. Record, Mar. 3, 1970.
[56]) BVerwG NJW 70, 1760.
[57]) Miller, 67 Mich.L.Rev. 1235.
[58]) S. 975 (1971), § 552 a „Freedom of Information Act", Sec. (a) (2); S. 1550, „The Constitutional Rights and Civil Liberties Protection Act of 1971, Cong. Record Apr. 15, 1971, S. 4910, Sec. 3 (6).
[59]) Ryan-Report, p. 77; Warner-Stone, a. a. O., p. 192; Jacob, Privacy and the Law, 1969, L.a.C.T. Oct. p. 23; Pipe, 18 Am.U.L.Rev. 547.
[60]) Das National Data Center sollte ursprünglich durch Zusammenfassung aller Daten aus dem Behördenbereich entstehen. Vgl. den Ruggles-Report, House Hearings, Anhang 1; Note, Privacy and Efficient Government: Proposals for a National Data Center, 82 Harv.L.Rev. 401 (1968).

gensätzlichen Autoren anerkannt wird [61]). Es würde gerade das entstehen, was unter allen Umständen zu vermeiden ist: ein absolut allwissender Staat verkörpert in dessen höchstem Geheimnisträger, den wir getrost auch unseren großen Bruder nennen können.

3. Pflicht, Daten periodisch zu löschen

Die Verrechtlichungstendenz kommt schließlich darin zum Ausdruck, daß es den datensammelnden Stellen nicht mehr erlaubt sein soll, personenbezogene Daten beliebig lange zu speichern. Regeln, die periodische Löschung von Daten vorschreiben, werden gefordert [62]). Die Löschung von Daten soll erfolgen, wenn die Daten durch Zeitablauf an Bedeutung verloren haben und ihre Offenbarung an Dritte den Betroffenen in einem nach dem Stand der Dinge falschen Licht erscheinen lassen würde. Es kommt nicht darauf an, ob die Daten wahr oder falsch sind [63]).

Aus der Strafregisterverordnung, die nun durch das Bundeszentralregistergesetz vom 18. März 1971 auf eine höhere Stufe der Verrechtlichung angehoben wurde, ist dem deutschen Juristen ein solches periodisches Löschungsverfahren vertraut. Auch das Problem des Fortlebens getilgter Strafen in anderen Akten und Unterlagen ist bekannt [64]). Das Problem des Fortlebens überholter Daten in etwas anderem Zusammenhang beschäftigt besonders die Gesetzentwürfe und Hearings, die sich mit dem Kreditauskunfteiswesen auseinandersetzen [65]). In der Kreditauskunftspraxis der USA ereignet sich täglich folgender Standardfall: Ein Kreditantragsteller wird auf Grund einer negativen Nachricht der Kreditagentur als „no pay" abgewiesen, weil in den Unterlagen der Agentur Forderungen gegen den Betroffenen als offen gemeldet sind. Die Agenturen entnehmen diese Nachrichten meist Listen der Gerichte über erhobene Klagen oder Meldungen ihrer Großkunden, unterlassen es jedoch, die Entwicklung der Streitigkeiten zu verfolgen, da es keine entsprechenden Listen der Gerichte gibt, die sich ebenso leicht in die Dossiers einarbeiten lassen [66]). Belastungen für den Betroffenen können entstehen, wenn die Nachricht falsch wird, weil die Forderung erledigt wurde, aber auch wenn die Forderung offen blieb, jedoch der „Fehltritt" sich in den Dossiers verewigt.

Die Schwierigkeiten, denen sich der Gesetzgeber gegenübersieht, wenn es gilt, obsolete Informationen zu beseitigen, sind bedeutender als ein oberflächlicher Betrachter anzunehmen geneigt ist. Im H. R. 16340 ist dem Problem ein ganzer Abschnitt gewidmet (§§ 51 bis 54). Daneben stellen weitere Vorschriften indirekt sicher, daß nur gültige Informationen in Auskünfte aufgenommen werden [67]).

Das Problem wird erweitert durch die Notwendigkeit der Fortschreibung von Daten, die nicht durch den Zeitablauf als solchen, sondern durch dazwischentretende Ereignisse überholt werden. Dies gehört systematisch zum Schutz gegen Entstellung des Lebensbildes, der jedoch nicht nur durch einen Berichtigungsanspruch [68]), sondern auch durch selbständige Berichtigungsvorkehrungen der Kreditauskunfteien zu gewährleisten ist [69]).

Eine Besonderheit ist hier die gesetzliche Verpflichtung der Auskunfteien, vor der Erteilung einer „erweiterten Auskunft" [70]) oder der Weitergabe von Informationen, deren Quelle öffentliche Akten oder Register sind [71]), den Inhalt der Auskunft nochmals nach strengen Maßstäben zu überprüfen [72]). Auch durch dieses Verfahren soll erreicht werden, daß überholte Daten nicht ständig weiterberichtet werden, weil ihre Gültigkeit keiner neuen Überprüfung unterzogen wird.

---

[61]) Miller, Statement, Credit-Hearings 70, p. 189 einerseits, Jordan, TRW-Credit Data, Letter, Credit-Hearing 70, p. 177 andererseits.

[62]) Miller, Statement, Senate-Hearings, p. 77: „the information recorded . . . must not be allowed to petrify". Ryan-Report, p. 86; Warner-Stone, a. a. O., p. 192.

[63]) Ryan-Report, p. 86; Amendment No. 261 of S. 975, 5 U.S.C. § 552 a (b).

[64]) Ob es mit § 50 BZRG angemessen gelöst ist, soll nicht untersucht werden.

[65]) Vgl. Fair Credit Reporting — Hearings before the Subcommittee on Consumer Affairs of the House Committee on Banking and Currency, 91st Cong., 2d Sess., on H.R. 16340, Credit-Hearings 1970, Übersicht auf p. 23 Ziff. 7, „obsolete information".

[66]) Beispiele für solche Fälle aus den Credit-Hearings 1970, p. 23, p. 41, p. 42/43, p. 78—81, p. 86. Manche der Beispiele sind geradezu surrealistisch (!) und doch wirklich.

[67]) Z. B. H.R. 16340 Sec. 63 (2); S. 823, § 605, § 611.

[68]) Hierzu siehe unten.

[69]) Vgl. H.R. 16340, Sec. 52 (a), Ziff. 5, 52 (b), 53 (2), 51.

[70]) S. 823, § 603 (e): investigative consumer report, H.R. 16340, Sec. 13 (d).

[71]) H.R. 16340, Sec. 53 (2): Public record information; S. 823, § 613 (2).

[72]) H.R. 16340, Sec. 13 (d), Sec. 63 (2); S. 823, § 613 (2), 614.

B. Technische Schutzmaßnahmen

Die rechtlichen Erfordernisse beim Speichern und Benutzen personenbezogener Daten werden natürlich zunächst technisch abzusichern sein. Daher verlangen so gut wie alle Autoren technische Schutzmaßnahmen, während nur wenige dazu übergehen, mögliche technische Schutzvorrichtungen zu beschreiben und auf ihre Wirksamkeit zu untersuchen [73]).

1. Zugangskontrollen

Bevor eine Person mit einer Datenbank in Berührung kommt, sollte sie schon rein äußerliche Zugangskontrollen zu passieren haben. Datenspeicher gehören in besonders gesicherte, von anderen Abteilungen eines Betriebes getrennte Räume [74]). Jeder Speicher und jedes Terminal sollte einen unabhängigen Schalter für die Energiezufuhr besitzen, der abschließbar sein muß [75]). Der Benutzer eines geöffneten Speichers wird auf diese Weise gehindert auch andere Speicher, die er für seine Arbeit nicht braucht, mitzubenutzen [76]).

Es kann auch so verfahren werden, daß nur zwei Personen gemeinsam Zugang zu bestimmten Informationen gegeben wird [77]). Was in einem Arbeitsspeicher nicht mehr benötigt wird, sollte so schnell wie möglich wieder daraus gelöscht werden, um zu vermeiden, daß Mitbenutzer einer Anlage nicht zufällig Zugriff erhalten. Auch sollte bei der Verarbeitung besonders zu schützender Daten der Zentralspeicher für andere Benutzer der Anlage gesperrt sein [78]).

In externen Speichern ruhen zu schützende Daten häufig am sichersten.

2. Benutzerindentifikation

Ein Benutzer, der Zutritt zu einer Anlage hat, muß sich dieser gegenüber zusätzlich ausweisen.

a) Kennwort- und Kennkartenkontrollen stehen hier im Vordergrund der Erörterungen [79]).

Diese Methoden reichen jedoch nicht aus, denn die Gefahr ist groß, daß das Kennwort verbreitet, die Kennkarte verloren oder gefälscht wird [80]). Kennwort und Kennkarte werden erst dann ausreichend sicher sein, wenn der Computer die Berechtigung der Träger der Identifikationsausweise selbst überprüfen kann.

Das kann geschehen, wenn der Fingerabdruckleser oder der „voice-print" genügend entwickelt ist [81]). Bis dahin werden Identifikationsdialoge mit dem Computer vorgeschlagen. Der Benutzer gibt seine Nummer ein, worauf der Computer eine andere Nummer antwortet. Mit dieser Nummer hat der Benutzer bestimmte Rechnungen auszuführen. Am Ergebnis erkennt der Computer, ob der Benutzer zugriffsberechtigt ist [82]).

b) Verfeinerte Identifikationssysteme überprüfen auch das Programm des Benutzers. Liegt das Programm für den Zugriff vorher fest, kann der Computer bei Abweichungen vom Programm Reaktionen bereithalten [83]). Wie bei vollkommen fehlender Identifikation schaltet er ab, notiert den Versuch des Zugriffs mit der Benützernummer oder auch alle sonstigen unprogrammgemäßen Vorgänge und Unternehmen um einen geschützten Speicher [84]), oder der Computer verhängt eine Sanktion gegen den Benutzer [85]).

Sind auf einem Speicher verschiedene Daten untergebracht, für die mehrere Personen ausschließlich zugriffsberechtigt sind, so muß bei den Daten die „Zugriffsinformation" gespeichert werden, damit der Computer entscheiden kann, welche Daten für wen bestimmt sind [86]).

Es versteht sich natürlich von selbst, daß die Benutzeridentifikation nicht nur für die Entnahme, sondern ebenso für die Eingabe und Änderung von Daten erforderlich ist. Alle diese Verfahren kosten

---

[73]) Vgl. besonders: Petersen and Turn, System Implications of Information Privacy, Proc. AFIPS 1967 Spring Joint Computer Conference, Vol. 30; Lance J. Hoffmann, Computers and Privacy, a Survey, 1969 Computing Surveys 85 (Vol. 1, No. 2) mit einer ausführlichen Bibliographie; vgl. auch Jürgen H. Schulze, Datensdutz in der Datenverarbeitung, IBM-Nachrichten 21, Heft 205, S. 640, dessen Beitrag die amerikanische Literatur verwertet, und auf den — unter Hinweis auf die überlegene Sachkunde seines Verfassers — hier ausdrücklich verwiesen werden muß.

[74]) Warner-Stone, a. a. O., 208.

[75]) Warner-Stone, a. a. O., p. 199; Westin a. a. O., p. 536.

[76]) Warner-Stone, a. a. O., p. 199; Niblett, a. a. O., p. 20.

[77]) Hargreaves, Workshop, Anhang.

[78]) Warner-Stone, a. a. O., P. 202.

[79]) Niblett, OECD-paper, p. 19/20; Warner-Stone, a. a. O., p. 204; Miller, Senate-Hearings, p. 78; Hargreaves, Workshop, Anhang, p. 3; Watson, Commonwealth Club of California, 5. April 1968, p. 9; Hoffmann, 1 Computing Surveys 89 (1969).

[80]) Warner-Stone, a. a. O., p. 204; Miller, 67 Mich.L.Rev. 1210.

[81]) Miller, 1967 Atlantic, Oct. p. 56; ders., 67 Mich.L.Rev. 1211; Warner-Stone, a. a. O., p. 205.

[82]) Hoffman, a. a. O., p. 92, der auch bei Fernverarbeitung auf den Rückruf — „dial up and call back-system" — hinweist.

[83]) Warner-Stone, a. a. O., p. 198.

[84]) Miller, Senate-Hearings, p. 78.

[85]) Vgl. zum „threat-monitoring" Hoffman, a. a. O., p. 93, 94; Petersen and Turn, a. a. O., p. 291, 292; Niblett, Workshop, Paper 1, p. 7; ders., OECD-paper, p. 22; Baran, House-Hearings, p. 162; Warner-Stone, a. a. O., p. 203.

[86]) Hoffman, a. a. O., pp. 89 seq.

auch Geld, je sicherer sie sind, desto mehr. Exakte Kostenberechnungen fehlen jedoch, da sie nur im Zusammenhang mit einem konkreten System möglich sind [87]).

3. Verschlüsselung

a) Bei der Speicherung

Als wirksamste Zugriffskontrolle wird die vollständige obligatorische Verschlüsselung der Daten bei der Eingabe in den Computer angesehen [88]). Die Verschlüsselung stellt einen großen Schutz vor unbefugtem Zugriff dar. Dennoch wäre die Gefahr, daß Fachleute von dem Typ der Maschine auch auf deren inneren Computer-Schlüssel schließen könnten, nicht gebannt. [89]) Eine Häufung von verschiedenen Codes wird nicht empfohlen. Dies hätte nämlich zur Folge, daß neue Fehlerquellen entstehen könnten, die das Sicherheitsstreben zunichte machen würden [90]). Das zeigt, daß auch Verschlüsselungen allein keinen wirksamen Schutz gewährleisten können. Bei der Speicherung von Dossiers mit persönlichen Daten soll nur eine Codenummer, die ein verschlüsseltes Personenkennzeichen ist, die Zuordnung ermöglichen [91]). Der Nummernindex sollte separat gespeichert werden. Dieses System eignet sich besonders für statistische Datenbanken, ist aber keineswegs undurchdringlich.

Darüber hinaus wird vorgeschlagen, die elektronischen Speicher auch mit Schutzfolien gegen „Abhörtechniken" (i. übertr. Sinne) zu schützen [92]).

b) Bei der Übermittlung von Daten

Bei der Datenfernübertragung ist die Gefahr des Anzapfens von Datenleitungen gegeben [93]). Aus den obengenannten Gründen reicht jedoch eine Verschlüsselung für die Übermittlung allein nicht aus. Bei der Übertragung über öffentliche Leitungen sollte daher eine Verzerrung zugeschaltet werden [94]).

Die Entzerrung kann dann nur von dem Adressaten-Terminal erfolgen.

4. Festsetzung von Geheimhaltungsstufen

Ein anderer Schutz gegen eine unbefugte Entnahme der gespeicherten Daten wird in einer Staffelung der Daten je nach dem Grad ihrer Vertraulichkeit gesehen [95]). Durch die Staffelung hätte man die Möglichkeit, mit steigendem Vertraulichkeitsgrad weniger Personen eine Zugriffsberechtigung zu geben. Von anderer Seite wurde jedoch auch mit Recht bezweifelt, ob es möglich sei, Daten in Geheimhaltungsstufen zu klassifizieren. [96])

5. Auswahl des Bedienungspersonals

Obgleich noch andere Vorschläge für eine wirksame Systemkontrolle diskutiert werden könnten, es bleibt dabei, daß das Sicherheitssystem „bezwungen" werden kann [97]). Die Skala der „potentiellen Bezwinger" reicht von dem Programmierer und den Mechanikern bis zu denen, die beim Hersteller des Computers beschäftigt sind und daher die Sicherheitssysteme, insbesondere die mitgelieferte Software, kennen. Alle diese Personen haben in der Regel Zutritt zu der Anlage. Diese Gruppe ist somit das weichste Glied in der Kette der Sicherheitsvorkehrungen. Dieser Eindruck verdichtet sich, wenn man die Ausbeute eines konventionellen Aktendiebstahls mit dem Umfang von Indiskretionen vergleicht, die Personen möglich sind, die von der Konsole eines Informationssystems Daten erreichen können, die physisch zu stehlen den Einsatz von tausend oder mehr bestochenen Putzfrauen erforderlich machen würde [98]). Deshalb sind vorrangige Schutzmaßnahmen gegen den Datenmißbrauch letztlich höhere berufliche Anforderungen an das Bedienungspersonal [99]). Strenge Auswahlkriterien und verpflichtende Berufsrichtlinien an das Bedienungspersonal werden zum integrierten Bestandteil der technischen Schutzmaßnahmen selbst in einem gesetzlich geregelten System [100]). Über die Notwendigkeit von beruflichen Kriterien für das Bedienungspersonal sind sich die meisten Autoren einig; konkrete Vorschläge hierzu lassen sie aber leider vermissen [101]). Es bleibt somit dem Gesetzgeber überlassen, durch Gesetze oder Verordnungen berufsständische Prinzipien und Auswahl- und Überprüfungskriterien aufzustellen. Bis dahin ist jedoch noch ein weiter Weg.

