PETER FORSTMOSER
unter Mitarbeit von Ernst Felix Schmid

Grundfragen und Lösungsmöglichkeiten einer Datenschutzgesetzgebung[1]

Das Thema "Datenbanken und Persönlichkeitsschutz" ist seit einigen Jahren – vorab im Ausland[2], neuerdings aber auch in der Schweiz[3] – Gegenstand intensiver Diskussion geworden.

1 Stark erweiterte und mit Anmerkungen versehene Fassung des am 7. November 1977 im Rahmen des Symposiums "Computer und Privatspähre" gehaltenen Referats. Stand der Bearbeitung: Ende 1977, mit einzelnen Nachträgen bis Mai 1978.

Mein Assistent, Herr lic. iur. *Ernst Felix Schmid*, hat mich beim Sammeln und der Aufbereitung der Literatur tatkräftig unterstützt und die Anmerkungen weitgehend selbständig redigiert. Für beides schulde ich ihm Dank. – Besonders dankbar bin ich sodann Herrn lic. iur. *Beat Lehmann*, der mir zahlreiche, oft schwer zugängliche Informationen beschafft und durch Kritik sowie eine Vielzahl von Anregungen den vorliegenden Beitrag massgebend beeinflusst hat.

Abkürzungen:

BGE	Bundesgerichtsentscheid	SJZ	Schweizerische Juristen-Zeitung
N	Note	ZGB	Zivilgesetzbuch
NZZ	Neue Zürcher Zeitung	ZR	Blätter für zürcherische Rechtsprechung
OR	Obligationenrecht	ZSR	Zeitschrift für Schweizerisches Recht

2 *Auswahl aus der ausländischen Literatur:*
Herbert Auernhammer, Datenschutzgesetzgebung – Magna Charta des Bürgers von heute, in: Erfassungsschutz ..., hg. von Helmut Krauch, Stuttgart 1975, S. 57 ff.; Bergmann/Möhrle, Datenschutzrecht, Handkommentar zum Bundesdatenschutzgesetz, Stuttgart/München/Hannover 1977 (Loseblattsammlung); Gola/Hümmerich/Kerstan, Datenschutzrecht, Teil I: Das Bundesdatenschutzgesetz, Verfassungsrechtlicher Datenschutz, Internationaler Datenschutz (Berlin 1977 = EDV und Recht, Band 10, hg. von Herbert Fiedler); Otto Mallmann, Zielfunktionen des Datenschutzes (Frankfurt a.M. 1977); Herbert Meister, Datenschutz und Privatrechtsordnung, Betriebs-Berater 1976, S. 1584 ff.; Paul J. Müller, Die Gefährdung der Privatsphäre durch Datenbanken, in: Dammann/Karhausen/Müller/Steinmüller, Datenbanken und Datenschutz, Frankfurt/New York 1974, S. 63 ff.; Wolfgang Schimmel, Datenschutz, in: Steinmüller (Hrsg.): ADV und Recht ... (2. A. Berlin 1976 = Juristische Arbeitsblätter Sonderheft 6); Schimmel/Steinmüller, Rechtspolitische Problemstellung des Datenschutzes, in: Dammann/Karhausen/Müller/Steinmüller: Datenbanken und Datenschutz, Frankfurt/New York 1974, S. 111 ff.; Ulrich Seidel, Datenbanken und Persönlichkeitsrecht ..., Köln 1972; Spiros Simitis, *Bundesdatenschutzgesetz* – Ende der Diskussion oder Neubeginn?, NJW 30 (1977), S. 729 ff.; Wilhelm Steinmüller, *Schutz* vor Datenschutz?, IBM-Nachrichten Nr. 218, 1973, S. 830 ff.; ders., *Stellenwert* der EDV in der öffentlichen Verwaltung und Prinzipien des Datenschutzrechts, in: A. Kaufmann (Hrsg.), Münchner Ringvorlesung, EDV und Recht, Möglichkeiten und Probleme, Berlin 1973, S. 175 ff.; Tiedemann/Sasse, Delinquenzprophylaxe, Kreditsicherung und Datenschutz in der Wirtschaft, Köln/Berlin/Bonn/München 1973. – Nach Abschluss des Manuskripts erschienen: Herbert Auernhammer, Bundesdatenschutzgesetz, Kommentar, Köln/Berlin/Bonn/München 1977; Simitis/Dammann/Mallmann/Reh: Kommentar zum Bundesdatenschutzgesetz (1. Lfg. Baden-Baden 1978).

Vgl. auch die Bibliographie von Kurt Nagel, Datenschutz und Datensicherung, Neuwied/Berlin 1974, ferner die folgenden Gesetzessammlungen: Burhenne/Perband (Hrsg.), EDV-Recht (Loseblattsammlung, Berlin 1970 ff.); Dammann/Mallmann/Simitis (Hrsg.), Die Gesetzgebung zum Datenschutz, eine internationale Dokumentation, Frankfurt a.M. 1977.

Im *Ausland* sind erste Datenschutzgesetze bereits in Kraft, so in Schweden[4], den USA[5], Frankreich[6] und Deutschland[7]. In fast allen übrigen westeuropäischen Staaten sind Gesetzesentwürfe in Bearbeitung[8]. Fachleute nehmen – m.E. freilich allzu optimistisch – an, dass bis 1980 die meisten westeuropäischen Staaten Datenschutzgesetze erlassen werden[9].

3 *Schweizerische Litereratur:*
B.N.: Die Entwicklung des Datenschutzes, sysdata + bürotechnik 8–9/77, S. X f.; Yves Burnand, Banques de données électroniques et droit de l'information, Diss Lausanne 1974; Bü.: Wie steht es um eine schweizerische Datenschutzgesetzgebung?, NZZ 23./24. April 1977, Nr. 94, S. 35; Werner de Capitani, Ein *Computergesetz*?, Bulletin der Schweizerischen Kreditanstalt, Oktober 1973, S. 6 ff.; ders.: EDV und Recht, Schriftenreihe der Schweizerischen Kreditanstalt, Heft 34 (2. A. Zürich 1977), Peter Forstmoser, Datenbanken und Persönlichkeitsschutz, SJZ 70 (1974), S. 217 ff.; Beat Lehmann, Datenschutz und Datensicherheit im Modell eines schweizerischen Datenschutzrechtes, sysdata + bürotechnik 6/77, S. V ff.; ohne Autor, Datenbanken und Persönlichkeitsschutz, NZZ 19. Oktober 1976, Nr. 245, S. 29; Heribert Rausch, Persönlichkeitsrecht contra Datenbanken, NZZ 23./24. April 1977, Nr. 94, S. 35; Jürg Schucan, Datenbanken und Persönlichkeitsschutz, Diss Zürich 1977 = EDV und Recht 4; ders., *Vorbereitung* gesetzlicher Massnahmen zum Datenschutz in der Schweiz, Anmerkungen zu Vorschlägen der Expertenkommission, Film und Recht 19 (1975), S. 682 ff.; Spiros Simitis, Über die *Schwierigkeiten* einer Datenschutzregelung – Zum Stand der Diskussion, Schweizerische Aktiengesellschaft 47 (1975), S. 1 ff.; Gerhard Stadler, Datenschutz zwischen Persönlichkeitsschutz und Informationsfreiheit, NZZ 12./13. November 1977, Nr. 266, S. 37; Horst Witt, Die Gefahren des Missbrauchs von Datenbanken, NZZ 13. Juni 1977, Nr. 269, S. 31. – Nach Fertigstellung des Manuskripts erschienen und nur noch teilweise verarbeitet: Willi Egloff, Braucht die Schweiz ein Datenschutzgesetz?, ZSR 96 (1977) I, S. 345 ff; Staffelbach, Albert: Rechtliche Aspekte des Datenschutzes, output 1/1978, S. 21 ff. – Weitere Literaturangaben im Text.

4 Datalagen vom 11. Mai 1973, (grösstenteils) in Kraft seit 1. Juli 1973; deutsche Übersetzung abgedruckt bei Schucan, Diss, zit. Anm. 3, S. 154 ff.; allgemeiner Überblick über die schwedische Regelung in sysdata + bürotechnik 8–9/77, S. XI.

5 Fair Credit Reporting Act vom 26. Oktober 1970 (Public Law No. 91–508, in Kraft seit 25. April 1971) und Privacy Act vom 31. Dezember 1974 (Public Law No. 93–579, sofortige Inkraftsetzung); deutsche Übersetzung beider Gesetze bei Dammann u.a., zit. Anm. 2, S. 146 ff.

6 Loi No 78–17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, das nach einer Übergangszeit von zwei Jahren vollumfänglich in Kraft tritt; publiziert in Journal Officiel de la République Française vom 7. Januar 1978, S. 227 ff.

7 Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz – BDSG) vom 27. Januar 1977 (Inkraftsetzung grösstenteils auf den 1. Januar 1978; auf den 1. Juli 1977 war der Datenschutzbeauftragte zu bestellen, und ab 1. Januar 1979 gelten die Bestimmungen über die Datensicherungsmassnahmen, vgl. § 47 BDSG; [deutsches] Bundesgesetzblatt I, S. 201 ff.). – Dem BDSG sind Landesdatenschutzgesetze der Länder Hessen (7. Oktober 1970) und Rheinland-Pfalz (24. Januar 1974) vorausgegangen, die (für ihren Kompetenzbereich) zum Teil vom BDSG abweichende Regelungen getroffen haben. – Die einzelnen Rechtsvorschriften sind abgedruckt bei Burhenne/Perband, zit. Anm. 2. – Für einen Überblick über das BDSG vgl. z.B. Simitis, Bundesdatenschutzgesetz, zit. Anm. 2.

8 In Österreich liegt ein Entwurf vom 16. Dezember 1975 vor, der noch 1977 verabschiedet werden soll (Gola/Hümmerich/Kerstan, zit. Anm. 2, S. 104; Text abgedruckt bei Dammann/Mallmann/Simitis, zit. Anm. 2, S. 9 ff., 54 ff.). Übersicht über den Stand der Datenschutzgesetzgebung im übrigen Europa von B.N. in sysdata + bürotechnik 8–9/77, S. XI.

9 So Gerhard Stadler in seinem Vortrag "Zwischen nationaler und internationaler Rechtsetzung für Informationsverkehr und Datenschutz" anlässlich des OECD-Symposiums über

Auch für eine *internationale Ordnung* sind Vorstösse im Gang, so im Rahmen der OECD[10], der EG[11] und des Europarates[12], der kürzlich den Vorentwurf für eine internationale Datenschutzvereinbarung vorgelegt hat[13].

In der *Schweiz* sah auf *kantonaler Ebene* ein – vom Volk abgelehnter – Schaffhauser Gesetzesentwurf von 1972 für Datenbanken des öffentlichen Bereichs Schutzbestimmungen vor[14]. In verschiedenen andern Kantonen sind Vorarbeiten an die Hand genommen worden, und am 1. März 1977 hat Genf als erster Kanton eine "Loi sur la protection des informations traitées automatiquement par ordinateur" in Kraft gesetzt[15].

Auf *Bundesebene* reichte Nationalrat *Bussey* im März 1971 eine Motion betreffend die Gesetzgebung über Computer ein. In der Begründung wird unter anderem ausgeführt:

"Die Speicher des Computers ermöglichen die Schaffung von eigentlichen Datenbanken, die z.B. viele bisher verstreut vorhandene Auskünfte über Personen oder Unternehmen zusammenfassen ... Eine geeignete Gesetzgebung könnte
a) den Bürger und seine Privatsphäre gegen missbräuchliche Verwendung der Computer schützen;
b) eine normale Entwicklung der Verwendung von Computern ermöglichen."[16]

Die Datenschutzproblematik ist damit klar umrissen.

Der 1974 vorgelegte Entwurf der Expertenkommission *Lüchinger* für eine Neugestaltung des Persönlichkeitsschutzes befasst sich in einem eigenen Artikel 28k mit der Gefährdung der Privatsphäre durch Datenbanken[17]. Insbesondere wird ein Auskunftsrecht der Betroffenen vorgesehen:

"Private, welche in Karteien, Datenbanken oder auf ähnliche Weise Angaben über persönliche Verhältnisse sammeln und Dritten zur Verfügung halten, haben auf Verlangen dem Betroffenen schriftlich Auskunft über den Bestand und Inhalt der auf ihn bezüglichen Angaben zu erteilen."

internationalen Datenverkehr und Datenschutz vom 20. September 1977 in Wien, ferner Schucan, zit. Anm. 3, S. XV.

10 Vgl. z.B. Policy issues in data protection and privacy, Concepts and perspectives, Proceedings of the OECD Seminar 24th to 26th June 1974 (1976).

11 Mitteilung der Kommission der EG an den Rat über die Politik der Gemeinschaft auf dem Gebiet der Datenverarbeitung, Dok. I Nr. 39, IV Nr. 20; (deutsche) Bundestags-Drucksache 7/1531.

12 Entschliessung (73) 22 vom 26. September 1973 über den Schutz der Privatsphäre natürlicher Personen gegenüber elektronischen Datenbanken im nicht-öffentlichen Bereich; Entschliessung (74) 29 vom 20. September 1974 über den Schutz der Privatsphäre natürlicher Personen gegenüber elektronischen Datenbanken im öffentlichen Bereich; beide abgedruckt bei Dammann u.a., zit. Anm. 2, S. 37 ff., 40 ff.

13 Comité d'experts sur la protection des données: Avant-projet "Convention internationale sur la protection des données" (77) 2 vom 15. Juni 1977.

14 Gesetz über die elektronische Datenverarbeitung in den öffentlichen Verwaltungen vom 6. März 1972. – Die Ablehnung erfolgte nicht wegen der Datenschutzbestimmungen, sondern weil sich die Gemeinden einer zentralen Datenbank hätten anschliessen müssen.

15 Gesetz vom 24. Juni 1976; offizielle Gesetzessammlung B. 4. 12.

16 Stenographisches Bulletin des Nationalrates 1972, S. 2127 ff.

17 Gesetzesentwurf abgedruckt in SJZ 71 (1975), S. 251 f.

Im Frühjahr 1977 reichte Nationalrat *Gerwig* eine parlamentarische Einzelinitiative ein mit der Forderung, es habe der Bund

"Bestimmungen öffentlich- und privatrechtlicher Natur zum verstärkten Schutz der Persönlichkeit, der persönlichen Entfaltung und beruflichen Betätigung und der Privatsphäre jedes Menschen zu erlassen, insbesondere im Hinblick auf die Gefährdungen und Verletzungen durch systematisches Sammeln, Verarbeiten, Weitergeben und durch jede Form des Verkehrs mit Informationen über Personen."[18]

Die Initiative, zu deren Behandlung eine parlamentarische Kommission gebildet worden ist, enthält im weiteren präzise Hinweise auf die möglichen Elemente eines Datenschutzgesetzes.

In die gleiche Richtung zielt auch eine Motion von Nationalrat *Carobbio*[19], der Gesetzesbestimmungen "über die öffentlichen und privaten Informationszentren" verlangt.

Im Rahmen der *Bundesverwaltung* schliesslich wird zur Zeit an einer Harmonisierung und Vereinheitlichung verschiedener bereits bestehender Verwaltungserlasse gearbeitet.

Bis zum Herbst 1978 will das Eidgenössische Justiz- und Polizeidepartement einen Zwischenbericht zur Frage des Datenschutzrechts vorlegen[20]. Ferner soll sich auch eine Datenschutzverordnung für den Bereich der Bundesverwaltung in Vorbereitung befinden[21].

Es ist daher an der Zeit, dass die Zielsetzung und die möglichen Elemente einer künftigen schweizerischen Datenschutzgesetzgebung in einem weiteren Kreis diskutiert werden.

******

Im folgenden gebe ich zunächst eine Übersicht über Problematik und Zielsetzung des Datenschutzes (Ziff. I). Anschliessend skizziere ich die Ordnung des geltenden schweizerischen Rechts (Ziff. II). Sodann weise ich auf die Gründe hin, aus welchen die heutige Ordnung als ungenügend erachtet wird (Ziff. III). Auf dieser Grundlage sollen die Zielsetzung, der Anwendungsbereich und das mögliche Instrumentarium eines künftigen schweizerischen Gesetzes beleuchtet werden (Ziff. IV). Abschliessend werde ich einige persönliche Folgerungen im Hinblick auf die Gesetzgebung in diesem Bereich ziehen (Ziff. V).

18 Vgl. Übersicht über die Verhandlungen der Bundesversammlung I/II/1977, S. 10; Text auch abgedruckt in SJZ 73 (1977), S. 244 lit. r + s.
19 Motion vom 15. Juni 1977; vgl. Übersicht über die Verhandlungen der Bundesversammlung III/1977, S. 27.
20 NZZ 10. Januar 1978, Nr. 7, S. 25.
21 Tages-Anzeiger, 10. Januar 1978, Nr. 7, S. 1.