---

[87]) Vgl. Warner-Stone, a. a. O., p. 210, spricht von 3½ bis 7½ % und 20 % in Extremfällen.

[88]) Miller, Senatement, Hearings, p. 78; Hoffman, a. a. O., p. 93; Baran, The Computer Conference Las Vegas, 1965; D'Agapeyeff, Workshop, Annex; Westin, Communications of the ACM, Vol. 10, p. 553; Warner-Stone, a. a. O., p. 199.

[89]) Warner-Stone, a. a. O., p. 203.

[90]) Hoffman, a. a. O., p. 93.

[91]) Chartrand, Law and Computer Technology, Oct. 1968, p. 18; Niblett, OECD-paper, a. a. O., p. 24.

[92]) Miller, 67 Mich.L.Rev. 1208.

[93]) Hoffman, a. a. O., p. 90; Miller, Senate-Hearings, p. 78.

[94]) Warner-Stone, a. a. O., p. 199; Miller, 1967 Atlantic, Oct. p. 57; Niblett, OECD-paper, a. a. O., p. 21.

[95]) Miller, 67 Mich.L.Rev. 1209; Baran, a. a. O.; Hargreaves, Workshop; Sharp, Workshop.

[96]) Vgl. Pipe, 18 Am.U.L.Rev. 542. Der Verfasser hält es für ausgeschlossen. Vgl. Kamlah, DÖV 70, 364.

[97]) Miller, 67 Mich.L.Rev. 1217; Warner-Stone, a. a. O., p. 192/193; Hoffman, a. a. O., p. 89; Peters and Turn, a. a. O., p. 294.

[98]) Vgl. Warner-Stone, a. a. O., p. 208; Hoffman, a. a. O., p. 90.

[99]) Niblett, Workshop, paper 1, p. 7; Niblett, OECD-paper, a. a. O., p. 14, 48; D'Agapeyeff, Workshop, Anhang, p. 6, 7; Warner-Stone, a. a. O., p. 191; Miller, 67 Mich.L.Rev. 1217; Piore, House Hearings on Computer Privacy, p. 119; Karst, 31 L.a.C.P., p. 362/3; Westin, 66 Col.L.Rev. 1205, 1208; Watson, a. a. O., p. 10.

[100]) Westin, 66 Col.L.Rev., p. 1218; Niblett, a. a. O., p. 14; Miller 67 Mich.L.Rev. 1217; Michael, 33 Wash. L.Rev. 279.

[101]) Der einzige bekanntgewordene Vorschlag ACM Code of Professional Conduct, abgedr. bei Warner-Stone, Appendix II, p. 232, zeigt die Schwäche berufsethischer Regeln.

C. Politische Schutzmaßnahmen

1. Staatliche Kontrolle

a) Anzeigepflicht

Um Datenbanken einer staatlichen Kontrolle zugänglich zu machen, kann der Gesetzgeber den Unternehmer — auch den öffentlichrechtlichen — gegenüber einer Aufsichtsbehörde anzeigepflichtig machen. Diese Form staatlicher Überwachung wird von sehr vielen Autoren für notwendig gehalten [102]).

Die Anzeigepflicht bewirkt, daß die Aufsichtsbehörde die Einhaltung eines Datenschutzgesetzes überwachen kann. Darüber hinaus hat die Allgemeinheit die Möglichkeit, Einfluß zu nehmen. Daß auch dies der Zweck der Anzeigepflicht ist, wird dadurch verdeutlicht, daß das Datenbankregister öffentlich sein soll [103]).

b) Erlaubnispflicht

Eine stärkere Kontrolle gibt der Gesetzgeber dem Kontrollorgan in die Hand, wenn dieses nicht nur Anzeigen entgegennehmen sondern auch Lizenzen vergeben kann, was die Befugnis einschließt, den Betrieb nicht genehmigter Datenbanken zu untersagen [104]). Von einigen wird ein Genehmigungsverfahren nur gegenüber privaten Datenbanken gefordert [105]). Die Genehmigungsbehörde kann von Anfang an sicherstellen, daß die Vorschriften eines Datenschutzgesetzes eingehalten werden können, indem es den Betrieb nicht genehmigt, wenn ausreichende technische Schutzvorkehrungen oder personelle Voraussetzungen fehlen.

Besonders hervorzuheben ist hier das Control of Personal Information Bill [106]), das gänzlich auf dem Genehmigungsprinzip beruht. Über das Instrument der Auflagen können weitere Ziele des Schutzes der Privatsphäre erreicht werden, wie z. B. das Einsichtsrecht des Betroffenen [107]), die Offenbarungspflicht bezüglich der Informanden [108]) und der aus den Daten gegebenen Auskünfte [109]) und anderes mehr.

c) Anknüpfungspunkt „Datenbank"

Als Anknüpfungspunkt für gesetzliche Regelungen wird meist nur von „Datenbanken" gesprochen, die der Kontrolle oder einem Gesetz unterliegen sollen [110]). Die Schwierigkeiten beginnen aber erst, wenn gefragt wird, was denn eine Datenbank eigentlich sei [111]).

Zur Anknüpfung bieten sich zwei Kriterien an, der Computer als formelles und die Datensammlung als materielles. Die umfangreiche Datenbankdiskussion, die von den Plänen zu einem National Data Center ausgelöst wurde, ging von einer Computer-Datenbank aus, die es noch nicht gab, die sich nur ungefähr vorstellen ließ und der vielleicht ein integriertes Verwaltungsinformationssystem auf ADV-Basis am nächsten kommt, wie es bei uns zwischen Bund, Ländern und Gemeinden diskutiert und aufgebaut wird [112]). Hier ging man wohl davon aus, daß jede dem Verbund angeschlossene Stelle zu überwachen sei, soweit sie Daten in Computern oder computerlesbarer Form speichert [113]).

Die Kreditauskunfteien dagegen wurden vom Gesetzgeber anders behandelt. Das materielle Kriterium gab den Ausschlag. Jede Kreditauskunftei fällt unter das Gesetz, gleich in welcher Form sie ihre Daten speichert [114]). Auch die kalifornischen Vorschläge knüpfen — etwas modifiziert — an das materielle Kriterium an [115]). Den Computerdatenbanken wird lediglich eine Übergangsfrist zur Umstellung zugebilligt [116]). Nur die Anmeldepflicht ist auf sie beschränkt. Uneingeschränkt gilt das materielle Kriterium in allen Fassungen des S. 975 [117]).

Das materielle Kriterium setzte sich auch im Control of Personal Information Bill [118]) durch, wenn auch eingeschränkt durch formelle Tatbestandsmerkmale, ohne die ein Datenschutzgesetz in der Praxis wohl kaum vollziehbar ist. Die formellen Einschränkungen gelten jedoch losgelöst vom Speichermedium. Es sind Datensammlungen angesprochen, bei denen mehr als 100 000 Personen betroffen sind. Werden Datensammlungen geringerer Größe im Verbund mit anderen entsprechenden Datensamm-

---

[102]) Vgl. Data Surveillance Bill 1969, Sec. 1; Bill 182 (Reid-Bill, Ontario), Sec. 2; Assembly-Bill 1982, Calif. Gov.Code, § 6253 d (1970).

[103]) Data Surveillance Bill 1969, Sec. 1 (7).

[104]) Jacob, Workshop, paper 11, p. 3; D'Agapeyeff, Workshop, Anhang, p. 7, Control of Personal Information Bill 1971; Sharp, Workshop, paper 8, p. 1; Kingston-Summaries conclusion 6: Die meisten workshops traten für Genehmigungspflicht ein.

[105]) Ryan-Report, a. a. O., p. 85, für Detekteien, Auskunfteien.

[106]) House of Commons, Feb. 2, 1971.

[107]) Sec. 6 (6) (b).

[108]) Sec. 6 (7) (a) (ii).

[109]) Sec. 6 (7) (a) (iii).

[110]) Vgl. Pipe, 18 Am.U.L.Rev. 547; 35th Report, a. a. O., p. 5 seq.; Miller, 67 Mich.L.Rev. 1089 (1969) spricht nur von Computerdatenbanken, als ob es konventionelle Datenspeicherung überhaupt nicht mehr gäbe!

[111]) Vgl. die Unsicherheit hierzu bei den einzelnen workshops der Kingston, Ontario, Conference 1970, Summaries No. 6.

[112]) Vgl. Pipe, 18 Am.U.L.Rev. 539.

[113]) Reid Bill 182, Sec. 1 (b); Data Surveillance Bill (1969), Sec. 1 and 10.

[114]) 15 U.S.C. § 1681 a, Consumer Credit Reporting Act; § 371 (e) N.Y. Credit Data Reporting Act (1970)

[115]) Assembly Bill 1381, Cal.Gov.Code Sec. 6252 (d): „all papers, maps, magnetic or paper tapes, photographic films and prints, magnetic or punched cards, discs, drums, and other documents containing information relating to . . .".

[116]) Assembly Bill 1982 (1970), Cal.Gov.Code, Sec. 6253 (c).

[117]) 5 U.S.C. § 552 a (a), Congr.Record, S. 11354 (1971).

[118]) Bill 98, House of Commons, Feb. 2, 1971, Sec. 6 (5).

lungen benützt, so gilt das Gesetz, wenn die Zahl 100 000 durch Zusammenrechnung der betroffenen Personen in jeder Datensammlung erreicht wird.

Solche Datensammlungen sind dann Datenbank im Sinne des Gesetzes [119]). Daran wird deutlich, daß die Computer-Datenbank zwar der Anlaß für das Einschreiten des Gesetzgebers ist. Sie gibt aber nicht ohne weiteres den Rahmen für gesetzliche Bestimmungen ab [120]).

2. Überwachungsorgan

a) Arten

Als Überwachungsorgan wird die Einrichtung eines Ombudsmannes in Datenangelegenheiten gefordert [121]), der von amtswegen oder nach Anrufung von seiten des Betroffenen für den Schutz der Rechte des einzelnen Bürgers eintritt. Der Ombudsmann soll eine unbürokratisch arbeitende Beschwerdestelle sein, die dem Betroffenen das Gefühl der Ohnmacht gegenüber dem Behördenapparat nehmen soll. Der Vorteil dieser Einrichtung ist in der Unabhängigkeit und Volksverbundenheit des Ombudsmannes zu sehen [122]). Ein Ombudsmann wird in den USA auch ohne Zusammenhang mit dem right of privacy gefordert, was wohl eine Modeerscheinung ist, wie bei uns, vielleicht aber auch damit zusammenhängt, daß der Rechtsschutz im öffentlichen Recht nicht so klar geregelt ist [123]).

Um aber bei der Vielfalt der anfallenden Probleme die Übersicht zu behalten, müßte der Typ eines technisch versierten Ombudsmannes gefordert werden [124]). Aber auch dann käme man nicht umhin, dem Ombudsman einen Expertenstab anzugliedern, um die technischen, sozialen und rechtlichen Probleme und Gesichtspunkte bei der Datenspeicherung und Datenübermittlung exakt erfassen und somit überwachen zu können [125]). Deshalb wird auch vorgeschlagen, anstelle eines einzelnen Ombudsmannes eine „watch-dog"-Kommission zu errichten [126]). Dieser Kommission sollten sowohl Repräsentanten aus verschiedenen Gruppen der Gesellschaft [127]) als auch eine noch festzulegende Anzahl von Fachleuten angehören, um die anfallenden technischen Probleme zu lösen [128]).

Mit dem Assembly Bill No. 1982 wurde vorgeschlagen, dem nach dem Cal.Gov.Code bereits bestehenden Intergovernmental Board on Electronic Data Processing, zwei Mitglieder aus dem öffentlichen Leben beizugeben, deren Aufgabe es sein soll, die Einhaltung der Vorschriften zum Schutze der Privatsphäre zu überwachen [129]). Damit schließt sich der Gesetzgeber geeigneten bestehenden Institutionen an. Diesen Weg beschreiten auch die Vorschläge der Fair Credit Reporting Acts, die Kreditauskunfteien der Aufsicht von Ministerialbehörden zu unterstellen [130]). Der Gesetzgeber ist im Fair Credit Reporting Act von 1970 dem Senatsvorschlag gefolgt, indem der FTC die Aufsicht anvertraut wurde [131]). Allerdings wird vertreten, daß sich Ministerien zur Aufsicht gegenüber staatlichen Datenbanken schlecht eignen, weil die dafür notwendige Unabhängigkeit fehle [132]).

Im Control of Personal Information Bill nimmt die Überwachungsbehörde natürlich eine zentrale Stellung ein. Sie ist zweigeteilt in eine Verwaltungs- und Untersuchungsbehörde (Chief Inspector of Data Banks) und eine richterliche Behörde (Tribunal) [133]). Auf diese interessante Konstruktion kann an dieser Stelle nur hingewiesen werden. Alle Entscheidungen werden vom Tribunal in richterlicher Unabhängigkeit getroffen.

Ein weiterer erwähnenswerter Vorschlag ist S. 1550 [134]). Hier ist eine aus Parlamentariern und Bürgern zusammengesetzte Kommission zur Untersuchung der gesamten staatlichen Datenüberwachung vorgeschlagen. Die Arbeit der Kommission soll nach einem Jahr in Gesetzgebungsarbeit übergehen [135]).

b) Aufgaben des Überwachungsorgans

Das Überwachungsorgan führt das Datenbankregister [136]) bzw. genehmigt den Betrieb von Datenbanken [137]). Darüber hinaus überwacht es laufend die ihm unterstehenden Datenbanken und untersucht, ob Datenschutzgesetze verletzt werden.

Die Kontrollbehörde soll

— bei Verstößen gegen die Datenschutzgesetze Anordnungen treffen können [138]). Ist eine Daten-

---

[119]) Sec. 6 (1) and (5).
[120]) Vgl. workshop No. 3, Kingston, Ontario, Conference 1970.
[121]) Miller, Statement, Senate-Hearings, p. 77; Ryan-Report, a. a. O., p. 97; Warner-Stone, a. a. O., p. 190; Jacob, Workshop, paper 11.
[122]) Miller, Statement, ebd.; Ryan-Report, a. a. O., p. 98.
[123]) Administrative Ombudsman Experimentation Act of 1971, H.R. 9562, Congr. Record June 30, 1971, H. 6193.
[124]) Warner-Stone, a. a. O., p. 190.
[125]) Vgl. Computer World, August 1969, p. 20.
[126]) 35th Report, a. a. O., p. 8; Westin, Workshop, Annex p. 5; Miller, 1967 Atlantic, Nov. p. 57; Cal.Gov.Code, Assembly Bill 1982, 1970; Ryan-Report, a. a. O., p. 97.
[127]) Vgl. Amendment 261 of S. 975, 5 U.S.C. § 552 Sec. 2.
[128]) Sharp, Workshop, p. 2.
[129]) Assembly Bill 1982, Apr. 1970, Calif. Legislature.
[130]) Vgl. S. 823, § 620: Federal Trade Commission; H.R. 6071: Federal Reserve Board; H.R. 16340, Sec. 21: Federal Reserve Board.
[131]) 15 U.S.C. § 1681 s, Fair Credit Reporting Act, Pub.L. 91 bis 508, 1970, Oct. 20th.
[132]) Westin, Workshop, Anhang; Miller, 67 Atlantic, Nov. p. 56; ders., Senate-Hearings, a. a. O., p. 79; Sharp, Workshop, paper 8, p. 2.
[133]) Vgl. Sec. 1 bis 4, Control of Personal Information Bill 1971.
[134]) The Constitutional Rights and Civil Liberties Protection Act of 1971, Cong.Record, Senate, Apr. 15, 1971, S. 4910 seq.
[135]) Auch in anderen Gesetzesvorschlägen findet sich oft ein spezielles Überwachungsorgan, wie z. B. im S. 1438, Bill to protect the civilian employees . . . (Sen. Ervin), Congr.Record, April 1, 1971, S. 4227, Sec. 5.
[136]) Data Surveillance Bill 1969, Sec. 2.
[137]) Kingston-Summaries, conclusion Nr. 5; Control of Personal Information Bill 1971, Sec. 6.
[138]) Fair Credit Reporting Act 1970, 15 U.S.C. § 1681 s (a) (6); Amendment No. 261 of S. 975, 5 U.S.C. § 552 Sec. 2 (b).

speicherung unzulässig, ist deren Löschung anzuordnen [139]).

- Klagen von Bürgern hören und verbescheiden [140]). Dazu kann sie auch Hearings abhalten [141]).
- die von Datenschutzgesetzen jeweils festgesetzten Sicherheitsauflagen überwachen [142]), damit sie auch angewendet werden, und sie auf ihren Sicherheitsgehalt überprüfen [143]).
- Richtlinien für die Datenspeicherung und Datenweitergabe erarbeiten [144])
- dem Parlament jährlich einen Bericht über die Entwicklung der Datenverarbeitung vorlegen [145]). Der Bericht sollte auch Verbesserungsvorschläge für Datenschutzgesetzgebung enthalten [146]). Die Berichterstattung ist besonders im S. 1550 [147]) eine hervorragende Aufgabe.

Dies sind die am häufigsten genannten Aufgaben [148]). Natürlich soll die Kontrollbehörde auch besondere Rechte zur Erfüllung ihrer Aufgaben haben, wie z. B. Hearings abzuhalten, Zeugen zu vernehmen, Beweismittel zu beschlagnahmen, Amtshilfe anderer Behörden in Anspruch zu nehmen und vieles mehr [149]).

[139]) Sharp, Workshop, paper 8; Miller, 1967 Atlantic, Nov. p. 57; ders., Senate-Hearings, a. a. O., p. 79; Chartrand, 1968 L.a.C.T. Oct. p. 18; Control of Personal Information Bill 1971, Sec. 7.
[140]) Amendment No. 261 of S. 957, a. a. O.
[141]) ebd.
[142]) Ryan-Report, a. a. O., p. 98; Miller, 1967, Atlantic, Nov. p. 57)
[143]) S. 1550, Sec. 3 (9) und Begründung dazu in Congr. Record, S. 4911, oben Fußn. 58.
[144]) Kingston-Summaries, conclusion Nr. 5; Ryan-Report, a. a. O., p. 98.
[145]) Data Surveillance Bill 1969, Sec. 3 (1); Miller, Senate-Hearings, a. a. O., p. 78; Ryan-Report, a. a. O., p. 99.
[146]) Ryan-Report, a. a. O., p. 99.
[147]) Vgl. Fußn. 58.
[148]) Für weitere vgl. Ryan-Report, a. a. O., p. 97 seq.; Kingston-Summaries, conclusions 5 und die Gesetzentwürfe.
[149]) Ausführlich S. 1550, Sec. 4 (a) (b), vgl. oben Fußn. 58.

D. Rechte des Betroffenen

Wie in den vorhergehenden Abschnitten gezeigt wurde, sind unter den möglichen gesetzlichen Schutzmaßnahmen die Rechte des Betroffenen zu seinem eigenen Schutz durchaus nicht das einzige, was den Schutz der Privatsphäre gewährleisten kann. Die Rechte des Betroffenen werden jedoch in der Literatur dadurch besonders betont, als ihre Erörterung am meisten wiederkehrt, sozusagen den größten Raum einnimmt. Die Gewährleistung dieser Rechte ist wohl auch in der Tat die Bedingung, mit der die Wirksamkeit aller sonstigen gesetzlichen Maßnahmen steht und fällt [150]). Zu fordern ist daher eine „Computer Bill of Rights" [151]), ein Bündel von Minimalrechten, deren Rang den Freiheitsrechten gleichkommt [152]).

1. Einsichtsrecht

a) Das Einsichtsrecht des Betroffenen nimmt unter seinen Rechten die Schlüsselstellung ein. Es wird daher von so gut wie allen Autoren gefordert, daß dem Betroffenen Zugang zu den ihn betreffenden Daten gebühre [153]). Ebenso fehlt das Einsichtsrecht in keinem Gesetzentwurf [154]).

Nach einem Zeitungsbericht hat bereits der Stadtrat von Queens, N. Y., ein Einsichtsrecht der Bürger im Zusammenhang mit einer Satzungsvorlage beraten [155]).

Das Einsichtsrecht des Betroffenen ist so elementar, daß es von den Kreditauskunfteien teilweise schon freiwillig gewährt wird [156]). Die großen Kreditauskunfteien haben auch keine Einwendungen gegen ein Einsichtsrecht der Betroffenen [157]). Eine Kreditagentur, der es auf nichts anderes ankommt, als auf eine zuverlässige Kreditbeurteilung, kann sich nur wünschen, daß der Betroffene sein Dossier überprüft und dadurch die Dienste der Kreditagentur zuverlässiger macht [158]). Das Einsichtsrecht ist daher auch in das Fair Credit Reporting Act 1970 aufgenommen worden und gilt in der vom Senat [159]) vor-

[150]) Westin, Workshop: Due process, habeas corpus, habeas data!
[151]) Van Tassel, The Computer Versus Privacy; A Computer Bill of Rights, 1970 L.a.C.T. Jan. p. 2; vgl. auch Lance J. Hoffman, Computers and Privacy: A Survey, Computing Surveys, June 1969, (p. 88) (1969), der auf John McCarthy hinweist, der 1966 ein „computer bill of rights" gefordert habe. Fatmi/Young, Habeas Scriptus, Workshop, paper 7; Kingston Conference Summaries, Abschnitt 7.
[152]) Vgl. auch Niblett, OECD-Papier, a. a. O., p. 34: habeas scriptum.
[153]) Miller, Statement, Senate Hearings, p. 77; ders., 1967 Atlantic, Nov. p. 55; ders. 67 Mich.L.Rev. 1212; Kingston Conference Summaries, Abschn. 7; Westin, Workshop, p. 5; Karst, 31 L.a.C.P. 342 ff., 358 (1966); Warner-Stone, a. a. O., p. 190.
[154]) Data Surveillance Bill, 1969, Sec. 4 (1); Bill 182 (Reid-Bill, Ontario), Sec. 5; § 6256 Cal. Gov. Code (1967); S. 823, § 609, 610; H.R. 6071, § 164; H.R. 16340, Sec. 31; S. 975 (1971) § 552 a Sec. (a) (4).
[155]) N.Y. Times, 29. 3. 1971.
[156]) Warner-Stone, a. a. O., p. 188.
[157]) Vgl. Analysis of H.R. 16340, Sec. 31, Credit-Hearings, 70, p. 145 (Spafford, ACB, Inc.); Jordan, Statement, Credit-Hearings 1970, p. 156 seq., 160: „I have no quarrel with the general concept expressed in sec 31".
[158]) Vgl. Karst, 31 L.a.C.P., p. 355: Einige Kreditagenturen haben sich diese Einsicht schon lange zunutze gemacht.
[159]) S. 823.

geschlagenen Form [160]). Ebenso gilt es im „credit data reporting act" des Staates New York [161]).

Auch der Staat hat wenig Grund, seinen Bürgern generell die Einsicht in ihn betreffende Unterlagen zu verwehren, da in den USA ohnehin der auf dem common law beruhende Grundsatz gilt, daß öffentliche Akten und Register von jedermann eingesehen werden dürfen [162]). Der Gesetzgeber hat Mühe, diesen Grundsatz aufrechtzuerhalten. Die Ausnahmen werden immer zahlreicher. Daher beschränkt sich die Aufgabe, das Einsichtsrecht des Betroffenen gesetzlich zu verankern, zunächst darauf, es unbeschadet der gegenüber Dritten erlassenen Ausnahmen vom allgemeinen Einsichtsrecht zu gewährleisten [163]).

---

[160]) 15 U.S.C. § 1681 g, Pub.L. 91 bis 508 (1970).

[161]) § 372 Gen.Bus.Law 1970, L. 1970, C 300, eff. Nov. 1, 1970.

[162]) Vgl. Kamlah, a. a. O., S. 126; anders in Deutschland: vgl. Hess. Datenschutzgesetz, wo ein Einsichtsrecht nicht besonders normiert wurde.

[163]) Vgl. Sec. 6253, 6254, 6256 Cal. Gov. Code; S. 975 (1971) § 552 a (a) (4) Freedom of Information Act; H.R. 854, Congressional Record H. 2948 (1971, Apr.).

[164]) Miller, Statement, Senate-Hearings, p. 77; Karst, 31 L.a.C.P. 374; Warner-Stone, a. a. O., p. 204.

[165]) Miller, ebd.

[166]) Miller, ebd.; Karst, 31 L.a.C.P. 374 für sonstige Fälle etwas allgemeiner. Vgl. auch Miller, 67 Mich.L. Rev. 1212, der vorschlägt, den „print-out" mit einer anderen periodischen Nachricht zu versenden (bei uns z. B. mit der jährlichen Lohnsteuerkarte).

[167]) H.R. 16340 Sec. 31; H.R. 6071, § 164, S. 823 §§ 609, 610 (hier auch Telefonauskunft möglich).

[168]) Credit-Hearings 70, p. 145, Analysis of H.R. 16340, Sec. 1 (Spafford, ACB, Inc.); dagegen Jordan, Statement, p. 156 seq., p. 161 oben.

[169]) Tgl. Analysis of S. 823, Credit-Hearings 1970, p. 94, Section 610.

[170]) 15 U.S.C. § 1681 h (e).

[171]) Statement, p. 161.

[172]) Vgl. Antragsformular der ACB, Inc., Credit-Hearings 1970, p. 141.

[173]) 15 U.S.C. § 1681 h (b) (2).

[174]) H.R. 16340, Sec. 31 (a).

[175]) Karst, 31 L.a.C.P. 374; Cal.Gov.Code, § 6253 (b) (1970); S. 975 (1971) § 552 a (a) (4); H.R. 854, Congressional Record, H. 2948 (1971, Apr.)

[176]) Cal.Gov.Code (1967) § 6256; Data Surveillance Bill, Sec. 4 (1).

[177]) Cal.Gov.Code, § 6257; H.R. 16340, Sec. 31 (a); Data Surveillance Bill, Sec. 4 (1).

[178]) Miller, Statement, Senate-Hearings, p. 77.

[179]) Karst, 31 L.a.C.P. 368; S. 975 (1971), § 552 a, Sec. (d) (2); H. R. 854, Congressional Record, H. 2948, (1971 Apr.).

[180]) S. 975 (1971), § 552 a, Sec. (d) (1); H.R. 854, Congressional Record, H. 2948 (1971, Apr.).

[181]) Westin, Science, Privacy and Freedom: Issues and Proposals for the 1970's, 66 Col.L.Rev. 1227 (1966); Data Surveillance Bill, Sec. 2 (1).

[182]) Data Surveillance Bill, Sec. 3 (1); Bill 182 (Reid-Bill, Ontario), Sec. 4: Hier keine Ausnahme für Sicherheitsdienste, da der Staat Ontario seine Regelungen nicht auf die Bundesbehörden und die Armee erstrecken kann.

[183]) S. 975 (1971), § 552 a, Sec. (d) (3).

b) Über die Form der Ausübung des Einsichtsrechts besteht weitgehend Unklarheit. Sie ist auch von sekundärer Bedeutung, wenn sie nicht so gestaltet wird, daß den Betroffenen die Wahrnehmung ihrer Rechte unangemessen erschwert ist. Einigkeit besteht nur insoweit, als die Einsichtgewährung in jeder Form etwas kostet, der Schutz der Privatsphäre aber auch einen Preis wert ist [164]).

Bei einem National Data Center würden natürlich die Portokosten für die Versendung eines jährlichen „print-out", wie es von Miller angeregt wurde [165]), sehr ins Gewicht fallen. Daher könnte ein Antragserfordernis verbilligend wirken, da viele Bürger nicht jährlich einen Antrag stellen würden [166]).

Für die Kreditauskunfteien wurde lediglich die Einsichtnahme durch den Betroffenen an Ort und Stelle vorgeschlagen [167]), wohl um zu vermeiden, daß der Betroffene sich einen Ausdruck seines Dossiers herstellen läßt, um diesen bei Kreditanträgen vorzulegen und u. U. in wenigen Stunden bei mehreren Banken Geld zu borgen. Im Gegensatz zum S. 823 bestimmt H. R. 16340 Sec. 31 (b), daß die Einsichtnahme nicht davon abhängig gemacht werden kann, daß der Betroffene die Auskunftei für vergangene Rechtsverletzungen von Schadensersatzansprüchen freistellt. Eine solche Freistellung wurde auch aus der Sicht einer großen Kreditauskunftei nicht für notwendig gehalten [168]). Der Gesetzgeber ist aber zunächst dem Senatsvorschlag gefolgt, und hat — trotz der dagegen vorgetragenen Kritik — [169]) das Einsichtsrecht nur gleichzeitig mit einer Haftungsfreistellung gewährt [170]). Dieses System kann natürlich nur funktionieren, wenn die Auskunftei genügend Zweigstellen unterhält, bei denen Einsicht genommen werden kann. Darauf weist besonders Jordan [171]) hin, indem er die Möglichkeit der Telefonauskunft empfiehlt [172]), die vom Fair Credit Reporting Act auch vorgesehen ist [173]).

Der Betroffene darf Notizen aufnehmen [174]), oder alles abschreiben, was ihm vorgelegt wird [175]). Sofern Daten in einen Computer gespeichert werden, kann der Betroffene nicht Einsicht nehmen, wenn die Daten nicht ausgedruckt sind. Daher ist ihm in diesem Falle in der Regel (ausgenommen bei Kreditauskünften) auch der Ausdruck auszuhändigen [176]). Zuweilen wird eine angemessene Verwaltungsgebühr verlangt [177]), die die Selbstkosten nicht übersteigen darf.

c) Das Einsichtsrecht kann natürlich nicht ganz ohne Ausnahme gewährt werden. Soweit Geheimhaltungsbedürfnisse rechtlich anzuerkennen sind, stehen sie dem Einsichtsrecht entgegen [178]).

Im strafprozessualen Ermittlungsverfahren gelten die Schranken des Prozeßrechts [179]). Die Akten der Sicherheitsdienste müssen den Betroffenen verschlossen bleiben [180]). Einen Sicherheitsdienst kann man nur politisch kontrollieren [181]). Auch werden Akten und Datenbanken der Polizeibehörden von einigen ganz ausgenommen [182]). Interessant ist, daß es für nötig gehalten wird, Ausnahmen für Briefe und Arbeitspapiere von Behörden zu machen, die der Willensbildung und Entscheidungsfindung im Staatsapparat vorangehen [183]).

d) Um das Einsichtsrecht zu ermöglichen, muß der Betroffene wissen, wo etwas über ihn gespeichert ist. Daher hat der Unternehmer einer Datenbank dem Betroffenen mitzuteilen, wenn er erstmals Daten über ihn in die Datenbank aufnimmt, also das Dossier eröffnet [184]). Andere Methoden, die das gleiche Ziel erreichen, nämlich die Betroffenen wissen zu lassen, wo sie Einsicht nehmen müssen, werden im Zusammenhang mit der Registrierungspflicht von Datenbanken vorgeschlagen: So hält es der Cal. Gov. Code (1970) für ausreichend, wenn der Unternehmer einer Datenbank der zuständigen Aufsichtsbehörde allgemein mitteilt, über welche Personengruppen Daten gespeichert werden [185]). Im englischen Data Surveillance Bill wird dies und die Eröffnungsmitteilung nebeneinander vorgeschlagen [186]).

e) Preisgabe der Informanden.