I. Problematik und Zielsetzung des Datenschutzes

Auszugehen ist davon, dass das Sammeln und Verwerten personenbezogener Information *legitim und notwendig*, von den Betroffenen *erwünscht*, aber auch *problematisch* ist:

Legitim und notwendig sind Sammlungen personenbezogener Daten insofern, als man im privaten wie im staatlichen Bereich ohne sie gar nicht mehr auskommen könnte[22]. Man denke etwa an die Auskünfte, welche Versicherungen benötigen, um das zu übernehmende Risiko richtig beurteilen zu können, an die Informationsbeschaffung, die vor der Erteilung von Krediten unumgänglich ist, an die umfassenden Angaben, die erforderlich sind, um geeignete Mitarbeiter auszuwählen. Man denke auch an die moderne Leistungsverwaltung – etwa an die Sozialversicherung mit ihren zahlreichen Sparten –, die ohne detaillierte Information über den einzelnen Bürger nicht funktionieren kann. In all diesen Fällen besteht ein schützenswertes Interesse an der Offenlegung persönlicher Verhältnisse.

Die durch die moderne Datenverarbeitung ermöglichten Dienstleistungen sind den Betroffenen in der Regel auch *erwünscht:* Der Neuzuzüger schätzt es, wenn er sich bei einer einzigen zentralen Stelle anmelden kann und die nötigen Informationen verwaltungsintern an die zuständigen Stellen weitergeleitet werden.

Notwendigkeit und Wünschbarkeit dürfen aber nicht über die *Problematik* des Sammelns personenbezogener Daten hinwegtäuschen:

- Jedes Sammeln und Auswerten personenbezogener Information bedeutet einen *Eingriff in die Privatsphäre*[23].
- Dieser ist besonders gravierend, wenn sich die Informationen als *fehlerhaft* erweisen sollten, was auf einem menschlichen oder technischen Versagen beruhen kann, allenfalls aber auch bewusst in Kauf genommen wird[24]. Fehlerhaft oder zumindest irreführend kann insbesondere eine Auskunft sein, die auf einem subjektiven Werturteil beruht, etwa eine Aussage über Charaktereigenschaften oder

22 Forstmoser, zit. Anm. 3, S. 218.

23 So erscheint etwa die Tätigkeit von Adressenverlagen (vgl. dazu statt vieler Seidel, zit. Anm. 2, S. 12 ff. und Schucan, Diss, zit. Anm. 3, S. 64 ff.), die Listen bestimmter Zielgruppen anbieten, zunächst recht harmlos. Sie ist es aber zweifellos nicht, wenn die zum Kauf angebotenen Listen etwa Adressensammlungen von Heiratslustigen, Erotikabestellern, aber auch von Mitgliedern privater Vereinigungen umfassen. – Bedeutend tiefer in das Privatleben greifen sodann Informationen ein, welche durch Auskunfteien (vgl. dazu z.B. Ruprecht Kamlah, Right of Privacy ..., Köln/Berlin/Bonn/München 1969, S. 44 ff.) gesammelt werden, und zwar selbst dann, wenn die Informationen aus allgemein zugänglichen Quellen zusammengetragen werden. – Hingewiesen sei sodann auf die sehr weitgehenden Auskünfte, die derjenige erteilen muss, der eine Lebensversicherung abschliessen, einen Kredit erlangen oder eine neue Stelle antreten will. – Etwas überspitzt kennzeichnet Simitis (Chancen und Gefahren der elektronischen Datenverarbeitung, Neue Juristische Wochenschrift 24, 1971, S. 673 ff., 675) die heutige Situation wie folgt: "Die spätindustrielle Gesellschaft kennt keine Privatheit mehr. Die ökonomischen Strukturen brechen die Privatsphäre auf und zerlegen sie in eine Summe marktstrategisch wichtiger Daten."

24 Vgl. dazu Forstmoser, zit. Anm. 3, S. 219 f.

den Gesundheitszustand. Verfälscht sind aber personenbezogene Auskünfte oft auch deshalb, weil sie aus dem Zusammenhang gerissen und verkürzt wiedergegeben werden[25].

– Gefahren bringt weiter der *Zugriff durch Unbefugte* mit sich: Gerade bei personenbezogenen Informationen ist es wesentlich, wer der Empfänger ist[26].

Diese und weitere Gefahren[27] sind zwar keineswegs neu, in einer informationshungrigen Gesellschaft jedoch *aktualisiert.* Hinzu kommen nun aber *zusätzliche Probleme der elektronischen Datenverarbeitung,* die beim Sammeln und Archivieren mit herkömmlichen Mitteln nicht bestehen[28]:

– Der Unterschied zwischen traditioneller Registrierung und elektronischer Datenverarbeitung ist zunächst ein *quantitativer:* Die EDV erlaubt es, grosse Informationsmengen zu ständig sinkenden Kosten zu speichern. Mit diesem quantitativen ist ein *qualitatives* Moment verbunden: Mittels Kombination zahlreicher Personendaten können neuartige Einsichten gewonnen und allenfalls ein eigentliches Persönlichkeitsprofil erstellt werden.
– Durch den Einsatz von Computern werden sodann *faktische Schranken* des Zugriffs und der Verarbeitung *abgebaut.*
– Weiter ermöglicht es die EDV – im Gegensatz zu den überlieferten Mitteln der Datenverarbeitung –, *"grosse Datenmengen* nach bestimmten Kriterien *umzugliedern* und einen gegebenen Datenbestand ohne besonderen Aufwand nach einer Vielzahl von Kriterien ... zu *selektieren"*[29].
– Endlich dürfte der Einsatz moderner und entsprechend kostspieliger Hilfsmittel zu einer *Konzentration* und Zentralisierung persönlichkeitsbezogener Information führen[30].

Hält man sich die Wünschbarkeit und Notwendigkeit von Personendatenbanken einerseits, ihre Problematik anderseits vor Augen, dann erstaunt nicht, dass sich der einzelne wie die öffentliche Meinung in einem echten, freilich meist kaum bewussten Zwiespalt befinden[31]: In der Affäre "Cincera/Demokratisches Manifest"[32] etwa wurde der Aufbau privater Personendatenbanken fast einhellig scharf verur-

25 Wer als "stockender Zahler" registriert ist, wird zweifellos an Kreditwürdigkeit einbüssen, wenn nicht gleichzeitig darauf hingewiesen wird, dass er die Zahlung deshalb verweigert, weil die Gegenpartei ihren Verpflichtungen nicht korrekt nachgekommen ist.

26 Auskünfte, die man einer Krankenkasse zu erteilen hat, sind nicht für den Arbeitgeber, solche an den Arbeitgeber nicht für eine Werbefirma gedacht.

27 Vgl. namentlich zur Verewigung einmal fixierter Daten und zur Furcht vor Registrierung als Druck zur Anpassung Forstmoser, zit. Anm. 3, S. 220 (mit weiteren Hinweisen).

28 Vgl. dazu Forstmoser, zit. Anm. 3, S. 220 ff.

29 Gerfried Mutz, Rechtsprobleme des sog. Datenschutzes, Juristische Blätter 95 (1973), S. 245 ff., 246.

30 Vgl. Forstmoser, S. 222 (mit weiteren Hinweisen) und Egloff, S. 348 f., beide zit. Anm. 3.

31 Ähnlich auch Egloff, zit. Anm. 3, S. 349 f.

32 Eine sich selbst als Staatsschützer verstehende Privatperson liess Dossiers anlegen, die v.a. linksstehende Personen erfassten.

teilt. Man war sich von links bis rechts einig, dass die Privatsphäre vor Eingriffen zu schützen, Gesinnungsschnüffelei abzulehnen sei. Im gleichen Zeitraum aber wurde – ebenfalls unisono – im Zusammenhang mit den Verfehlungen leitender Organe der Filiale Chiasso einer Schweizer Grossbank der Vorwurf erhoben, die Mitarbeiter würden nicht genügend überwacht, man kümmere sich zu wenig um ihr Privatleben, ihre ausserberuflichen Interessen und ihren Charakter. Erscholl im einen Fall der Ruf nach einem *vermehrten Schutz der Privatsphäre,* so wurde im anderen die *Offenlegung und Überprüfung auch der privaten Verhältnisse* gefordert.

****

Im folgenden sei kurz skizziert, wie das geltende Recht diesen Zielkonflikten Rechnung trägt. Daraus wird sich zeigen, dass die bestehende Ordnung nicht zu genügen vermag, dass vielmehr eine *intensivere Regelung,* die den heutigen technischen Möglichkeiten Rechnung trägt, erforderlich ist.

II. Die Ordnung des geltenden schweizerischen Rechts

Das geltende schweizerische Recht enthält eine Reihe von Bestimmungen, die – obwohl nicht mit Rücksicht auf Datenbanken geschaffen – zumindest teilweisen Datenschutz bieten:

A. Datenschutz im privaten Bereich

Für den privaten Sektor ist vor allem daran zu erinnern, dass gemäss Art. 28 ZGB *jedermann, der "in seinen persönlichen Verhältnissen unbefugterweise verletzt wird", auf Beseitigung der Störung, auf Schadenersatz und allenfalls auf Genugtuung klagen kann*[33].