In den Gesetzentwürfen zur Regelung des Auskunfteiwesens begegnen wir noch einer interessanten Erweiterung des Einsichtsrechts, die den systematischen Zusammenhang mit dem Berichtigungsrecht besonders deutlich macht. Die Kreditauskunftei muß, wenn der Betroffene die Richtigkeit einer Information bestreitet, und weder die Auskunftei die Richtigkeit, noch der Betroffene die Unrichtigkeit der Information beweisen kann, entweder die Information löschen oder den Informanden preisgeben [187]). Die Vertreter der Auskunfteien haben sich nicht grundsätzlich gegen diese Verpflichtung gesträubt, jedoch eine Freistellung der Informanden von Klagen des Betroffenen gewünscht [188]). Diesem Wunsch ist der Bundesgesetzgeber im Fair Credit Reporting Act gefolgt [189]). Eine ähnliche Regelung gilt im Staate New York [190]).

2. Berichtigungsrecht

a) Als Ausfluß des Persönlichkeitsrechts hat der Betroffene einen Berichtigungsanspruch gegen Entstellung seiner Daten. Er muß sich nicht gefallen lassen, vor seiner Umwelt in einem falschen Licht zu erscheinen [191]).

Daher wird von allen Autoren, die sich mit den Problemen der ADV befassen, ein Berichtigungsanspruch gegenüber Datenbanken vorgeschlagen [192]). Der Berichtigungsanspruch ist leichter gefordert als durchgeführt, da die Fehlerquellen sehr unterschiedlich sein können. Sie wurden verschiedentlich genauer untersucht [193]).

Daten können zunächst stets falsch sein, da sie einen Lebensvorgang niemals vollständig beschreiben. Die Eintragung einer Vorstrafe ist dann irreführend, wenn den Empfänger die Resozialisierung des Täters interessiert [194]), oder z. B. der Zusatz: „Überzeugungstäter" weggelassen ist [195]). Die Eintragung „geschieden" ist richtig und falsch zugleich, wenn über die Wiederverheiratung der Geschiedenen nichts ausgesagt ist [196]). Um den Wahrheitsgehalt einer Eintragung zu prüfen, muß daher feststehen, zu welchem Zweck die Daten gespeichert sind [197]) In einem allgemeinen Informationssystem dürfte dies sehr schwierig sein [198]). Auch aus diesem Grunde ist die Entfremdungsregel von fundamentaler Bedeutung. Ihre Aufhebung muß zu unrichtiger Datenübermittlung und damit zu Ungerechtigkeiten führen [199]).

Die Fehlerquellen werden erweitert, wenn man bewertende Äußerungen als Daten behandelt und speichert. Bewertende Attribute sind nicht nur vom Zusammenhang abhängig, in dem sie gegeben werden, sondern auch in sich schillernd und geben zu Mißdeutungen Anlaß [200]). Werden Bewertungen weitergegeben, sind sie falsch, wenn der Empfänger nicht dieselben Bewertungsgrundsätze anwendet [201]).

b) Aus diesen Überlegungen folgt, daß dem Berichtigungsanspruch des Betroffenen auf verschiedenste Art genügt werden muß.

Was schlicht falsch ist, z. B. Namensverwechslung, falsche Anschrift, falsche Daten usw., ist durch das Richtige zu ersetzen [202]). Was qualifiziert falsch ist („contextual error"), ist u. U. zu erweitern [203]), indem eine Erklärung des Betroffenen hinzugefügt wird [204]). Letzteres hat auch zu geschehen, wenn ein

---

[184]) § 372 N.Y. Gen.Bus.Law 1970: Credit data reporting act; Data Surveillance Bill, Sec. 4 (1); Bill 182 (Reid-Bill) Sec. 5 (1); Richard J. Miller, Computers and the Law of Privacy, 1968 Detamation, Sept. p. 55; Fatmi/Young, Workshop, Paper 7; S. 975 (1971) § 552 a (a) (1) „Freedom of Information Act"; H.R. 854, Congr. Record H. 2948 (1971, Apr.); Warner-Stone, a. a. O., p. 190 (Thesen des NCCL).

[185]) Cal.Gov.Code, Sec. 6253 (d) (1970).

[186]) Data Surveillance Bill, Sec. 1 (2) (e).

[187]) H.R. 16340, Sec. 32; S. 823, § 609 (2).

[188]) Spafford, Analysis of H.R. 16340, Credit-Hearings 1970, p. 145.

[189]) 15 U.S.C. § 1681 h (e).

[190]) § 372 N.Y. Gen.Bus.Law 1970.

[191]) Prosser, Right of Privacy, 48 Cal.L.Rev. 398; vgl. auch Kamlah, Right of Privacy, a. a. O., S. 143.

[192]) Karst, Legal Controls over Stored Personal Data, 31 L.a.C.P. 353 ff.; Miller, 1967 Atlantic, Nov. p. 55; ders., Senate Hearings, p. 77; ders. 67 Mich.L.Rev. 1214; Jacob, Privacy and the Law, 1969, L.a.C.T., Oct. p. 21; van Tassel, 1970, L.a.C.T., Jan. p. 7; Richard J. Miller, 68 Detamation, Sept. p. 55; Watson (IBM), Speech at the Commonwealth Club of California, Technology and Privacy, Apr. 5, 1968; Fatmi/Young, Habeas Scriptus, Workshop, Paper 7 und viele andere.

[193]) Karst, a. a. O., 31 L.a.C.P. 354; Miller, 67 Mich.L.Rev. 1114.

[194]) Karst, ebd.

[195]) Miller, 67 Mich.L.Rev. 1115.

[196]) Karst, ebd.

[197]) Karst, ebd., p. 354.

[198]) Miller, 67 Mich.L.Rev. 1115.

[199]) Miller, Statement, Credit-Hearings 1970, p. 189.

[200]) Miller, 67 Mich.L.Rev. 1116: „soft" data.

[201]) Karst, 31 L.a.C.P. 356.

[202]) Amendment 261 of S. 975, 5 U.S.C. § 552 a (6).

[203]) Karst, a. a. O., 31 L.a.C.P. 375; Cal.Gov.Code 1970, Sec. 6253 (b).

[204]) So z. B. ausdrücklich in Sec. 43, H.R. 16340; S. 975, § 552 a Sec. (a) (5) (1971); H.R. 854, Congressional Record, H. 2948 (1971, Apr.).

Streit über die Richtigkeit von Daten nicht bereinigt werden kann [205]). Eine Kreditauskunftei hat die Information als bestritten zu kennzeichnen und die Gegendarstellung künftigen Auskünften beizufügen [206]). Nach § 372 (3) b N. Y. Gen. Bus. Law 1970 ist auch früheren Empfängern eine berichtigte Auskunft zu übersenden, wenn eine Unrichtigkeit nachgewiesen ist.

Schließlich kann eine Eintragung so falsch sein, daß sie nicht berichtigt werden kann. Sie muß folglich gelöscht werden [207]). Dies gilt z. B. für eine Rechnung, die in einer Kreditauskunft als unbezahlt bezeichnet ist, während sie in Wahrheit nicht gestellt wurde oder bezahlt ist [208]).

c) Vom Berichtigungsanspruch ist der *Beseitigungsanspruch* im allgemeinen zu unterscheiden, der eingreift, wenn die Datenspeicherung als solche einen unzulässigen Eingriff in die Privatsphäre darstellt, ohne Rücksicht darauf, ob die gespeicherten Daten richtig oder falsch sind [209]). Wenn auch die einschlägigen Äußerungen spärlich sind, so ist doch die Forderung die notwendige Folge der angestrebten Verrechtlichung. Soll schon die Speicherung bestimmter Daten verboten sein [210]), muß der Betroffene auch einen Beseitigungsanspruch haben, wenn Daten über ihn unzulässig gespeichert wurden [211]). In den bisher vorliegenden Gesetzentwürfen findet sich dafür jedoch noch kein deutlicher Hinweis, obwohl der Wortlaut des Data Surveillance Bill 1969 eine entsprechende Auslegung zulassen würde [212]). Es kann jedoch auch sein, daß der hier behandelte Löschungsanspruch nicht deutlich genug unterschieden wird und daher unbeachtet blieb.

3. Protokollierungspflicht

a) Es hätte keinen Sinn, die Datenverwendung gesetzlich zu regeln, wenn die Durchsetzung der Vorschriften nicht nachprüfbar wäre. Daher wird von vielen Seiten vorgeschlagen, daß der Unternehmer einer Datenbank über die Datenverwendung Aufzeichnungen zu machen hat wie eine Bank über ein Kontokorrentkonto [213]). Dieser Vorschlag hat auch schon in Gesetzentwürfe Eingang gefunden [214]), die allerdings, soweit bekannt ist, noch nicht Gesetz geworden sind [215]).

Mit dem Fair Credit Reporting Act, der zunächst alle Aussichten hatte, in der Form des H. R. 16340 Gesetz zu werden, der dann doch in der weniger strengen Fassung des S. 823 Ende 1970 erlassen wurde [216]), haben wir jedoch ein Gesetz vor uns, das fern von aller Privacy-Utopie die Protokollierungspflicht verwirklicht, indem es verlangt, daß auf bis zu zwei Jahre zurück über erteilte Auskünfte dem Betroffenen auf Verlangen Mitteilung zu machen ist, was ja wohl irgendeine Form von Protokollierung der Datenverwendung voraussetzt [217]).

Die Vertreter der Kreditauskunfteien haben in den Hearings 1970 keine grundsätzlichen Einwände gegen die Protokollierungspflicht vorgetragen, vielmehr lediglich eine Beschränkung des Zeitraumes angeregt, während dessen Unterlagen über abgelaufene Auskunftszeiträume aufbewahrt werden müssen [218]). Dem ist der Gesetzgeber auch nachgekommen [219]).

b) Das Protokoll soll ermöglichen, für zurückliegende Zeiträume festzustellen, wer Daten eingespeichert bzw. entnommen hat. Es soll die Empfänger der Daten angeben und den Verwendungszweck [220]). Darüber hinaus dient das Protokoll dazu, die Funktionstüchtigkeit der technischen Sicherheitsvorrichtungen und die Zugriffsprogramme zu überwachen [221]). Wenn der Betroffene Bedenken hat, ob eine nach dem Protokoll erteilte Auskunft zulässig war, so kann er nach Einsicht des Protokolls auch ein Einschreiten der Registerbehörde verlangen [222]) oder bei Fehlen einer solchen auf dem Rechtsweg vorgehen [223]). Es ist jedoch u. U. sinnvoll, die Protokollierungspflicht auf ADV-Datenbanken zu beschränken, da sie nur mit Hilfe der

---

[205]) Sec. 43, H.R. 16340; § 611, S. 823.
[206]) Sec. 43, H.R. 16340; 15 U.S.C. § 1681 i (b) (1970).
[207]) Jacob, 1969 L.a.C.T., Oct. p. 21; van Tassel, 1970 L.a.C.T., Jan. p. 4.
[208]) Sec. 42, H.R. 16340.
[209]) Van Tassel, 1970 L.a.C.T., Jan. p. 7.
[210]) Note, 82 Harv.L.Rev. 413 und oben S. (8).
[211]) Vgl. Kingston Conference Summaries, Workshop Nr. 3: an injunction to restrain acts or situations alleged to injure the applicant.
[212]) Vgl. Sec. 5: „unfair"; ähnlich offen Sec. 7 (1), Control of Personal Information Bill 1971, der jedoch das Recht des Betroffenen auf Löschung auch nur über die Aufsichtsbehörde (Tribunal) gewähren würde.
[213]) Miller, 67 Mich.L.Rev. 1212: „log"; Karst, 31 L.a.C.P. 373; van Tassel, 1970 L.a.C.T., Jan. p. 7; Fatmi/Young, Workshop, Paper 7; Hunnings, Workshop, Paper 10; Westin, Privacy and Freedom, (1967) p. 324; Warner-Stone, a. a. O., p. 190; Baran, Communications, Computers and People, Senate-Hearings, p. 162.
[214]) Data Surveillance Bill 1969, Sec. 2 (2), Sec. 4 (2); Bill 182 (Reid-Bill, Ontario) Sec. 5 (2); Control of Personal Information Bill 1971, Sec. 6 (7) (a) (iii); Assembly Bill 1983 (1970) to amend Sec. 6253 Cal.Gov. Code, Sec. 6253 (c); S. 975 (1971), § 552 a (a) (3) „Freedom of Information Act"; H.R. 854 (1971) „Fed. Privacy Act".
[215]) H.R. 854 (1971) wird jedoch von 150 Kongreßabgeordneten unterstützt: Congressional Record, H. 2948 (1971, Apr.); H. 3108 (Apr. 27, 1971): 114 House Cosponsors.
[216]) Pub.L. 91—508 (1970), 15 U.S.C. § 1681 seq., § 1681 g (3).
[217]) § 1681 g (3) für allgemeine Auskünfte; allerdings nur 6 Monate für Kreditauskünfte. Demgegenüber verlangte Sec. 31 a des H.R. 16340 Protokollierung für fünf Jahre. Vgl. auch Data Surveillance Bill 1969, Sec. 2 (2) als Voraussetzung für Sec. 4 (2) (b) (c).
[218]) Credit Hearings 1970, Analysis of H.R. 16340 by Mr. Spafford, p. 145; ebd., Statement of Mr. Jordan, p. 160.
[219]) Vgl. 15 U.S.C. § 1681 g (3) mit H.R. 16340, Sec. 31 (a).
[220]) Jacob, 1969 L.a.C.T., Oct. p. 21; Data Surveillance Bill 1969, Sec. 2 (2); H.R. 854 (1971) Federal Privacy Act; S. 975 (1971) § 552 a (a) (3).
[221]) Miller, 67 Mich.L.Rev. 1212; Warner-Stone, a. a. O., p. 203, 204.
[222]) Data Surveillance Bill 1969, Sec. 5.
[223]) Cal.Gov.Code Sec. 6258.

ADV wirtschaftlich durchführbar ist [224]). Eine solche Beschränkung wurde bei den Credit-Hearing 70 nicht ins Auge gefaßt [225]), ist auch im Fair Credit Reporting Act nicht enthalten [226]).

c) Die Protokollierungspflicht ist auch in anderer Hinsicht Voraussetzung eines wirksamen Rechtsschutzes. Nur wenn die Empfänger von Daten bekannt sind, kann ihnen eine Berichtigung oder ein Widerruf zugesendet werden, was der Betroffene nach den Vorschlägen vieler verlangen kann [227]). Nach § 374 des „Credit data reporting act" [228]) ist dem Betroffenen regelmäßig auf dessen Verlangen ein Auszug aus dem Protokoll zu übersenden, dem er entnehmen kann, welche Personen und Stellen Daten über ihn empfangen haben.

d) Natürlich würde die Einführung einer Protokollierungspflicht etwas kosten [229]). Jedoch hat noch niemand erklärt, daß die Verwirklichung dieser Vorschläge am Kostenfaktor scheitern müßte. Es herrscht vielmehr die Überzeugung vor, daß man sich den Schutz der Privatsphäre etwas kosten lassen soll [230]). Die Auskunfteivertreter haben in den Credit-Hearings vor dem Sullivan-Committee 1970 nicht einmal den Versuch gemacht, die Durchführung der entsprechenden Vorschläge des H. R. 16340 für unmöglich zu erklären [231]). Sie sind zuversichtlich, die auf sie zukommenden Kosten auf die Kreditwirtschaft abwälzen zu können [232]). Wie schon oben ausgeführt, waren sie bestrebt — was ihr gutes Recht ist — durch ihre Stellungnahmen auf kostensenkende Maßnahmen hinzuwirken. Im übrigen sind lediglich gleiche Wettbewerbsbedingungen wesentlich [233]).

---

[224]) Vgl. aber Cal.Gov.Code (1970) § 6253 (c) Satz 2, (Assembly-Bill 1982), der nur eine Schonfrist für Computer vorsieht, aber die Protokollierungspflicht nicht auf Computerdatenbanken beschränkt, sondern nur die Registrierungspflicht (Sec. 6253 [d]).

[225]) Vgl. z. B. Jordan, Statement, Credit Hearings 70, p. 160.

[226]) 15 U.S.C. § 1681 g, 1681 a (g); ebensowenig im N.Y. credit data reporting act 1970, § 370 Gen.Bus.Law.

[227]) Data Surveillance Bill 1969, Sec. 5 (2): annullary order; Bill 182 (Reid-Bill, Ontario) Sec. 6 (2); Warner-Stone, a. a. O., p. 190; H.R. 16340 Sec. 31 (1), Sec. 42, Sec. 43; S. 823, § 611 (d); 15 U.S.C. § 1681 i (d).

[228]) N.Y. Gen.Bus.Law 1970

[229]) Warner-Stone, a. a. O., S. 203, 204.

[230]) Miller, Statement, Senate-Hearings, p. 77.

[231]) Spafford, Analysis of H. R. 16340, Sec. 31, Credit-Hearings 1970, p. 145; Jordan, TRW-Information Services, Inc., Statement, Credit-Hearings 70, p. 160.

[232]) Jordan, Statement, a. a. O., p. 160.

[233]) Vgl. Control of Personal Information Bill 1971, das in Sec. 6 (b) ausdrücklich darauf hinweist.

Schlußwort

Der Verfasser hat versucht, über die Fülle der Vorschläge zur Gesetzgebung, die sich in der angloamerikanischen Literatur und in Gesetzgebungsvorschlägen auffinden lassen, einen gedrängten Überblick zu geben. Es galt, einen für den Leser gangbaren Mittelweg zwischen Ausführlichkeit und Zusammenfassung zu finden. Der Leser durfte nicht in den Dschungel vieler Details geführt werden, was natürlich verlangte, auf die Darstellung mancher verwirrender Widersprüche zu verzichten, in die sich die Vorschläge untereinander zuweilen verstricken.

Die strafrechtliche Absicherung der gefundenen Regeln wurde nicht untersucht. Es sei nur darauf hingewiesen, daß der Erlaß von Strafvorschriften selbstverständlich auch erwogen wird [234]). Eine genaue Systematik der vorgeschlagenen Strafvorschriften konnte im Rahmen dieses Gutachtens nicht erarbeitet werden. Vielleicht findet sich eine berufenere Feder [235]).

Die Verletzung des right of privacy wird auch zivilrechtlich als unerlaubte Handlung angesehen. Daher werden einhellig Schadensersatzansprüche für den Betroffenen gefordert [236]). Die Verfasser müssen sich wenig Gedanken über die Schadensberechnung machen, da die amerikanischen Gerichte bei der Festsetzung der Schadenshöhe Phantasie nicht vermissen lassen. Die Lobby der Kreditauskunfteien hat jedoch erreicht, daß der Gesetzgeber die Schadenshöhe in bestimmten Fällen durch einen Schadensrahmen begrenzt hat [237]).

Der Verfasser ist schließlich nicht näher darauf eingegangen, wie der Betroffene jeweils seine Rechte durchsetzen kann. Nach allgemeiner Auffassung ist der Rechtsweg gegeben [238]), sofern er nicht aus besonderen Gründen ausdrücklich ausgeschlossen wurde. Letzteres ist wiederum bei den Kreditauskunfteien der Fall, wenn der Betroffene von einer Rechtsverletzung erfahren konnte, nachdem ihm die Auskunftei Einblick in sein Dossier gegeben hat [239]). Ob dieses Beispiel, das dem Schutz der Informanden gilt, nachahmenswert ist, soll hier offenbleiben. Da die Gerichtssysteme der USA

---

[234]) Vgl. Cal. Penal Code (1970), Sec. 631: strafbar das „Abhören" von Computersystemen, Entwendung fremder Daten durch Mißbrauch von Zugriffsmöglichkeiten. § 376 (3) N. Y. Gen. Bus. Law 1970, Erschleichen von Daten unter Vortäuschung einer Zugriffsberechtigung. Vgl. auch Kingston, Conference Summaries No. 8; Fatmi/Young, workshop, a. a. O.

[235]) Ein DAAD-Stipendiat soll zur Zeit an strafrechtlichen Problemen des Persönlichkeitsschutzes in den USA arbeiten. Von deutscher Seite: von zur Mühlen-Scholten, Computer Manipulationen aus strafrechtlicher Sicht, NJW 71, 1642; „Computer Kriminalität", Wirtschaftswoche 1971/37, 23 ff.

[236]) Privacy and the Law, a. a. O., p. 34 No. 136; Hunnings, workshop, a. a. O.; Karst, 31 L. a. C. P. 342 350; van Tassel, 1970 L. a. C. T., Jan. p. 7; Jacob, 1969 L. a. C. T., Okt. p. 21.

[237]) § 376 N. Y. Gen. Bus. Law 1970

[238]) § 6258 Cal. Gov. Code (1967), z. B.

[239]) § 372 (4) N. Y. Gen. Bus. Law 1970

und der Bundesrepublik Deutschland verschieden sind, erscheinen weitere rechtsvergleichende Untersuchungen in diesem Zusammenhang nicht als sinnvoll.

Wesentlich sind vor allem die einzelnen Schutzbestimmungen. Ehe diese nicht gefunden sind, ist es kaum notwendig, sich über ihre Durchsetzung den Kopf zu zerbrechen. Die Computerspezialisten beteuern, daß sie viel tun können, wenn ihnen nur endlich gesagt wird, was, wie und vor wem zu schützen ist. Sobald dies gesagt werden kann, werden sich auch rechtliche Sanktionen leichter finden lassen.

Anlage 3

Überlegungen zu technischen Möglichkeiten des Datenschutzes im Hinblick auf ein Bundesdatenschutzgesetz

Prof. Dr.-Ing. Karl Steinbuch
Dipl.-Ing. Herbert Wacker

Institut für Nachrichtenverarbeitung und -übertragung
Universität Karlsruhe

Januar 1972

Inhalt

0. Einleitung und Zusammenfassung

Dieses Gutachten entstand im Auftrag des Bundesministeriums des Innern. Es sollte die Frage untersucht werden, ob aus technischer Sicht Rahmen- oder Mindestbestimmungen über technische oder organisatorische Vorkehrungen in ein Bundesdatenschutzgesetz einfließen können.

Aufgrund der Komplexität des gesamten Problems kann jedoch keine vollständige und in alle Details gehende Darstellung erwartet werden.

Vorangestellt ist ein Abschnitt, der kurz auf den Hintergrund und die Schwierigkeiten eines Bundesdatenschutzgesetzes eingeht.

Nach der anschließenden Skizzierung der technischen Möglichkeiten und ihrer Grenzen werden wesentliche Kriterien zur Beurteilung vom Verfahren des Datenschutzes und denkbare technisch-organisatorische Forderungen in einem Datenschutzgesetz angegeben, die als Basis für intensivere Diskussionen und interfakultative Gespräche unter Fachleuten dienen sollen.

Ein weiterer Abschnitt diskutiert die Frage des Auskunftsrechts über eigene Daten und der Protokollierung von Zugriffen aus technischer Sicht.

Einige allgemeinere Bemerkungen, die sich zum Teil auf den vorliegenden Auszug des vorläufigen Referentenentwurfs eines Datenschutzgesetzes (im Anhang) [1]) beziehen, beschließen das Gutachten.

1. Hintergrund und Probleme eines Bundesdatenschutzgesetzes

Die Hauptanwendung der elektronischen Datenverarbeitung (EDV) war bisher durch die Erledigung von Massen- und Routinearbeiten gekennzeichnet. Inzwischen hat sich ein bedeutender Wandel angebahnt: Für die gegenwärtige und zukünftige Entwicklung ist der integrierte Einsatz der EDV für komplexe Anwendungsgebiete charakteristisch. Die wichtigsten dieser Anwendungsmöglichkeiten sind Dokumentationssysteme, Informationszentren für volkswirtschaftliche Daten, Gesetzgebung, Rechtsprechung, Statistik usw., weiterhin Management-Informationssysteme, Simulationsmodelle für das Aufstellen langfristiger Planungen. Schließlich findet sich auch bei der Verwirklichung solcher Planungen ein weites Anwendungsfeld für die Steuerung komplizierter Produktionssysteme oder komplexer Verwaltungsabläufe. Grundlagen solcher Systeme sind äußerst umfangreiche Datenbestände, die alle für den betreffenden Vorgang relevanten Daten enthalten und über die gegenwärtig als „Datenbanken" oder „Informationsbanken" so viel diskutiert wird.

Diese neuen Anwendungen bringen auch neue Probleme: Solche Datensammlungen bergen in sich die Gefahr, die schutzwürdige Privatsphäre — sowohl von Einzelpersonen als auch von Institutionen — beeinträchtigen zu können.

Diese Fragen erhalten ein besonderes Gewicht, wenn man an die Möglichkeit denkt, solche Informationsbanken zu informationellen Verbundnetzen zusammenzufassen, bei denen räumlich entfernte Benutzer über Terminals und Datenübertragungswege zu den verschiedenen Datenbeständen zugreifen können. In zunehmendem Maße wird daher die Forderung erhoben, alle Möglichkeiten des Datenschutzes auszuschöpfen, d. h. gesetzgeberische, organisatorische und technische Maßnahmen zu treffen, um den Schutz der Privatsphäre bei der EDV zu gewährleisten.

Die Forderung nach dem Schutz der Privatsphäre ist dabei keineswegs neu und schon gar nicht durch den Einsatz von Computern bedingt. In unserer Rechtsordnung gibt es seit langem eine Fülle von Rechtsvorschriften, die diesem Anliegen Rechnung tragen. Erinnert sei vor allem an das Grundgesetz, ferner gibt es im BGB, StGB und in Einzelgesetzen eine Reihe von Strafvorschriften, von Auskunftsverboten und Geheimhaltungsbestimmungen, z. B. Steuer- und Statistikgeheimnis. Doch in jüngster Zeit ist die öffentliche Diskussion um den Datenschutz wieder heftig in Gang gekommen. Anlaß hierzu waren vermutlich nicht zuletzt die Planungen zur Einführung eines Personenkennzeichens. Bundestag und Bundesregierung beschäftigen sich schon seit längerer Zeit mit dieser Problematik, beispielsweise wurden im zweiten EDV-Bericht der Bundesregierung, ferner in mehreren Kleinen Anfragen im Bundestag Fragen des Schutzes der Privatsphäre angesprochen.

Auf der Länderebene sind in Hessen, Bayern und Baden-Württemberg bereits Gesetze entstanden, die sich mit dem Schutz der Privatsphäre gegen Eingriffe beim Einsatz der EDV beschäftigen. In Rheinland-Pfalz befindet sich ein Gesetzentwurf im Stadium der Parlamentarischen Beratung (1).

Die Bundesregierung hat inzwischen mit den Vorbereitungen für den Entwurf eines Bundesgesetzes über den Datenschutz begonnen. Veranlassung hierzu gab nicht nur der rasante technologische Fortschritt, von dem eine besondere Bedrohung der Privatsphäre befürchtet wird. Auch die Aktivitäten auf dem Gebiet des Datenschutzes im Länderbereich, deren Zunahme zu einer Zersplitterung der Rechtslage für den Datenschutz in der Bundesrepublik führen kann, haben diese Initiative beeinflußt.

Die Schwierigkeiten beim Entwurf eines umfassenden Datenschutzgesetzes sind vor allem:

1. Es fehlen weitgehend Vorbilder; die bisher bekannten Gesetze — auch aus dem Ausland — regeln nur Teilaspekte.

[1]) *Anmerkung des Bundesministeriums des Innern*
Die wiedergegebene auszugsweise Fassung der §§ 4, 7, 8 und 9 des vorläufigen Referentenentwurfs entspricht nicht mehr dem derzeitigen Stand.

(1) s. Seite 224

2. Integrierte Verbundsysteme existieren bisher nur in Ansätzen; die Anforderungen an ein einschlägiges Gesetz sind in den Einzelheiten noch nicht vollständig überschaubar.
3. Wichtige Grundfragen, vor allem rechtlicher Art, sind noch ungeklärt; erinnert sei an die Kompetenzfragen zwischen Bund und Ländern, darüber hinaus ist auch nicht einzusehen, warum sich der Datenschutz nur auf EDV beschränken soll.

Diese wichtigen Hinweise lassen bereits die Komplexität der gesamten Problematik erkennen. Ziel dieses Gutachtens ist die Untersuchung eines Teilproblems dieses Komplexes, nämlich der Frage, ob in einem Bundesdatenschutzgesetz bereits Rahmen- oder Mindestbestimmungen über technische bzw. organisatorische Vorkehrungen festgelegt werden können bzw. sollen, oder ob man sich auf Allgemeinplätze beschränken muß, wie sie z. B. im Entwurf des Hessischen Datenschutzgesetzes nachzulesen sind (2): „§ 2 Die vom Datenschutz erfaßten Unterlagen, Daten und Ergebnisse sind so zu ermitteln, weiterzuleiten und aufzubewahren, daß sie nicht durch Unbefugte eingesehen, verändert, abgerufen oder vernichtet werden können. Dies ist durch geeignete personelle und technische Vorkehrungen sicherzustellen."

Ähnliche Formulierungen kennzeichnen auch andere Entwürfe.

Der nun folgende Teil steht unter der Geißel der oben skizzierten Schwierigkeiten. Insbesondere zwingen sie zu einem relativ hohen Abstraktionsgrad, um eine möglichst weitgehende Allgemeingültigkeit zu gewährleisten.

2. Allgemeine Problemstellung, technische Möglichkeiten und ihre Grenzen

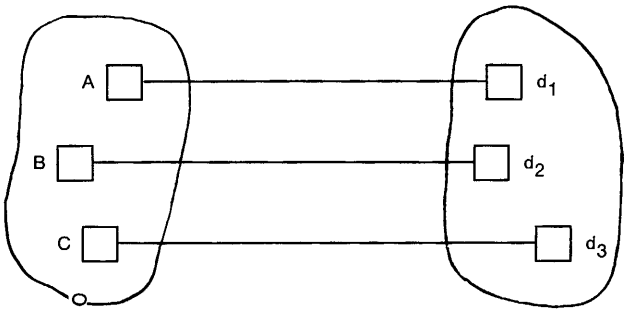
Unter „Datenschutz" versteht man zunächst den Schutz gegen unberechtigten Zugriff, er umfaßt auch alle Maßnahmen zum Schutz der Daten gegen Verfälschung, Mißbrauch oder Zerstörung durch Unbefugte. Dagegen gehören zur „Datensicherung" Maßnahmen gegen Verfälschung oder Zerstörung von Daten durch physikalische Fehlfunktionen, Bedienungsfehler oder höhere Gewalt bzw. Verfahren zur automatischen und schnellen Regenerierung von Daten, die auf diese Weise verfälscht oder zerstört worden sind.

Der Datenschutz ist zunächst ein rechtliches Problem: Es muß geklärt werden, wer, wann, wo, was eingeben, abfragen, ändern oder löschen darf (3). Die folgenden Ausführungen sind zunächst auf den Begriff „Zugriff" schlechthin beschränkt. Es sei jedoch betont, daß in der Praxis zumindest zwischen Lesezugriff und Schreibzugriff unterschieden werden muß. Trotz — bzw. gerade wegen — dieser Beschränkung werden die Prinzipien deutlich gemacht werden können.

Das Problem stellt sich mit dieser Vereinfachung so dar: Es gibt eine Menge von Daten und eine Menge von Benutzern. Jeder Benutzer A, B, C hat zu je einem Datenelement d_1, d_2, d_3 Zugriff (Bild 1).