33 Vgl. Burnand No. 101 ff., Schucan, Diss, S. 12 ff., Egloff S. 357 ff.. (alle zit. Anm. 3); ferner etwa Richard Frank, Der Schutz der Persönlichkeit in der Zivilrechtsordnung der Schweiz, Archiv für civilistische Praxis 172 (1972), S. 56 ff.; Peter Jäggi, Fragen des privatrechtlichen Schutzes der Persönlichkeit, ZSR 79 (1960) II, S. 133a ff., 229a ff.; Jacques-Michel Grossen, La protection de la personnalité en droit privé, ZSR 79 (1960) II, S. 1a ff., 73a ff.; ders., Das Recht der Einzelpersonen, in: Schweiz. Privatrecht II (Basel/Stuttgart 1967), S. 285 ff., 354 ff.; Kaspar Ernst Hotz, Zum Problem der Abgrenzung des Persönlichkeitsschutzes nach Art. 28 ZGB, Diss Zürich 1967, S. 69 ff.

Dass diese Norm gerade im Bereich des Datenschutzes bedeutsam werden könnte[34], zeigt ein neuerer Bundesgerichtsentscheid[35], der das Verhalten eines Adressenverlages zu beurteilen hatte. Dieser hatte eine Reihe von "Spezial-Adress-Verzeichnissen" zum Kauf angeboten, darunter der Mitglieder der Freimaurer- und Odd-Fellows-Logen, des Lions-Clubs und der Philantropischen Gesellschaft Union. Auf Klage einer dieser Vereinigungen hin bestätigte das Bundesgericht, dass die Zugehörigkeit zu einem der genannten Vereine eine Tatsache sei, die zur Privatsphäre sowohl der Mitglieder wie auch des Vereins selbst gehöre. Es schützte entsprechend eine Klage aus Art. 28 ZGB und das Verbot des Vertriebs der Verzeichnisse.

Ein weiterer Schutz liegt in den *Berufsgeheimnissen*, namentlich dem Anwalts-[36], dem Arzt-[37] und dem Bankgeheimnis[38]. Diese und die Geheimhaltungspflichten, die sich als Nebenpflichten aus einem Vertrag ergeben können[39], finden auch auf die Datenverarbeitung Anwendung: Der zur Geheimhaltung Verpflichtete muss daher die nötigen Vorkehren treffen, um Informationen vor dem Zugriff Unbefugter zu sichern.

Endlich sei noch darauf hingewiesen, dass es in den Beziehungen zwischen Privatpersonen grundsätzlich *keine Pflicht zur Auskunftserteilung*[40] gibt, dass es also dem einzelnen rechtlich freisteht, Einblick in seinen Privatbereich zu verweigern. Dieser Schutz ist allerdings oft mehr theoretischer Natur: Einmal können mit modernen Mitteln zahlreiche Rückschlüsse auf private Verhältnisse aus allgemein zugänglichen Informationen gezogen werden. Sodann ist in vielen Fällen die Freiheit, Auskunft zu erteilen, illusorisch, weil ohne Gewährung von Einblick gewisse Rechtsgeschäfte gar nicht getätigt werden können[41].

34 Vgl. aus der schweizerischen Literatur z.B. Heinz Hausheer, Verstärkter Persönlichkeitsschutz ..., in: Festgabe Henri Deschenaux, Fribourg 1977, S. 81 ff., 94.

35 BGE 97 II 97 ff.; vgl. auch die Besprechung von Peter Liver in Zeitschrift des Bernischen Juristenvereins 109 (1973), S. 57. – Frühere einschlägige Entscheide besprochen von Rausch, zit. Anm. 3.

36 Art. 321 Strafgesetzbuch. – Vgl. dazu statt vieler Heinz Walter Blass, Die Berufsgeheimhaltungspflicht der Ärzte, Apotheker und Anwälte, Diss Zürich 1944; W. Stocker, Das Anwaltsgeheimnis, Schweizerische Zeitschrift für Strafrecht 68 (1953), S. 1 ff.; Paul Wegmann, Die Berufspflichten des Rechtsanwaltes, Diss Zürich 1969, insb. S. 156 ff. und Reinhard W. von Meiss, Die persönliche Geheimsphäre und deren Schutz im prozessualen Verfahren, Diss Zürich 1975, S. 176 ff.

37 Art. 321 Strafgesetzbuch. – Vgl. dazu etwa Blass, zit. Anm. 36; Willy Heim, Le secret médical ..., Diss Lausanne 1944; René Russek, Das ärztliche Berufsgeheimnis, Diss Zürich 1954, ferner ZR 76 (1977) Nr. 45, S. 84 ff. Speziell zur Frage Computer und ärztliches Berufsgeheimnis Peter Forstmoser, Der Einsatz von Computern und das ärztliche Berufsgeheimnis, Schweizerische Ärztezeitung 55 (1974), S. 729 ff.; ders., EDV und Persönlichkeitsschutz, veska 39 (1975), S. 285 ff.; Piero Schäfer, Das ärztliche Berufsgeheimnis und die elektronische Datenverarbeitung, Diss Zürich, erscheint 1978.

38 Art. 47 Bankengesetz. – Vgl. dazu statt vieler die Kommentierung von Bodmer/Kleiner/Lutz, Zürich 1976, ferner Aubert/Kernen/Schönle, Le secret bancaire suisse, Bern 1976 und Pius Schwager, Das schweizerische Bankgeheimnis, Diss Fribourg 1973 (alle mit weiteren Literaturangaben).

39 Vgl. z.B. im Arbeitsvertrag OR 321a IV.

40 Vgl. z.B. Merz in Berner Kommentar, Einleitungsband N 270 zu ZGB 2.

41 Z.B. Versicherungs- oder Darlehensverträge.

B. Datenschutz im öffentlichen Bereich

Im öffentlichen Bereich ist Grundlage das Recht auf *Unverletzlichkeit der Privatsphäre,* das in der Schweiz als ungeschriebenes Freiheitsrecht anerkannt ist. Damit besteht ein Schutz schon auf *Verfassungsstufe*[42].

Im *Verwaltungsrecht* ist vor allem auf die *Pflicht des Beamten zur Geheimhaltung* und die damit verbundene Schweigepflicht hinzuweisen[43]. Verwaltungsangestellte müssen über im Rahmen ihrer Aufgabe erlangte Wahrnehmungen Stillschweigen bewahren, und zwar nicht nur gegenüber Privaten, sondern auch gegenüber anderen Amtsstellen[44].

Während die Schweigepflicht die Weiterleitung von Daten unterbindet, wird die Datenregistrierung als solche durch den Grundsatz der *Gesetzmässigkeit der Verwaltung*[45] eingeschränkt. Wo keine entsprechende Kompetenz vorliegt, können Verwaltungsorgane nicht befugt sein, personenbezogene Informationen zu sammeln und zu verarbeiten[46].

C. Datenschutz im Strafrecht

Im Strafrecht gibt es ebenfalls einzelne Vorschriften, die dem Schutz der Privatsphäre auch im Hinblick auf Datenbanken dienen können, so namentlich die Normen betreffend die Verletzungen von Amts- und Berufsgeheimnissen[47,48].

42 Vgl. z.B. BGE 100 Ia 193 E 3a, 90 I 34 ff.; Burnand, no. 214, Egloff, S. 356 f. und Schucan, Diss, S. 1 ff., alle zit. Anm. 3; ferner Hans Peter Renfer, Das Grundrecht der persönlichen Freiheit (Diss Basel 1972, Maschinenschrift).

43 Vgl. dazu Paul Reichlin, Die Schweigepflicht des Verwaltungsbeamten, Zentralblatt für Staats- und Gemeindeverwaltung 53 (1952), S. 475 ff., 505 ff.; Imboden/Rhinow, Schweizerische Verwaltungsrechtsprechung II, 5. A. Basel/Stuttgart 1976, Nr. 149, S. 1089 ff.; Thomas Fleiner, Grundzüge des allgemeinen und schweizerischen Verwaltungsrechts, Zürich 1977, S. 396; ferner ZR 76 (1977) Nr. 45, S. 24 ff.; speziell in bezug auf den Datenschutz Schucan, Diss, zit. Anm. 3, S. 8 f.

44 Vgl. SJZ 69 (1973), S. 331. – Vorbehalten ist die Auskunftserteilung an die hierarchisch vorgesetzte Instanz, SJZ 68 (1972), S. 15 f.

45 Vgl. dazu André Grisel, Droit administratif suisse, Neuenburg 1970, S. 164 ff.; Imboden/Rhinow, zit. Anm. 43, I Nr. 59, S. 348 ff.; Fleiner, zit. Anm. 43, S. 63.