Bild 1

Zugriffsberechtigung als Abbildung der Menge der Benutzer (-gruppen) auf die Menge der Daten (-gruppen)



Damit kann man, abstrakt betrachtet, die Zugriffsberechtigung als Abbildung der Menge der Benutzer auf die Menge der Daten auffassen. Dabei sei vermerkt, daß die einzelnen Datenelemente d_1, d_2 und d_3 auch Datengruppen darstellen können, ebenso wie die Benutzer A, B und C Benutzergruppen mit gleichen Zugriffsberechtigungen sein können. An diesem einfachen Beispiel ist die Abbildung sogar umkehrbar eindeutig und läßt sich in einer sehr einfachen Tabelle festhalten (Tabelle 1). Es sei nun vorausgesetzt, daß sowohl die Daten als auch die Zugriffsberechtigungstabelle in einem Computer gespeichert sind und daß die Benutzer über Datenstationen mit dem Computer verkehren.

Tabelle 1

Zugriffsberechtigungstabelle

Benutzer (-gruppe)	Daten (-gruppe)
A	d_1
B	d_2
C	d_3

Bereits an diesem Beispiel kann man erkennen, daß das Problem zunächst in zwei Teile zerfällt:

1. Benutzererkennung,
2. Überprüfung der Zugriffsberechtigung.

2.1. Benutzererkennung

Zur Benutzererkennung muß sich der Benutzer dem System ausweisen. Dies kann auf verschiedene Arten geschehen:

1. Durch etwas, was nur er weiß: also eine Losung, ein Kennwort oder einen Sicherheitscode.
2. Durch etwas, was nur er hat: Darunter fallen Schlüssel, Ausweis, Magnetschriftkarte, etwa im im Format einer Scheckkarte. Hierzu wären be-

(2), (3) s. Seite 224

sondere Vorrichtungen an den Datenstationen erforderlich.

3. Durch ein persönliches Merkmal: z. B. Unterschrift, Fingerabdruck, Körpergeruch oder Stimme. Da es bisher zur automatischen Erkennung solcher Merkmale keine wirtschaftlichen Verfahren gibt, scheidet diese Art der Erkennung vorläufig aus.
4. Vorprogrammiertes Frage- und Antwortspiel: Dies ist im Prinzip das gleiche, wie unter 1., nur daß der Benutzer mehrere Kennwörter wissen muß. Vom Aufwand her betrachtet, scheint es sinnvoll, dieses Frage- und Antwortspiel mit Daten zu treiben, die sowieso gespeichert sind; eine zusätzliche Aufnahme und Speicherung von Erkennungsdaten erübrigt sich dadurch weitgehend.
5. Zeitpunkt des Anrufes: D. h., daß ein bestimmter Benutzer nur zu einer bestimmten, festvorgegebenen Zeit anrufen darf (auch das gehört prinzipiell zu 1.).
6. Ort des Anrufes: Das läuft darauf hinaus, daß die Datenstation identifiziert wird. Dazu muß in der Datenstation ein automatischer Kennungsgeber eingebaut sein. Ferner muß sichergestellt sein, daß die Datenstation nur für legitimierte Benutzer zugänglich ist, was durch organisatorische und räumliche Maßnahmen sichergestellt werden müßte.

All diese Erkennungsverfahren haben einen entscheidenden Nachteil:

Sie bieten — auch bei fehlerfreier Funktion der technischen Einrichtungen — keine hundertprozentige Sicherheit. Betrachten wir die einzelnen Maßnahmen nochmals der Reihe nach:

Zu 1:

Wird das Kennwort einem anderen bekannt, so hat auch dieser Zugriff. Ein Kennwort läßt sich auch durch Blick über die Schulter eines gerade arbeitenden autorisierten Benutzers erfahren. Meist wird am Terminal ein Protokoll über den Ablauf der Arbeit geführt. Falls hierbei das Kennwort mit ausgegeben wird, kann auch ein unachtsam in den Papierkorb geworfenes Protokoll die Kennwortquelle für den nächsten Benutzer sein. Sofern man also mit Kennwörtern arbeitet, sollten Kennwörter auf der Datenstation nicht mitprotokolliert werden (siehe auch Abschnitt 4).

Zu 2:

Etwas, was man hat, kann man auch verlieren oder einmal verlegen. Der Finder hat dann ebenfalls Zugriff.

Zu 3:

Die Erkennung mit Hilfe eines persönlichen Merkmals wäre vermutlich das sicherste Verfahren, aber dazu gibt es, wie bereits erwähnt, bisher keine wirtschaftlichen Verfahren.

Zu 4 und 5:

Es ergeben sich ähnliche Nachteile wie bei 1, da auch dieses Verfahren darauf beruht, daß der Benutzer etwas weiß.

Zu 6:

Hier ist das Problem im wesentlichen auf organisatorische und räumliche Maßnahmen verlagert, auf die nur mit dem Hinweis eingegangen sei, daß auch sie nicht hundertprozentig sicher sind.

Die Sicherheit läßt sich natürlich erhöhen, wenn man diese hier aufgezählten Maßnahmen kombiniert. Z. B. schützt eine Kombination von 1 und 2 bereits weitgehend vor Mißbrauch bei Verlust der Magnetschriftkarte oder auch beim erwähnten Blick über die Schulter (dieses „Oder" ist freilich als Exklusiv-Oder zu verstehen).

Die zuweilen vorgeschlagene Erhöhung der Sicherheit durch periodischen Wechsel der Kennungen oder Karten kann bei Systemen mit wenigen Zugriffsberechtigten tragbar sein — für allgemeine (öffentliche) Informationsbankensysteme sollte man dies nur in Sonderfällen oder für Daten allerhöchsten Sicherheitsgrades (die man unter Umständen sowieso nicht in die Datenbanken einbringt) vorsehen.

Die so eingegebenen Ausweisungsinformationen müssen im Computer nun auf Zusammengehörigkeit und Übereinstimmung geprüft werden.

Um dies zu ermöglichen, muß im System eine Benutzererkennungstabelle gespeichert sein (Tabelle 2). Eine programmierte Erkennungsroutine vergleicht die eingegebenen Erkennungsdaten mit dieser Tabelle und nur wenn alle Daten übereinstimmen, gilt der Benutzer als ausgewiesen und erkannt.

Tabelle 2

Benutzererkennungstabelle

Benutzer (-gruppe)	Kennwort	Magnetkarten-Nr.
A	KW_A	MN_A
B	KW_B	MN_B
C	KW_C	MN_C

2.2. Überprüfung der Zugriffsberechtigung

Nun muß mit Hilfe der Zugriffsberechtigungstabelle und einem entsprechenden Prüfprogramm noch überprüft werden, ob dieser Benutzer zu den gewünschten Daten zugreifen darf und erst, wenn auch diese Prüfung positiv verlaufen ist, wird der eigentliche Zugriff ermöglicht (darin steckt implizit ein weiterer Schutz: Auch die Daten müssen unter Namen aufgerufen werden und dazu muß sie der Benutzer wiederum kennen).

Falls keine Zugriffsberechtigung vorliegt, wird die Anfrage abgewiesen. In diesem Falle muß jedoch der Versuch der Anfrage automatisch protokolliert

werden. Ein solches Protokoll wird zuweilen auch Logbestand genannt.

An dieser Stelle sind noch einige Bemerkungen zur Zugriffsberechtigung erforderlich. Es wurde bereits oben darauf hingewiesen, daß die in Bild 1 dargestellte umkehrbare eindeutige Abbildung eine Vereinfachung ist. Im allgemeinen werden sich die vielfältigen Zugriffsberechtigungen überschneiden, so daß auch lineare oder hierarchische Sicherheitsstufen nicht ausreichen. Ein Beispiel, das in modifizierter Form aus (4) entnommen wurde, soll dies verdeutlichen. Ein denkbarer Bestand einer Personaldatenbank könnte folgende Angaben enthalten:

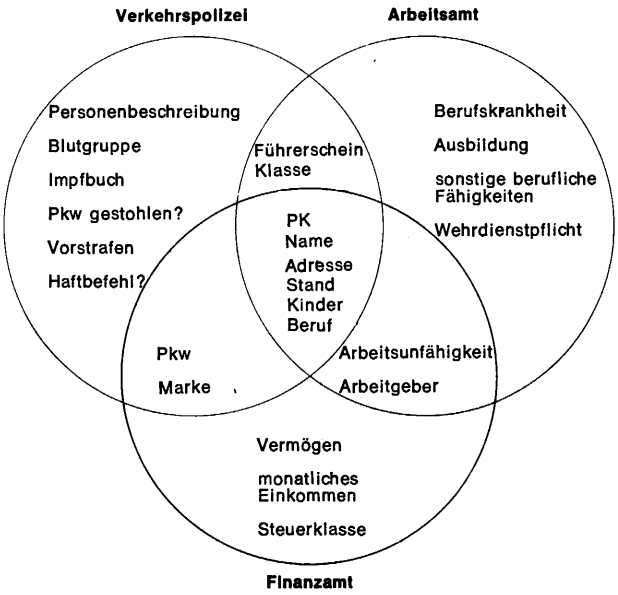
Personenkennzeichen,
Name,
Adresse,
Stand,
Kinder,
Beruf,
Berufskrankheit,
Ausbildung,
Sonstige berufliche Fähigkeiten,
Wehrdienstpflicht,
Arbeitgeber,
Arbeitsunfähigkeit,
Monatliches Einkommen,
Vermögen,
Steuerklasse,
Pkw,
Pkw gestohlen?
Marke,
Führerschein,
Klasse,
Personenbeschreibung,
Blutgruppe,
Impfbuch,
Vorstrafen,
Haftbefehl?

Diese Datei ist vielseitig verwendbar, so daß verschiedene Benutzergruppen auf bestimmte Teile Zugriff haben sollen. Als Beispiel seien die drei Benutzergruppen Verkehrspolizei, Arbeitsamt und Finanzamt betrachtet. Die Zugriffsberechtigung richtet sich nun danach, welche Daten zur Erfüllung der verschiedenen Aufgaben erforderlich sind und kann vielleicht so vorgenommen werden, wie Bild 2 zeigt. Man sieht hier, daß es Daten gibt, die nur einer einzigen Benutzergruppe zugänglich sein dürfen und Daten, auf die mehrere zugreifen dürfen. Man sieht hier auch, daß lineare Sicherheitsstufen — zum Beispiel vertraulich, geheim, streng geheim — nicht ausreichen. Der Sachbearbeiter der Verkehrspolizei erhält Informationen, die der Direktor des Arbeitsamtes — also ein Benutzer höherer Sicherheitsstufe — nicht erhält. In einem solchen Falle wird die Befugnistabelle entsprechend komplizierter, auch das betreffende Prüfprogramm muß aufwendiger sein. Anstelle einer Befugnistabelle wird man dann

(4) s. Seite 224

Bild 2

Mögliche Aufteilung der Zugriffsberechtigung für drei Benutzergruppen zu einer Personaldatenbank



eine Befugnismatrix verwenden, die für jeden Benutzer eine Zeile und für jedes Datenelement eine Spalte enthält. Steht auf dem Kreuzungspunkt eine Eins, so darf der Benutzer das Feld abfragen, steht dort eine Null, so wird eine Anfrage des Benutzers, die sich auf das gesperrte Feld bezieht, abgewiesen, und es erfolgt zusätzlich eine Eintragung im Logbestand.

Vermutlich bringt es in manchen Fällen bei der Realisierung gewisse Vorteile, wenn man von der direkten Abbildung der Benutzer (-gruppen) auf die Daten (-gruppen) abgeht und vielleicht Zwischenstufen einführt. Ein möglicher Weg wäre eine Unterteilung des Datenbestandes in Zugriffsberechtigungsklassen. Allgemein gilt, daß ein Datenbestand, zu dem N Benutzergruppen unterschiedliche Zugriffsberechtigung haben, in maximal $2^N - 1$ Zugriffsberechtigungsklassen eingeteilt werden kann.

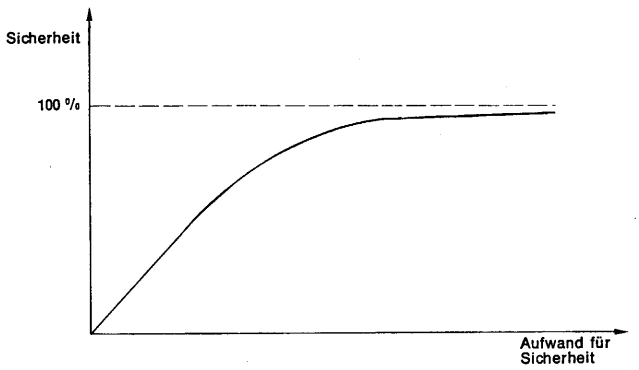
Eine weitere Komplikation ergibt sich durch die bereits erwähnte Unterteilung in Schreib- und Leseberechtigung. Noch komplizierter und komplexer wird dieser ganze Sachverhalt, wenn die Zugriffsberechtigung darüber hinaus vom Inhalt anderer Datenelemente abhängig ist.

Ungeachtet der Vielfalt der Befugnismöglichkeiten und Prüfalgorithmen bleibt das Prinzip, daß die Zugriffsberechtigung in irgendeiner Form im System gespeichert ist und durch entsprechende Programme überprüft wird. Damit ergibt sich das nächste Problem: Wer die Sicherheitstabellen und -programme kennt oder gar ändern kann, beherrscht das ganze System. Deshalb benötigen die Speicherplätze für Sicherheitstabellen und -programme den stärksten Schutz und die genauesten Prüfverfahren. Da auch dieser systemresident ist, bedürfte auch er wieder eines (noch genaueren) Schutzes.

Je vollkommener man den Schutz machen will, desto größer wird der Aufwand. Trägt man die angestrebte Sicherheit über den dafür erforderlichen Aufwand auf, so ergibt sich qualitativ etwa der Verlauf nach Bild 3. Für hundertprozentige Sicherheit müßte ein unermeßlicher Aufwand — nicht nur an technischen Einrichtungen — getrieben werden. Ganz deutlich gesagt: Hundertprozentige Sicherheit ist nicht möglich.

Bild 3

Die Sicherheit in Abhängigkeit vom dafür getriebenen Aufwand (qualitativer Verlauf)



3. Kriterien zur Beurteilung von Verfahren des Datenschutzes

Es stellt sich die Frage, nach welchen Kriterien man Verfahren des Datenschutzes beurteilen kann. Die wesentlich erscheinenden Kriterien sind hier angegeben:

1. Schutzwürdigkeit der Daten

   Ausgangspunkt für alle Überlegungen zu Verfahren des Datenschutzes muß die Festlegung der Schutzwürdigkeit der Daten sein.

   Dahinter verbirgt sich die Frage, welchen Schaden ein Mißbrauch zur Folge haben könnte. Je schutzbedürftiger die Daten sind, um so größer wird der Aufwand sein können (und müssen), der für die Technik des Datenschutzes getrieben wird. Konkrete Angaben in dieser Richtung gibt es jedoch noch nicht.

2. Sicherheit

   Hierin verbirgt sich vor allem die Frage: Wie schwierig ist es für einen Unbefugten (einen „Informatikverbrecher"), unerlaubten Zugriff zu bekommen? Diese Frage ist jedoch quantitativ nur schwer — wenn überhaupt — zu erfassen.

3. Adaptionsmöglichkeit und Flexibilität

   Das Sicherheitssystem muß sich den im Laufe der Zeit veränderlichen Bedürfnissen anpassen lassen, ohne daß dies mit zu großen Schwierigkeiten und mit zu hohem Aufwand verbunden ist. Veränderungen können z. B. notwendig werden, wenn sich ein Benutzer beim Eintippen seines Kennzeichens beobachtet fühlte. Es muß dann ein neues Kennzeichen vergeben werden.

4. Aufwand und Kosten

   Dieses Kriterium bezieht sich nicht nur auf die Hardware-Einrichtungen, z. B. für die Ausrüstung von Terminals mit Magnetkartenlesern oder für zusätzliche Speicher, sondern auch auf die Software, wobei neben der reinen Software-Erstellung auch ihr Einfluß auf die Systembelastung durch die Laufzeit der Sicherheitsroutinen zu beachten sind.

   Weiterhin bringen organisatorische und personelle Maßnahmen meist eine Kostensteigerung mit sich.

5. Benutzerfreundlichkeit

   Für den Benutzer stellen die Schutzmaßnahmen eine gewisse Belastung dar, die in erträglichen Grenzen gehalten werden sollte. Sie dürfen nicht zu schwierig oder zu umständlich sein.

Bei all diesen Kriterien muß man die Frage einbeziehen, ob das Kriterium in einem angemessenen Verhältnis zur Schutzwürdigkeit der Daten steht. Es müßte allerdings noch präzisiert werden, was in konkreten Fällen als „angemessen" betrachtet werden kann und was nicht.

4. Denkbare technisch-organisatorische Forderungen in einem Datenschutzgesetz

Im folgenden werden einige technisch-organisatorische Forderungen zur Diskussion gestellt, die vermutlich ein hohes Maß an Sicherheit bei vertretbarem Aufwand bieten. Diese Forderungen sind grob formuliert und bedürfen sicherlich weiterer Differenzierungen und Ergänzungen. Sie mögen als Basis für intensivere Diskussionen und interfakultative Gespräche unter Fachleuten dienen.

1. Datenbanken mit öffentlichem Zugriff, die Daten enthalten, die über den Kreis der Zugriffsberechtigten hinaus nicht bekannt werden dürfen, müssen im closed-shop-Betrieb arbeiten, d. h. nur autorisiertes Bedienungspersonal soll zum eigentlichen Maschinenraum Zutritt haben. So wird gewährleistet, daß nur ein beschränkter Personenkreis direkt mit dem Computer arbeiten kann.

2. Die Auslösung bestimmter Funktionen oder Befehle von den anschaltbaren Datenstationen muß — auch für Spezialisten — unmöglich sein.

   Insbesondere muß dadurch ein Zugriff auf Daten und Programme verhindert werden, die zu den Schutzroutinen gehören. Diese Blockierung von Funktionen ließe sich evtl. auch hardware-mäßig realisieren. Sicherheitsschlüssel dürfen an der Datenstation nicht mit protokolliert werden.

3. Alle Tätigkeiten, die das Schutzsystem betreffen, müssen — selbstverständlich innerhalb des closed-shop — protokolliert werden. Insbesondere muß jeder Versuch, die Sicherheitsvorkehrungen zu verletzen, erkannt und besonders aus-

führlich protokolliert werden. Bei wiederholtem Versuch ist das betreffende Terminal zu sperren oder die Leitungsverbindung abzubrechen.

4. Die Schutzvorkehrungen müssen bei der Installation gründlich ausgetestet und ferner fortlaufend durch regelmäßige, jedoch in unregelmäßigen Abständen erfolgende Tests überwacht werden, z. B. durch bewußten und fachkundigen Versuch, die Schutzvorkehrungen vom Terminal aus zu durchbrechen.
5. In einer Datenbank ist ein Sicherheitsbeauftragter einzusetzen, der für die Einhaltung der Sicherheit verantwortlich ist. Daß ein solcher Sicherheitsbeauftragter Computerfachmann sein sollte, sei ausdrücklich betont. Aufgabenbereich und vor allem Verantwortungsbereich des Sicherheitsbeauftragten bedürfen jedoch noch einer näheren Analyse — eine sicherlich sehr schwierige Aufgabe.

5. Zur Frage des Auskunftsrechts über eigene Daten und der Protokollierung von Zugriffen

In einem Datenschutzgesetz sollte für jedes Individuum, gemeint sind natürliche Personen, juristische Personen, Institutionen usw., das Recht verankert sein, eine Berichtigung verlangen zu können, wenn unrichtige, unvollständige oder veraltete Daten über es gespeichert werden. Voraussetzung dafür ist das Recht, diese Daten einsehen zu können. Es scheint sinnvoll, daß jedes Individuum zunächst ohne sein Zutun und kostenlos einen Ausdruck der bei der Erfassung eingespeicherten Daten erhält. Darüber hinaus sollte jedes Individuum das Recht haben, jederzeit auf Antrag (ggf. unter Bezahlung einer Gebühr) einen solchen Ausdruck verlangen zu können. (Eine derartige Regelung war in der „DATA SURVEILLANCE BILL" vorgesehen). (9)

Diese Rechte sollten sich aus technischer Sicht vorwiegend auf den aktuellen Stand beschränken.

Zuweilen wird weiterhin gefordert, daß neben dem gegenwärtigen Stand der Information auch der Stand bei der Einspeicherung, ferner alle Weitergaben und Veränderungen samt Ort, Zeitpunkt und Empfänger sowie der jeweilige Stand festgehalten und zur Auskunft bereitstehen sollen. Diese Forderung ist aus technischer Sicht unrealistisch, da hierzu ein ungeheuerer Aufwand — zunächst für die Protokollierung aber auch für die gezielte Wiedergewinnung der Protokolle — getrieben werden müßte.

Für die Protokollierung der gesamten Zugriffshistorie von Datensätzen über größere Zeiträume läßt sich der Nettospeicherbedarf nach folgender Gleichung abschätzen:

$$S_P = Z \cdot L_P \cdot G \cdot t$$

Dabei bedeuten die einzelnen Größen

S_P zu erwartender Netto-Speicherbedarf für **P**rotokolle (z. B. in Bytes)

Z mittlere Anzahl der **Z**ugriffe pro Datensatz in einem Zeitintervall (z. B. pro Jahr)

L_P mittlere **L**änge eines **P**rotokollsatzes (z. B. in Bytes)

G Anzahl der betrachteten **G**runddatensätze

t betrachtete Zeitintervalle (z. B. Jahre)

Ohne Speicherung der Historie ergibt sich

$$S_G = L_G \cdot G$$

mit

S_G Netto-**S**peicherbedarf für die **G**runddatensätze

L_G mittlere **L**änge der **G**runddatensätze.

Der Quotient

$$\frac{S_P}{S_G} = \frac{Z \cdot L_P \cdot t}{L_G}$$

gibt an, um welchen Faktor der Nettospeicheraufwand zur Protokollierung aller Zugriffe größer ist, als der Nettospeicheraufwand ohne Protokollierung.

Anhand einer groben Überschlagsrechnung soll nun gezeigt werden, zu welchen absoluten Zahlen dies führt. Diese Überschlagsrechnung basiert auf Schätzungen über den Arbeitsanfall im Einwohnerwesen aus der „Analyse zum Datenvolumen und Datenverkehr" für das Bayerische Informationssystem, siehe (7). Tabelle 3 zeigt in zusammengefaßter

Tabelle 3

Übersicht über den Arbeitsanfall im Einwohnerwesen, zusammengefaßte Darstellung aus (7).

Anzahl je 1000 Einwohner und Jahr

Aufgabenbereiche	Zugriffe		z. B. protokollpflichtig
	direkt	seriell	
Natürliche Bevölkerungsbewegung (Geburten und Sterbefälle)	213		213
Wanderungsbewegung (Zu-, Fort- und Umzüge)	345		345
Eheschließung/Ehescheidung	46		46
Ausweise	500		—
Vorbereitung von Wahlunterlagen		725	—
Lohnsteuerkarten	100	750	—
Pflichtimpfungen	31	62	93
Wehrerfassung		15	15
Einzelauskünfte	500		500
Planungen		4 000	—
Gesamt (gerundet)	1 750	5 600	1 212
	7 350		

(7), (9) s. Seite 224

Form die geschätzte Anzahl von Zugriffen für verschiedene Aufgabenbereiche im Einwohnerwesen pro 1000 Einwohner und Jahr, vgl. auch (8). Auf die Bedeutung der letzten Spalte wird später eingegangen. Es sei an dieser Stelle ausdrücklich betont, daß diese Angaben nur einen *Teilbereich der öffentlichen Verwaltung* betreffen. Nicht berücksichtigt ist z. B. der Datenaustausch mit Arbeitsämtern, Kirchen, Rentenversicherungen, Finanzämtern, Kraftverkehrsämtern, Versicherungen usw.

In der genannten Analyse wird damit gerechnet, daß eine sinnvolle, vorläufige Festlegung des Einwohnerdatensatzes zu einer variablen Datensatzlänge von durchschnittlich 250 Bytes führt; es wird jedoch darauf hingewiesen, daß es bereits Zusammenstellungen gibt, die zu ca. 2000 Bytes maximal und ca. 600 Bytes im Durchschnitt führen.

Die folgende Rechnung geht von diesen Annahmen aus:

1. Grunddatensatzlänge: 250 Bytes.
2. Protokolle werden laufend für *jeden* Zugriff geführt.
3. Zur Wiederaufführung der Protokolle.
   3.1. Ein Feld des Grunddatensatzes beinhaltet einen Zeiger, der auf den jeweils jüngsten Protokollsatz zu dem betreffenden Grunddatensatz verweist.
   3.2. Ein Feld des Protokollsatzes verweist auf den letzten vorangegangenen Protokollsatz.

   Damit ist es möglich, ausgehend vom aktuellen Datensatz in chronologischer Reihenfolge (rückwärts) alle Protokolle wieder zu finden.
4. Der Protokollsatz müßte etwa folgende Angaben enthalten:

   Person oder Institution, die zugreift,

   Zeitpunkt und/oder Ort des Zugriffs,

   Spezifizierung über die Art des Zugriffs,
   bei Anfragen: weitergegebene Daten,
   bei Änderungen: Stand vor der Änderung und Änderung selbst,

   Verweis auf vorheriges Protokoll (s. a. 3.2.).

   Damit dürfte der Protokollsatz im Mittel etwa ebenso lang sein wie der Grunddatensatz; hier wird eine Länge von 250 Bytes angenommen. Die kurzlebigeren Protokolle, die zur System*sicherung* erforderlich sind, werden hier nicht berücksichtigt.
5. Nach Tabelle 3 beträgt die Gesamtzahl der Zugriffe ca. 7350 pro 1000 Einwohner und Jahr; hier wird vereinfacht mit 7 jährlichen Zugriffen pro Datensatz gerechnet.

Tabelle 4 zeigt für 1000, 0,5 Millionen und 60 Millionen Einwohnerdatensätze den Nettospeicher-

Tabelle 4

Zusammenfassung der Überschlagsrechnung für den Speicheraufwand ohne und mit Protokollierung von Zugriffen
(Erläuterungen und zugrunde liegende Annahmen siehe Text)

Anzahl der Einwohnerdatensätze	Zeitraum in Jahren	Nettospeicherbedarf ohne Protokollierung in Bytes	Zahl der Zugriffe = Zahl der Protokollsätze	Nettospeicherbedarf für Protokollierung aller Zugriffe in Bytes (250 Byte/Zugriff)	Anzahl benötigter Bänder (gerundet) für Protokolle bei Blockungsfaktor		
					1	10	100
1 000	1	$2{,}5 \cdot 10^5$	$7 \cdot 10^3$	$1{,}75 \cdot 10^6$	1	1	1
	5	$2{,}5 \cdot 10^5$	$3{,}5 \cdot 10^4$	$8{,}75 \cdot 10^6$	1	1	1
	10	$2{,}5 \cdot 10^5$	$7 \cdot 10^4$	$1{,}75 \cdot 10^7$	2	1	1
	50	$2{,}5 \cdot 10^5$	$3{,}5 \cdot 10^5$	$8{,}75 \cdot 10^7$	10	3	2
0,5 Millionen	1	$1{,}25 \cdot 10^8$	$3{,}5 \cdot 10^6$	$8{,}75 \cdot 10^8$	$9{,}1 \cdot 10^1$	$2{,}6 \cdot 10^1$	$2 \cdot 10^1$
	5	$1{,}25 \cdot 10^8$	$1{,}75 \cdot 10^7$	$4{,}37 \cdot 10^9$	$4{,}6 \cdot 10^2$	$1{,}3 \cdot 10^2$	$1 \cdot 10^2$
	10	$1{,}25 \cdot 10^8$	$3{,}5 \cdot 10^7$	$8{,}75 \cdot 10^9$	$9{,}1 \cdot 10^2$	$2{,}6 \cdot 10^2$	$2 \cdot 10^2$
	50	$1{,}25 \cdot 10^8$	$1{,}75 \cdot 10^8$	$4{,}37 \cdot 10^{10}$	$4{,}6 \cdot 10^3$	$1{,}3 \cdot 10^3$	$1 \cdot 10^3$
60 Millionen	1	$1{,}5 \cdot 10^{10}$	$4{,}2 \cdot 10^8$	$1{,}05 \cdot 10^{11}$	$1{,}1 \cdot 10^4$	$3{,}2 \cdot 10^3$	$2{,}4 \cdot 10^3$
	5	$1{,}5 \cdot 10^{10}$	$2{,}1 \cdot 10^9$	$5{,}25 \cdot 10^{11}$	$5{,}5 \cdot 10^4$	$1{,}6 \cdot 10^4$	$1{,}2 \cdot 10^4$
	10	$1{,}5 \cdot 10^{10}$	$4{,}2 \cdot 10^9$	$1{,}05 \cdot 10^{12}$	$1{,}1 \cdot 10^5$	$3{,}2 \cdot 10^4$	$2{,}4 \cdot 10^4$
	50	$1{,}5 \cdot 10^{10}$	$2{,}1 \cdot 10^{10}$	$5{,}25 \cdot 10^{12}$	$5{,}5 \cdot 10^5$	$1{,}6 \cdot 10^5$	$1{,}2 \cdot 10^5$

(8) s. Seite 224

bedarf ohne und mit Protokollierung von Zugriffen über verschiedene Zeiträume. Für den Fall, daß die Protokolle auf Band geführt werden, ist in den letzten Spalten der Tabelle 4 die ungefähre Anzahl der benötigten Bänder bei verschiedenen Blockungsfaktoren angegeben. Der Blockungsfaktor gibt an, wie viele Protokolldatensätze zu einem Datensatz zusammengefaßt werden. (Bei Magnetbändern können nur ganze Blöcke pro Zugriff gelesen bzw. geschrieben werden. Zwischen den Blöcken befinden sich auf dem Band unbeschriebene Blocklücken von ca. 1,5 cm; diese werden zum Beschleunigen und Abbremsen des Bandes benötigt. Werden mehrere Sätze zu einem Block zusammengefaßt, so sind weniger Blocklücken erforderlich, womit man eine höhere Kapazitätsausnutzung des Bandes erzielt. Diesem Vorteil steht der Nachteil gegenüber, daß die Blockung größere Arbeitsspeicherbereiche als Ein/Ausgabepuffer erfordert.)

Der Berechnung der Anzahl benötigter Bänder liegen folgende Annahmen zugrunde

Bandlänge 730 m,

Schreibdichte 1 600 BPI (Bytes per inch) entspricht 630 Bytes/cm,

Blocklücke 1,5 cm.

Damit errechnen sich die Anzahl der Sätze pro Band bei verschiedenen Blockungsfaktoren und einer Satzlänge von 250 Bytes nach Tabelle 5.

Tabelle 5

Blockungsfaktor	Anzahl der Sätze pro Band
1	$3{,}84 \cdot 10^4$
10	$1{,}33 \cdot 10^5$
100	$1{,}76 \cdot 10^5$

Rechenzentren für 0,5 Millionen Einwohner

Geht man in Anlehnung an das Bayerische Informationssystem davon aus, daß pro 0,5 Millionen Einwohner ein Rechenzentrum errichtet wird, so entfallen auf jedes Rechenzentrum nach 50 Jahren zwischen ca. 4600 und ca. 1000 Protokollbänder (Tabelle 4).

Um über diese Zeit eine Zusammenstellung aller Zugriffsprotokolle eines Datensatzes zu bekommmen, so müßte in ungünstigsten Fällen auf bis zu 350 Bänder zugegriffen werden. Legt man pro Bandzugriff eine Dauer von nur 5 Minuten zugrunde, so dauert die ganze Recherche ca. 30 Stunden.