46 Zum Legalitätsprinzip im Bereich der Datenverarbeitung Adalbert Podlech, Datenschutz im Bereich der öffentlichen Verwaltung, Berlin 1973, S. 55 ff.; Bernhard Schlink, Der Bürger als Datenobjekt, in: Kilian/Lenk/Steinmüller (Hrsg.), Datenschutz, Frankfurt 1973, S. 155 ff., 159 ff.; Schucan, Diss, zit. Anm. 3, S. 6 f.

47 Art. 320, 321 Strafgesetzbuch, ferner Art. 47 Bankengesetz. – Vgl. die vorn Anm. 33–38 zitierte Literatur sowie Martin Lüscher, Das schweizerische Bankgeheimnis in strafrechtlicher Hinsicht, Diss Zürich 1972; Anna-Maria Grossmann, Die Verletzung des Amtsgeheimnisses aufgrund des Art. 320 StGB, Diss Zürich 1946; Alexander Sieben, Das Berufsgeheimnis aufgrund des Schweizerischen Strafgesetzbuches, Diss Bern 1944. Vgl. auch die übrigen strafrechtlichen Bestimmungen betreffend Geheimnisverletzungen, namentlich Art. 162, 273, 283 Strafgesetzbuch.

48 Zur Frage, ob das datenverarbeitende Personal – soweit es mit ärztlichen oder ähnlichen

III. Ungenügen des geltenden Rechts

Obschon – wie soeben gezeigt – das geltende Recht nicht zu unterschätzenden Schutz gewährt, ist heute kaum bestritten, dass die herkömmliche Ordnung allgemein zum Schutz der Persönlichkeit, besonders aber angesichts von Datenbanken nicht mehr zu genügen vermag[49].

A. Allgemeines Ungenügen des Persönlichkeitsschutzes

Unbestritten ist zunächst, dass der im wesentlichen vom Anfang dieses Jahrhunderts stammende Persönlichkeitsschutz des schweizerischen Rechts den heutigen Bedürfnissen nicht mehr genügt[50]. Zwar hat er sich als ausserordentlich elastisch und anpassungsfähig erwiesen, doch trägt er modernen Entwicklungen zu wenig Rechnung. Sodann ist zu Recht der fast ausschliesslich repressive Charakter der geltenden Ordnung kritisiert worden[51].

Der Bundesrat hat denn auch eine Expertenkommission mit der Revision des zivilrechtlichen Persönlichkeitsschutzes beauftragt[52]. Ein entsprechender Entwurf liegt seit 1974 vor, dürfte aber erst nach 1979 zur Behandlung in den Räten kommen.

B. Ungenügen spezifisch im Hinblick auf Datenbanken

Nicht zu genügen vermag die geltende Ordnung besonders im Hinblick auf Personendatenbanken:

- Die einschlägigen *Rechtsvorschriften* sind in *verschiedenen Erlassen verstreut* und decken den Datenschutz mehr zufällig ab. Dies führt zu Inkonsequenzen[53].
- Die vorhandenen Rechtsnormen sind *zu wenig konkret*, und es lässt sich schwer voraussehen, was aus den Generalklauseln mit Bezug auf die Verarbeitung personenbezogener Daten im einzelnen abzuleiten ist[54].

Informationen zu tun hat – als Hilfspersonal im Sinne von Art. 321 Strafgesetzbuch zu bezeichnen ist und somit unter das entsprechende Berufsgeheimnis fällt, vgl. Forstmoser, zit. Anm. 3, S. 227, Anm. 83; Schäfer, zit. Anm. 37, 3. Kap. § 4 B II.

49 Vgl. statt vieler Hausheer, zit. Anm. 34, insb. S. 94.

50 Ebenso Rausch; Burnand no. 124 ff., beide zit. Anm. 3.

51 Rausch, zit. Anm. 3.

52 Sog. Kommission Lüchinger.

53 Allgemein Hausheer, zit. Anm. 34, S. 96.

54 Vgl. auch Schucan, Diss, zit. Anm. 3, S. 13.

- Gerügt worden ist, dass das geltende Recht *kein Einsichtsrecht der Betroffenen*[55] vorsieht und dass daher eine Persönlichkeitsverletzung allenfalls gar nicht feststellbar ist.
- Sodann *fehlt* im geltenden Recht die *präventive Kontrolle*[56] und kann praktisch nur eingeschritten werden, wenn Persönlichkeitsrechte bereits verletzt worden sind.
- Zu wenig beachtet wurde meines Erachtens bisher ein weiteres Element: das *Erfordernis, mit der internationalen Entwicklung* im Bereich des Datenschutzes *Schritt zu halten*[57]. Schon heute wird im Ausland – im Anschluss an die steuerrechtliche Terminologie – kritisch von der Möglichkeit von "data haven", "Datenoasen", gesprochen[58]. Ausländische Gesetze und Gesetzesentwürfe[59] sehen bereits Restriktionen für den grenzüberschreitenden Datenverkehr vor für den Fall, dass im Ausland nicht der gleiche Standard des Datenschutzes gewährleistet ist[60].

Die *Notwendigkeit einer besonderen Gesetzgebung für Personendatenbanken scheint allgemein anerkannt*[61]: So hat der Bundesrat schon 1972 in seiner Antwort auf die Motion Bussey festgehalten, dass "les clauses générales de notre droit positif ne permettent probablement pas de protéger suffisamment la personalité contre les atteintes inhérentes aux importants systèmes d'information de l'avenir"[62]. Die Expertenkommission Lüchinger hat – obwohl sie eine spezielle Bestimmung zum Schutz gegenüber Datenbanken vorschlägt – erklärt, es werde eine umfassende Datenschutzgesetzgebung "auf die Dauer nicht zu umgehen sein"[63]. Vor wenigen Monaten hat sodann Bundesrat Furgler erneut auf die Notwendigkeit einer Datenschutzgesetzgebung hingewiesen[64].

55 Burnand, zit. Anm. 3, no. 126. Rausch, zit. Anm. 3, vertritt allerdings die These, ein Einsichtsrecht liesse sich eventuell aus ZGB 1 II herleiten, indem der Richter eine sog. echte Gesetzeslücke annehmen könnte. Persönlich möchte ich dies eher bezweifeln. – Allenfalls liesse sich ein Auskunftsrecht aus ZGB 2 begründen (vgl. Merz, zit. Anm. 37, N 278 zu ZGB 2).

56 Vgl. Rausch, zit. Anm. 3.

57 Vgl. auch Schucan, Diss, S. 44 ff. und Burnand no. 191, beide zit. Anm. 3.

58 Vgl. Stadler, zit. Anm. 9, S. 8; Pantages/Pipe, A New Headache For International DP, Datamation Juni 1977, S. 115 ff.

59 Vgl. die Zusammenstellungen bei Hans Joachim Ordemann, Grenzüberschreitender Datentransport – Internationales Datenschutzübereinkommen, Öffentliche Verwaltung und Datenverarbeitung 1977, S. 3 ff., 4 f.; sowie bei Stadler, zit. Anm. 9, S. 4 f.

60 So z.B. § 11 Satz 2 Datalagen.

61 Vgl. etwa Hausheer, zit. Anm. 34, S. 94, allerdings kritisch zum Phänomen, dass durch die zunehmende Bildung von Spezialgesetzen Grundgedanken, die in eine allgemeine Kodifikation gehörten, aufgesplittert werden (S. 96). – Eine leicht andere Auffassung vertritt dagegen Egloff, zit. Anm. 3, S. 364, 368: Die Schaffung eines speziellen Datenschutzgesetzes erscheint ihm als nicht vordringlich, dafür seien aber punktuelle Verbesserungen notwendig, so z.B. die Statuierung von Auskunftsansprüchen.

62 Stenographisches Bulletin des Nationalrates 1972, S. 2130.

63 Schlussbericht S. 5 f.; ferner Adolf Lüchinger, Der Schutz der Persönlichkeit, Mitteilungen des Schweizerischen Anwaltsverbandes Heft 57, September 1977, S. 1 ff.

64 Stellungnahme anlässlich der Jahresversammlung 1977 des Schweizerischen Anwaltsverbandes, NZZ 27. Juni 1977, Nr. 148, S. 13.

Es ist daher im folgenden zu prüfen, welche Elemente eine schweizerische Datenschutzgesetzgebung enthalten könnte.

IV. Anwendungsbereich, Inhalt und Instrumentarium einer schweizerischen Datenschutzgesetzgebung

A. Anwendungsbereich und Gesetzgebungstechnik

1. Der Schutzzweck eines Datenschutzgesetzes

In der Literatur wird das Ziel der Datenschutzgesetzgebung gelegentlich äusserst weit gefasst: Eine Datenschutzgesetzgebung hätte danach zur Aufgabe die "Verhinderung aller gesellschaftlich unerwünschten Folgen der Datenverarbeitung"[65].