Wollte man die Protokolldaten von 50 Jahren gar im Direktzugriff halten, so wären beim derzeitigen Stand der Technik ca. 190 Magnetplattenspeicher mit einem jährlichen Mietpreis von ca. 57 Millionen DM bzw. ca. 83 Magnetkartenspeicher mit einem jährlichen Mietpreis von 12,5 Millionen DM erforderlich. (Annahme: Magnetplattenspeicher: Kapazität ca. 240 Millionen Bytes, Kosten ca. 300 000 DM im Jahr; Magnetkartenspeicher: Kapazität etwa 530 Millionen Bytes, Kosten etwa 150 000 DM im Jahr).

Konsequenzen

Wenngleich die zur Verfügung gestandenen Angaben nicht generell als repräsentativ gelten, so zeigt diese Übersicht doch deutlich, zu welchen Dimensionen an Speicherbedarf voreilige Protokollierungsforderungen führen. Daher sollte sich das Auskunftsrecht in der Regel auf den aktuellen Bestand beziehen. Nur für ganz besonders wichtige Daten (welche?) sollte langfristige Protokollierung der Zugriffe vorgesehen werden.

Sind z. B. nur die in der letzten Spalte von Tabelle 3 angegebenen Zugriffe protokollpflichtig, so wird der Speicherplatzbedarf für die Protokollierung auf etwa $^1/_6$ reduziert.

Schließlich sollten so viel Zugriffe wie möglich öffentlich — d. h. ohne Identifikation und vor allem ohne Protokollierung — erlaubt sein; dies gilt insbesondere für Adreß- oder Telefonbuchdaten sowie in der Regel für aglomerierte Daten.

Auf die Möglichkeit einer „indirekten Protokollierung" wird im Abschnitt 6 hingewiesen.

6. Abschließende Bemerkungen

Jedes technische Verfahren, mag es auch noch so aufwendig sein, kann von denjenigen, wenigen Leuten, die das System genau kennen und an ihm arbeiten, umgangen werden. Durch die Tatsache, daß bestimmte Computerfunktionen über Terminals nicht ausgelöst werden können, wird der Kreis derer, die potentiell „Informationsmißbrauch" treiben, schon sehr weit eingeschränkt. Der Spezialist hat jedoch innerhalb des closed-shop-Betriebes die Möglichkeit, diese Schranken zu durchbrechen. Er weiß ja, wie er einen Speicherabzug der Befugnistabellen erzeugt, er kann diese Liste weitergeben und somit unter Umständen Unbefugten den „Sesam öffne Dich" zukommen lassen. Besonders problematisch wird dies z. B., wenn er am System Veränderungen vornimmt, die die Blockierung der Terminals für bestimmte Funktionen aufheben. Man muß sich darüber im klaren sein: EDV kann im Dienst des Datenschutzes äußerst wirksam sein, doch Menschen beherrschen den Computer — und die Variable Mensch ist nicht programmierbar. Hier muß die Rechtsordnung eingreifen. Zur Wahrung von Berufsgeheimnissen unter Strafandrohung sind bisher u. a. verpflichtet: Beamte, Ärzte, Zahnärzte, Anwälte, Notare sowie ihre Hilfspersonen. Man wird künftig auch EDV-Spezialisten, die an schutzbedürftigen Datenbanken arbeiten, in diesen Kreis aufnehmen müssen, vgl. (5).

Man darf sich jedoch auch über die technischen Schutzmaßnahmen keine Illusionen machen: Gelegentliche Fehlfunktionen haben Automat und Mensch gemein. Durch eine Computerfehlfunktion kann der Fall eintreten, daß ein Benutzer ungewollt Informationen erhält, die außerhalb seiner Zugriffsberechtigung liegen. Es ist zu prüfen, ob und inwieweit man solche Fälle in einem Datenschutzgesetz

(5) s. Seite 224

berücksichtigen sollte, in dem man die Nutzung oder Weitergabe solchermaßen erhaltener Informationen ausdrücklich unter Strafe stellt.

Ein Punkt der bekanntgewordenen Gesetze und Gesetzentwürfe verdient besondere Beachtung. Im Entwurf des Bundesmeldegesetzes (1), im Gesetz über die Organisation der elektronischen Datenverarbeitung im Freistaat Bayern (6) heißt es in den Abschnitten, die die Strafvorschriften für Datenmißbrauch regeln, daß die Tat nur auf Antrag des Verletzten verfolgt wird. Diese Einschränkung erscheint problematisch: Es gibt noch keine präzisen Prognosen über die Auswirkungen des Einsatzes solch potenter Medien der Informationsbereitstellung auf die Gesellschaft. Es ist jedoch nicht auszuschließen, daß künftig der Informationsmißbrauch schlimmere Folgen haben könnte, als beispielsweise Eigentumsdelikte der Gegenwart. Die Weichen der Gesetzgebung sollten jedoch bereits jetzt unter diesem Aspekt gestellt werden. Das Grundgesetz verpflichtet alle staatliche Gewalt, die Menschenwürde zu achten und zu schützen. Wenn unbefugter Eingriff in Daten der Privatsphäre des einzelnen eine Verletzung seiner Menschenwürde bedeuten kann, dann sollte jeder, wie auch immer bekanntgewordene Datenmißbrauch verfolgt werden. Zumindestens sollte festgelegt sein, daß die Betroffenen über bekanntgewordenen unerlaubten Zugriff zu ihren Daten unterrichtet werden.

Im Anhang ist der vorläufige Text des § 4 Abs. 3 des Referentenentwurfes eines Bundesdatenschutzgesetzes wiedergegeben, in dem die Ermächtigung zum Erlaß einer Rechtsverordnung zu technischen und organisatorischen Datenschutzmaßnahmen geregelt wird; ferner sind die vorläufigen Fassungen der Abschnitte angegeben, auf die der § 4 Abs. 3 unmittelbar bzw. mittelbar Bezug nimmt.

Aus technischer Sicht sind gegen diesen Entwurf keine grundsätzlichen Einwände zu erheben.

Zu den einzelnen Abschnitten seien einige kritische Hinweise gegeben:

Zu § 4 Abs. 3

Warum beschränkt sich dieser Abschnitt ausdrücklich auf Individualinformationen? Im Hinblick auf die zu erwartenden Informationsbankensysteme, z. B. das allgemeine, arbeitsteilige Informationsbankensystem für die Bundesrepublik Deutschland, die zu einer allgemeinen Verbesserung der Informationsmöglichkeiten führen sollen, erscheint diese Einschränkung problematisch: Ein umfassendes Bundesdatenschutzgesetz sollte auch auf Zerstörung, Verlust oder Entstellung nicht personenbezogener Informationen eingehen. Beispielsweise könnte doch die Entstellung anonymisierter Wirtschaftsstatistiken enorm schädliche wirtschaftliche Folgen haben.

Der Abschnitt gebietet Rücksichtnahme auf ein „angemessenes" Verhältnis zwischen der Wirksamkeit der Vorkehrungen zugunsten des Datenschutzes und den durch ihre Einführung und Unterhaltung entstehenden Kosten. Im Abschnitt 3 dieses Gutachtens wurde bereits darauf hingewiesen, daß der Begriff des „angemessenen" Verhältnisses weiterer Präzisierung bedarf. Man wird jedoch erst aus zukünftigen Erfahrungen in der Praxis lernen müssen, diesen Begriff konkret zu präzisieren, was dann in der Rechtsverordnung seinen Niederschlag finden sollte.

Zu § 7 Abs. 3, § 8 Abs. 2 und Abs. 3

In Abschnitt 5 dieses Gutachtens wird die Frage der Protokollierung von Zugriffen aus technischer Sicht ausführlich diskutiert. Da die Anforderungen an das Bundesdatenschutzgesetz heute noch nicht in allen Einzelheiten überschaubar ist, sollte — ebenfalls aus technischer Sicht — vorgesehen werden, das Spektrum der nicht protokollierungspflichtigen Informationsweitergabe flexibler zu halten. Dies scheint insbesondere notwendig, wenn man die Beschränkung des § 4 Abs. 3 auf Individualinformationen aufhebt. Es wäre denkbar, den § 8 Abs. 2 durch einen Punkt 6 zu ergänzen, z. B.:

„6. Weitere Informationen, die in der Rechtsverordnung nach § 4 Abs. 3 festgelegt werden können."

Daraus resultierte eine Möglichkeit zur weitgehenden flexiblen Anpassung an die sich im Laufe der Zeit verändernden Bedürfnisse. Diesem Vorteil der Flexibilität steht jedoch der Nachteil gegenüber, daß die Transparenz des Gesetzes leidet, da die für den Bürger u. U. sehr wichtigen Bestimmungen aus dem Gesetz in die Rechtsverordnung verlagert werden.

Aus Tabelle 3 ist zu entnehmen, daß die Mehrzahl der Zugriffe auf routinemäßigen Arbeiten beruht (die auch meist seriell durchgeführt werden). Zur Vorbereitung von Wahlunterlagen wird beispielsweise auf die Datensätze von all denjenigen Einwohnern zugegriffen, die das Wahlalter erreicht haben. In solchen Fällen sollte man aus Gründen des Speicherbedarfs von der direkten Protokollierung abgehen und eine *„indirekte Protokollierung"* einführen: Anstatt zu jedem Grunddatensatz einen eigenen Protokollsatz zu erstellen, genügt die Dokumentation der Tatsache, daß auf alle Datensätze mit dem Merkmal „Alter größer oder gleich Wahlalter" (= Zugriffs-Kriterium) zugegriffen wurde und daß bestimmte Informationen an den betreffenden Empfänger weitergegeben wurden.

Zur Dokumentation der vielfältigen routinemäßigen Zugriffe läßt sich eine „Routine-Zugriffs-Datei" erstellen, die für jeden Routine-Zugriff etwa folgende Angaben enthält:

laufende Nummer des Routine-Zugriffs,
Institution, die zugreift,
Zeitpunkt und/oder Ort des Zugriffs,
Zugriffskriterium,
weitergegebene Informationen.

Um, ausgehend von einem bestimmten Grunddatensatz, alle Weitergaben festzustellen, muß die gesamte Routine-Zugriffs-Datei durchgekämmt werden, wobei für jeden Routine-Zugriff überprüft wird, ob das Zugriffskriterium auf den betreffenden Grunddatensatz zutrifft.

Es erscheint sinnvoll, daß § 7 Abs. 3 Satz 3 ausdrücklich auf diese Möglichkeit eingeht: Auf diese Weise wird der Protokollierungsaufwand sehr stark reduziert ohne jedoch die grundsätzliche Protokollierung aufzugeben.

(1), (6) s. Seite 224

7. Literaturhinweise

(1) Personenkennzeichen, Meldewesen, Datenverarbeitung, Datenschutz. Veröffentlichung der Reihe „betrifft". Herausgegeben vom Bundesministerium des Innern Bonn 1971.

(2) Großer Hessenplan, Entwicklungsprogramm für den Aufbau der Datenverarbeitung in Hessen, Hessische Zentrale für Datenverarbeitung, Wiesbaden 1970.

(3) Steinbuch, K.; Wacker, H.: Gutachten über „Technische Konzeptionen und technische Wegeplanung für ein allgemeines arbeitsteiliges Informationsbankensystem für die Bundesrepublik Deutschland". Institut für Nachrichtenverarbeitung und -übertragung, Universität Karlsruhe, März 1971.

(4) Schulze, J.-H.: Datenschutz in der Datenverarbeitung. IBM-Nachrichten, 21 (1971) 205, S. 640 bis 645.

(5) Kaufmann, O. K.: Der registrierte Mensch. Vortrag gehalten bei der UNIVAC Herbsttagung 1970 in Zürich.

(6) Gesetz über die Organisation der elektronischen Datenverarbeitung im Freistaat Bayern (EDVG) vom 12. Oktober 1970, in: Bayerisches Gesetz- und Verordnungsblatt Nr. 22 vom 16. Oktober 1970.

(7) Angermann, A.; Crusen, W. G.; Schmidt, W.: Analyse zum Datenvolumen und Datenverkehr, Beiträge zur integrierten Datenverarbeitung in der öffentlichen Verwaltung Bayerns, Heft 2. Hrsg.: Siemens AG/Unternehmensbereich Datentechnik 1970.

(8) Einsele, T.; Knöpfle, R.: Gutachten über „Technische Möglichkeiten und Überlegungen zur Realisierung eines allgemeinen arbeitsteiligen Informationsbankensystems für die Bundesrepublik Deutschland", Institut für Datenverarbeitung, Technische Universität München, März 1971.

(9) Niblett, G. B. F.: Digital information and the privacy problem. OECD Informatics Studies, OECD Paris, 1971.

8. Anhang: Auszug aus dem vorläufigen Referentenentwurf eines Bundesdatenschutzgesetzes [2])

§ 4
Durchführung des Datenschutzes

(3) Der Bundesminister des Innern wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates zu bestimmen, welche technischen und organisatorischen Vorkehrungen gegen Mißbräuche bei der Informationsverarbeitung und gegen Zerstörung, Verlust oder Entstellung der Individualinformationen im Geltungsbereich dieses Gesetzes zu treffen sind. Auf die in § 7 Abs. 3, § 8 Abs. 3 und § 9 Abs. 2 genannten Anwendungsfälle ist dabei einzugehen; das gleiche gilt für die entsprechenden, in den Abschnitten III und IV genannten Anwendungsfälle. Bei der Bestimmung der zu treffenden technischen und organisatorischen Vorkehrungen ist auf ein angemessenes Verhältnis zwischen ihrer jeweiligen Wirksamkeit zugunsten des Datenschutzes und den durch ihre Einführung und Unterhaltung entstehenden Kosten Rücksicht zu nehmen.

§ 7
Informationsaustausch innerhalb des öffentlichen Bereichs

(3) Bei Weitergabe von Individualinformationen durch selbsttätige Einrichtungen ist durch geeignete Vorkehrungen und Maßnahmen sicherzustellen, daß die Informationen nur in dem nach Absatz 1 zulässigen Umfang weitergegeben und nicht durch Unbefugte abgerufen werden können. Über die Weitergabe ist ein Protokoll zu führen, das Empfänger und Art der weitergegebenen Informationen sowie den Zeitpunkt der Weitergabe ausweist. Satz 2 gilt nicht, wenn nur die in § 8 Abs. 2 genannten Informationen weitergegeben werden oder wenn durch die Dokumentation der Datenverarbeitungsprogramme und erforderlichenfalls durch weitere Unterlagen nachgewiesen werden kann, an welche Behörden und sonstige Stellen in welchem Umfang regelmäßig Individualinformationen weitergegeben werden.

§ 8
Informationsweitergabe an Dritte

(2) Die Zustimmung des Betroffenen gilt für die Weitergabe folgender Informationen als erteilt:

1. Familienname,
2. Vornamen,
3. Beruf,
4. Anschrift,
5. Personenkennzeichen.

Soweit der Betroffene ein berechtigtes Interesse glaubhaft macht, kann er die Weitergabe dieser Informationen untersagen.

(3) § 7 Abs. 3 gilt entsprechend. Erfolgt die Weitergabe von Informationen auf andere Weise als durch selbsttätige Einrichtungen, sind die in § 7 Abs. 3 Satz 2 genannten Angaben aktenkundig zu machen.

§ 9
Informationsveränderung

(1) Die Löschung und sonstige Veränderungen der nach § 6 ermittelten Individualinformationen sind nur zulässig, soweit sie für die ermittelnde Behörde oder das ermittelnde Gericht zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben erforderlich sind und in diesem Gesetz nichts anderes bestimmt ist.

(2) Bei automatischer Informationsverarbeitung ist durch geeignete Vorkehrungen sicherzustellen, daß die Informationen nur in dem nach Absatz 1 zulässigen Umfang und nicht durch Unbefugte verändert werden können.

[2]) *Anmerkung des Bundesministeriums des Innern*
Die wiedergegebene auszugsweise Fassung der §§ 4, 7, 8 und 9 des vorläufigen Referentenentwurfs entspricht nicht mehr dem derzeitigen Stand.