Eine solch weite Fassung ist meines Erachtens abzulehnen[66], da sonst der ohnehin etwas verschwommene Begriff des Datenschutzes vollends ausufern würde. Datenschutz ist vielmehr in einem engeren Sinne zu verstehen: Schutzzweck soll die *Privatsphäre der Person, und zwar in erster Linie der natürlichen Person* im Hinblick auf die Datenspeicherung und Datenverarbeitung sein. Diese enge Zielsetzung deckt sich – soweit ich sehe – mit den bisherigen politischen Vorstössen[67] wie auch den in Schweden und Deutschland realisierten Lösungen.

2. Zu schützende Personen und Daten

a. Geschützte Personen

Wenn auch ein Datenschutzgesetz in erster Linie die natürliche Person zu schützen hat, sollten sich – entgegen der Regelung etwa des deutschen Bundesdatenschutzgesetzes[68] – auch juristische Personen[69] auf die Schutzbestimmungen berufen

65 Wilhelm Steinmüller u.a., Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, (deutsche) Bundestags-Drucksache VI/3826. Ebenfalls umfassend Bergmann/Möhrle, zit. Anm. 2, Systematik Ziff. 1.4.1. Lehmann, zit. Anm. 3, S. V, will den Datenschutz verstanden wissen als "Schutz von Institutionen und ihrer verfassungsrechtlichen Position". – Immerhin anerkennen Schimmel/Steinmüller, zit. Anm. 2, S. 124 auch den Datenschutz im Sinne des Schutzes des einzelnen als sog. Datenschutz im engern Sinn oder Individualdatenschutz.

66 Ebenso Schucan, Diss, zit. Anm. 3, S. 12; Auernhammer, zit. Anm. 2, S. 63.

67 So die Initiativen Bussey und Gerwig, zit. Anm. 16 bzw. 18.

68 § 2 I BDSG.

69 Ebenso Schucan, Diss, S. 26; de Capitani, EDV und Recht, S. 30; Burnand no. 215, alle zit. Anm. 3.

können. Es entspricht dies schweizerischer Tradition im Bereich des Persönlichkeitsschutzes[70] und schliesst eine Differenzierung im Einzelfall[71] keineswegs aus.

b. *Geschützte Daten*

Aus dem vorstehend umschriebenen Schutzzweck ergibt sich, dass *personenbezogene Daten* – d.h. *Informationen, welche die Privatsphäre betreffen* – zu schützen sind. Mit dieser Umschreibung ist freilich "nicht mehr als eine Richtungsangabe"[72] gewonnen. Es fragt sich daher, ob eine präzisere Formulierung im Gesetz möglich und tunlich ist. Kann und soll das Gesetz etwa nach bestimmten Kategorien differenzieren, wie dies die auch vom Bundesgericht[73] übernommene Sphärentheorie[74] versucht? Soll auf Gesetzesstufe näher umschrieben werden, was zum Geheim-, was zum Privat- und was zum Gemeinbereich, zur vie intime, vie privée und zur vie publique gehört?

Meines Erachtens sollte der *Gesetzgeber von einer* solchen *Unterscheidung grundsätzlich absehen* und sie dem Richter *im Einzelfall überlassen*[75]. Der Sphärentheorie ist zu Recht entgegengehalten worden, dass eine Definition verschiedener Kategorien nur kasuistisch, nicht aber abstrakt erfolgen kann[76]. Eine überzeugende Alternative, die eine klare Abgrenzung ermöglichen würde, ist m.W. bisher nicht vorgelegt worden. Es dürfte dies auch kaum möglich sein, ist doch der Stellenwert

70 Vgl. BGE 97 II 97 ff., 100; 95 II 488 E 4; Rolf Bär, Persönlichkeitsschutz der juristischen Person, Zeitschrift des Bernischen Juristenvereins 103 (1967), S. 100 ff.; Christian Riesen, Die Persönlichkeitsrechte der juristischen Personen (Diss Basel 1955, Maschinenschrift); kritisch zu BGE 95 II 488 Heribert Rausch, Wieviel Fiktion ist genug?, in: Festgabe Meier-Hayoz, Zürich 1972, S. 53 ff.

71 August Egger, Zürcher Kommentar zum Personenrecht (2. A. Zürich 1930) N 9 ff. zu ZGB 53; Riesen, zit. Anm. 70, S. 126 ff.

72 Simitis, Schwierigkeiten, zit. Anm. 3, S. 4.

73 BGE 97 II 100 f. E 3.

74 Danach werden die Lebensbereiche eines Menschen gewöhnlich in drei Teilbereiche aufgeteilt: Dem Gemeinbereich werden die vom Persönlichkeitsschutz erfassten Geheim- und Privatbereiche gegenübergestellt. – Die Bereiche werden in der Literatur folgendermassen umschrieben: Der Geheimbereich umfasst die "Lebensvorgänge, von denen der Mensch will, dass sie der Wahrnehmung und dem Wissen aller übrigen Mitmenschen entzogen sind, es sei denn, dass er ein Geheimnis mit einem bestimmten Andern (und nur mit diesem) teilen will" (Jäggi, zit. Anm. 30, S. 227a). Demgegenüber umfasst der Privatbereich die "Lebensäusserungen, die der Einzelne gemeinhin mit nahe verbundenen Personen, aber nur mit diesen, teilen will ..." (Jäggi, ebenda, S. 227a; ähnlich BGE 97 II 101). Der Gemeinbereich schliesslich umfasst die Lebensbetätigungen, "durch die sich der Mensch wie jedermann in der Öffentlichkeit benimmt ..." (Jäggi, ebenda, S. 229a). – Vgl. auch Schucan, Diss, zit. Anm. 3, S. 16 ff.

75 Für eine Interessenabwägung im Einzelfall ebenfalls Rausch, zit. Anm. 3, ferner Adolf Lüchinger, Der privatrechtliche Schutz der Persönlichkeit und die Massenmedien, SJZ 70 (1974), S. 321 ff., 324.

76 Vgl. Schimmel in Steinmüller, zit. Anm. 2, S. 148.

einer die Person betreffende Aussage je nach Adressat[77], Zeitpunkt[78] und weiteren Umständen[79] sehr verschieden[80].

Das Gesetz hätte damit *jede Art der Datenverarbeitung, die die persönlichen Verhältnisse verletzt,* für *widerrechtlich* zu erklären. Die Differenzierung und Konkretisierung wäre dem Richter zu überlassen, wobei immerhin schon im Gesetz einige Beispiele aufgezählt werden könnten.

Der Grundsatz wäre freilich in einer Richtung zu modifizieren: Sogenannte *Intimdaten,* "heisse Daten", Informationen, die – in den Worten des Bundesgerichts[81] – "der Kenntnis aller anderen Leute entzogen sein sollen, mit Ausnahme jener Personen, denen diese Tatsachen besonders anvertraut wurden", sollten zusätzlich geschützt werden. Ich denke an ein ausdrückliches Verarbeitungs*verbot* mit genau umschriebenen Ausnahmen[82].

Dagegen würde ich die Ausklammerung sogenannt *freier Daten*[83] ablehnen[84], da auch diese in einer die Persönlichkeit verletzenden Art zusammengetragen werden können[85]. Eine vernünftige Datenschutzordnung wird der legitimen Verarbeitung allgemein zugänglicher Daten ohnehin keine übermässigen Schranken auferlegen.

3. Zu erfassende Datenbanken

a. Regelung des öffentlichen und des privaten Bereichs

Zu regeln sind – wie in Schweden[86] und der BRD[87] und entsprechend der Initiative Gerwig – sowohl der *öffentliche wie der private Bereich.* Die Argumente, welche in

77 Simitis, Schwierigkeiten, zit. Anm. 3, S. 5.
78 Vgl. dazu das bei Rausch, zit. Anm. 3, angeführte Beispiel; ferner Schimmel/Steinmüller, zit. Anm. 2, S. 130.
79 Vgl. Schucan, Diss, zit. Anm. 3, S. 21 f.
80 Ebenso Egloff, zit. Anm. 3.
81 BGE 97 II 101.
82 Verschiedentlich treffen Datenschutzgesetze Sondervorschriften für Intimdaten, so z.B. § 552a lit. e VII Privacy Act betreffend Informationen über die Ausübung von Rechten des First Amendment (Meinungsäusserungsfreiheit und andere Grundrechte). – Als Intimdaten könnten etwa – entsprechend einem Vorschlag des Europarates (vgl. Art. 3 lit. b, zit. Anm. 13) – bezeichnet werden Daten betreffend Rasse, philosophische, religiöse, politische oder gewerkschaftliche Ansichten, ferner auch Informationen über den Gesundheitszustand.
83 Das BDSG hat – trotz der Kritik eines Teils der deutschen Literatur (z.B. Auernhammer, S. 64 und Schimmel/Steinmüller, S. 156, beide zit. Anm. 2), – in §§ 24 II und 32 III gewisse Daten von der Gesetzesregelung ausgenommen.
84 Ebenso Schucan, Diss, zit. Anm. 3, S. 23.
85 So kann z.B. anhand mehrerer Jahrgänge des Telefonbuches festgestellt werden, wie oft jemand in einem bestimmten Zeitraum die Wohnung wechselte, was weitere Schlussfolgerungen zulässt.
86 § 1 III Datalagen.
87 § 1 II BDSG.

der Literatur zugunsten einer Beschränkung sei es auf den öffentlichen sei es auf den privaten Bereich vorgetragen werden, vermögen nicht zu überzeugen[88].

Dies heisst freilich nicht, dass private und staatliche Datenbanken notwendig dem gleichen Gesetz zu unterstellen sind[89].

b. Erfassung der für eigene Bedürfnisse und der für Dritte geführten Datenbanken

Keine Rolle spielen darf sodann, ob eine Personendatenbank nur für eigene Zwekke[90] oder für Dritte[91] geführt wird.

c. Erfassung automatisch und manuell bearbeiteter Datenbanken

Stark umstritten ist, ob auch manuell geführte Datenbanken durch eine spezifische Datenschutzgesetzgebung zu erfassen sind oder ob für sie der allgemeine Persönlichkeitsschutz ausreicht. Für eine Beschränkung wird vor allem ins Feld geführt, bei manuell geführten Datenbanken *fehle die besondere Gefährlichkeit,* die eine eigene Regelung erforderlich mache[92].

Meines Erachtens sind trotzdem *alle Personendatenbanken* in eine spezifische gesetzliche Ordnung einzubeziehen[93], und zwar aus verschiedenen Gründen:

- Einmal dürfte es heute schon schwierig und künftig überhaupt unmöglich sein, saubere Kriterien zur *Grenzziehung* zwischen manueller Verarbeitung einerseits und elektronischer bzw. automatischer Verarbeitung anderseits zu finden[94].
- Sodann könnte eine zu enge Fassung zu einer unerwünschten *Diskriminierung oder Privilegierung* der einen oder anderen Art der Verarbeitung führen.
- Endlich – und dies scheint mit vor allem wichtig – könnte eine zu enge Fassung dazu führen, dass gerade bei fragwürdigen Anwendungsformen auf die nicht geregelte manuelle Verarbeitung ausgewichen und damit der *spezifische Datenschutz illusorisch* gemacht wird[95,96].

88 Gleicher Meinung auch Burnand no. 174 ff., insb. 181; de Capitani, Computergesetz, S. 7; Schucan, Diss, S. 43, alle zit. Anm. 3; Lüchinger, zit. Anm. 60; ferner die bei Forstmoser, zit. Anm. 3, S. 224, Anm. 65, aufgeführte deutsche Literatur.

89 Vgl. nachstehend S. 45 f., ferner auch Hausheer, zit. Anm. 34, S. 95.

90 Etwa das Personalinformationssystem eines Unternehmens.

91 So die Datenbanken von Auskunfteien.

92 So Schucan, Vorbereitung, S. 683; Burnand no. 171, beide zit. Anm. 3; ferner Tiedemann/Sasse, zit. Anm. 2.

93 Vgl. neben der bei Forstmoser, zit. Anm. 3, S. 224, Anm. 66, aufgeführten deutschen Literatur de Capitani, EDV und Recht, zit. Anm. 3, S. 30.

94 Ebenso Schucan, Vorbereitung, zit. Anm. 3, S. 683.

95 Ebenso de Capitani, EDV und Recht, zit. Anm. 3, S. 30 und Steinmüller, Stellenwert, zit. Anm. 2, S. 193; zustimmend auch Schucan, Diss, zit. Anm. 3, S. 41, der aber gleichwohl manuelle Datenbanken von einem Datenschutzgesetz ausnehmen will (S. 42 f.).

96 Im Gegensatz zum schwedischen Datalagen (§ 1 III) umfasst das BDSG auch die manuellen

4. Exkurs: Gesetzgebungsstufe und Gesetzgebungstechnik

a. Legiferierung auf Bundesebene oder in den Kantonen?

Offensichtlich ist zunächst, dass die Verarbeitung personenbezogener Daten durch *Private* auf Bundesebene geregelt werden müsste. Ob dabei die bestehenden Bundeskompetenzen ausreichen[97] oder ob vorab eine besondere Verfassungsgrundlage zu schaffen wäre, müsste freilich im einzelnen noch überprüft werden[98].

Datenbanken des *öffentlichen Bereichs auf Bundesebene* sind zwangsläufig durch den Bund zu ordnen. Neue Bundeskompetenzen sind hiefür kaum erforderlich[99].

Für *kantonale und kommunale Datenbanken* wäre der Bund dagegen nach geltendem Recht nur sehr beschränkt zur Gesetzgebung zuständig[100]. Eine gewisse Harmonie auch in diesem Bereich könnte durch ein *Rahmengesetz*, allenfalls auch durch ein *Konkordat*, verbunden mit einem Mustergesetz, erzielt werden.

b. Einheitliches Datenschutzgesetz oder Einzelbestimmungen in Spezialgesetzen?

Eine weitere gesetzgebungstechnische Frage ist die, ob die einschlägigen Bestimmungen in einem *einheitlichen Gesetz* zusammenzufassen oder ob sie *in Erlasse, die sich primär mit anderen Fragen befassen*[101], *einzubauen* sind. Der Entscheid fällt besonders schwer, weil der Datenschutz – wie in der deutschen Literatur[102] betont wird – eine sogenannte *Querschnittsmaterie* darstellt: Datenschutzrechtliche Probleme stellen sich in überaus vielen, voneinander weitgehend unabhängigen Rechtsgebieten[103].

Offenlassen möchte ich vorab die Frage, ob es möglich ist, für den öffentlichen und den privaten Bereich eine gemeinsame Grundlage zu schaffen. Für diesen letzteren gebe ich einem *einheitlichen Datenschutzgesetz* im Interesse der Übersicht-

Datenbanken (§ 2 III Ziff. 3; dazu z.B. Bergmann/Möhrle, zit. Anm. 2, § 2 Anm. 4; ebenso § 2 Ziff. 3 des österreichischen Entwurfs).

97 So Schucan, Diss, zit. Anm. 3, S. 44.

98 Kritisch auch Burnand, zit. Anm. 3, no. 185; vgl. auch Fritz Gygi, Zur Rechtsetzungszuständigkeit des Bundes auf dem Gebiete des Zivilrechtes (BV 64), ZSR 95 (1976) I, S. 343 ff.

99 Schucan, Diss, S. 43; Burnand no. 189, beide zit. Anm. 3.

100 Nämlich nur soweit Kantone und Gemeinden Bundesrecht ausführen (Schucan, Diss, S. 44; Burnand no. 190, beide zit. Anm. 3); "es sei denn, es lasse sich eine Gesetzeskompetenz des Bundes daraus ableiten, dass ein Verfassungsauftrag zur Konkretisierung des Grundrechtes der persönlichen Freiheit angenommen wird" (Hausheer, zit. Anm. 31, S. 95, Anm. 39).

101 Etwa im Arbeitsvertragsrecht, im AHV-Gesetz, in Gerichtsverfassungs-, Universitäts- und Beamtengesetzen, im Strafgesetz usw.

102 Statt vieler Bergmann/Möhrle, zit. Anm. 2, Systematik Ziff. 2.2.

103 So gelten für die datenschutzrechtlichen Aspekte von Tests, Befragungen, Personalakten usw. die obligationenrechtlichen Normen über den Arbeitsvertrag, für diejenigen der Berufsgeheimnisse das Strafgesetzbuch.

lichkeit und Einheitlichkeit den Vorzug. Freilich müsste diese Ordnung ziemlich allgemein und abstrakt gehalten werden[104]. Sie könnte für einzelne Bereiche durch zusätzliche Bestimmungen ergänzt und modifiziert werden[105]. Dem allgemeinen Datenschutzgesetz käme daher – wie auch in Deutschland[106] – *subsidiärer Charakter* zu.

B. Schranken des Sammelns, der Speicherung, Bearbeitung und Weitergabe personenbezogener Daten

1. Speicherungsverbot und -beschränkungen

Auszugehen ist davon, dass die Speicherung und Verarbeitung personenbezogener Daten *zulässig*[107] sein muss, falls ein schützenswertes Interesse besteht[108]. Abzulehnen wäre es, die Verarbeitung personenbezogener Information generell von der Zustimmung des Betroffenen abhängig zu machen.

Dies schliesst freilich nicht aus, dass – wie bereits angetönt –für Intimdaten ein Speicherungsverbot mit Erlaubnisvorbehalt vorgesehen wird[109].

2. Bearbeitungs- und Weitergabeverbote und -beschränkungen

Unter dem Gesichtspunkt des Persönlichkeitsschutzes problematisch ist vielfach nicht so sehr die Auswertung der Einzelinformation, als die *Kombination* von Personendaten, aus der sich neue, andersartige Aussagen ergeben. Es ist daher zu prüfen, ob und in welcher Form der Daten*integration* Schranken aufzuerlegen sind. Einen konkreten Vorschlag wage ich beim gegenwärtigen Stand der Diskussion nicht zu machen.

Wiederholt ist sodann darauf hingewiesen worden, dass bei personenbezogenen Daten der *Empfänger* von Bedeutung ist[110]. Diesem Umstand ist Rechnung zu tragen, indem eine Weitergabe von Personendaten nur zu gestatten ist, wenn und soweit der Betroffene damit einverstanden ist oder rechnen muss.

104 Vgl. auch Auernhammer, zit. Anm. 2, S. 71.
105 Vgl. dazu Simitis, Schwierigkeiten, zit. Anm. 3, S. 4 f.; Mallmann, zit. Anm. 2, passim.
106 § 45 BDSG.
107 Vgl. auch Rausch, zit. Anm. 3.
108 Der deutsche Gesetzgeber hat den umgekehrten Ansatz gewählt: Gemäss § 3 I ist die Verarbeitung personenbezogener Daten nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat. Ebenso der Vorschlag von Burnand, zit. Anm. 3, no. 216 ff.
109 Vgl. Forstmoser, zit. Anm. 3, S. 223. Für ein Verbot unter Vorbehalt öffentlicher Interessen die parlamentarische Initiative Gerwig, zit. Anm. 18, Ziff. 7.
110 Vgl. vorn S. 35.

Für den *staatlichen Bereich* wäre sodann eine Art *Gewaltenteilung* vorzusehen[111], wonach jedes Organ nur die Daten erhalten und verarbeiten darf, die es legitimerweise zur Erfüllung seiner Aufgaben benötigt[112].

3. Besondere Berufsgeheimnisse?

Im öffentlichen Bereich bietet das *Amtsgeheimnis* Schutz vor der unerwünschten Weitergabe personenbezogener Information[113].

Für den privaten Bereich müsste dagegen ein besonderes *Berufsgeheimnis* für die mit der Verarbeitung personenbezogener Information Beschäftigten oder allgemein für die datenverarbeitenden Berufe ins Auge gefasst werden[114]. Ein Anfang wurde 1971 bei der Revision des Bankengesetzes gemacht: Das Bankgeheimnis soll nach neuer Formulierung Anwendung finden nicht nur auf Organe und Angestellte von Banken, sondern auch auf "Beauftragte"[115]. Diese Formulierung wurde bewusst gewählt, um die Datenverarbeitung ausser Haus durch Banken einzubeziehen.

4. Pflicht zur Datenrichtigkeit

Unrichtige und unvollständige Personeninformationen können schwerwiegende Folgen haben. Es ist daher zu verlangen, dass Personendaten *richtig*[116] und *vollständig* sind[117].

Richtigkeit und vor allem Vollständigkeit lassen sich freilich nie absolut realisieren. Zu berücksichtigen ist auch, dass die zumutbaren Anforderungen je nach Art der Information unterschiedlich sind. Die gesetzliche Lösung sollte daher flexibel sein: Zu verlangen ist die *den Umständen und insbesondere der Art der Information angemessene Sorgfalt.* Eine solche der schweizerischen Gesetzestradition entsprechende[118] Formulierung würde es ermöglichen, dem Einzelfall Rechnung zu

111 Vgl. Hansjörg Geiger, Datenschutz und Gewaltenteilung, S. 173 ff.; Klaus Lenk, Datenschutz in der öffentlichen Verwaltung, S. 15 ff., 23; beide in: Kilian/Lenk/Steinmüller, Datenschutz, Frankfurt a.M. 1973.

112 Eine solche ergibt sich übrigens schon aus geltendem Recht, vgl. vorn S. 38.

113 Vgl. vorn S. 38.

114 Ebenso die Initiative Gerwig, zit. Anm. 18, Ziff. 10; ferner die bei Forstmoser, zit. Anm. 3, S. 224, Anm. 57, aufgeführte Literatur.

115 Artikel 47 I Bankengesetz; zur analogen Problematik beim Arztgeheimnis vgl. Peter Forstmoser: EDV und Persönlichkeitsschutz, Das Schweizer Spital 39 (1975), S. 285 ff., 286.

116 Unrichtige Informationen verletzen das Persönlichkeitsrecht auch dann, wenn sie nicht ehrverletzend sind (vgl. Rausch, zit. Anm. 3).

117 Es muss sich niemand gefallen lassen, "dass von ihm ein Zerrbild geschaffen wird" (Rausch, zit. Anm. 3).

118 Vgl. etwa Art. 959 OR.

tragen, aber auch die Anforderungen dem technischen Fortschritt anzupassen, ohne dass das Gesetz revidiert werden müsste.

Kann verlangt werden, dass Personendaten *aktuell* sein und allenfalls à jour gehalten werden müssen? Ich möchte dies grundsätzlich verneinen, da dadurch der an sich legitimen und erwünschten Bearbeitung von Personendaten allzu grosse Schranken auferlegt würden. Doch könnte vielleicht gefordert werden, dass bei der Weitergabe personenbezogener Information jeweils der *Stand der Bearbeitung* mitgeteilt wird[119].

Besondere Probleme stellen sodann nicht objektivierbare, auf einem *subjektiven Werturteil* beruhende Angaben. Der Gesetzgeber kann hier wohl keinen spezifischen Schutz gewähren, es sei denn, er verbiete die Verarbeitung solcher Daten schlechthin. Eine solche Extremlösung könnte höchstens für abgegrenzte Teilbereiche in Betracht gezogen werden.

5. Pflicht zur Datensicherung

Zu verlangen ist, dass personenbezogene Daten durch angemessene *technische und organisatorische Massnahmen* vor Entwendung, Verstümmelung und Missbrauch *geschützt* werden[120, 121]. Wiederum ist einer flexiblen gesetzlichen Umschreibung, die auf technische Einzelheiten verzichtet, der Vorzug zu geben: Wer eine Personendatenbank führt, ist zu verpflichten, angemessene *Sicherungsmassnahmen nach anerkannten Grundsätzen und entsprechend dem jeweiligen Stand der Technik* vorzusehen[122].

6. Exkurs: Rechtfertigungsgründe

Die Pflicht zur Einhaltung gesetzlicher Vorschriften kann durch besondere Rechtfertigungsgründe[123] entfallen. Als solche kommt neben überwiegenden öffentlichen

119 Vgl. auch Lehmann, zit. Anm. 3, S. VII.

120 Ebenso Initiative Gerwig, zit. Anm. 18, Ziff. 8; Simitis, Schwierigkeiten, zit. Anm. 3, S. 1; ausführlich Lehmann, zit. Anm. 3, S. 6 ff. und Jochen Schneider, Technische Möglichkeiten des Datenschutzes, in: Kilian/Lenk/Steinmüller, zit. Anm. 107, S. 223 ff.; ferner die bei Forstmoser, zit. Anm. 3, S. 224, Anm. 62, aufgeführten Autoren.

121 Ferner muss ein Datenschutzgesetz die Dauer der Datenaufbewahrung regeln, um zu verhindern, dass die für die Auskunftserteilung notwendigen Daten zu früh gelöscht werden. Es könnte hier eine Lösung analog Art. 962 OR (Aufbewahrung der Geschäftsbücher) – freilich vielleicht mit anderen Fristen – getroffen werden.

122 Vgl. Art. 959 OR.

123 Vgl. dazu allgemein Karl Oftinger, Schweizerisches Haftpflichtrecht I, 4. A. Zürich 1975, S. 134.

und privaten Interessen vor allem die *Einwilligung* des Betroffenen in Betracht. Doch ist – soll der Datenschutz nicht illusorisch werden – allfälligen Unterordnungsverhältnissen Rechnung zu tragen. Die Einwilligung sollte daher als Rechtfertigungsgrund nur zugelassen werden, wenn sie nicht durch ein rechtliches oder faktisches Abhängigkeitsverhältnis veranlasst wurde.

C. Die Kontrollstruktur

1. Möglichkeiten

Die Einhaltung der gesetzlichen Vorschriften ist durch eine angemessene Kontrolle zu überwachen. In Betracht zu ziehen sind dabei die *Individualkontrolle* durch die Betroffenen selbst, die *Selbstkontrolle* durch das datenverarbeitende Unternehmen und schliesslich die *Fremdkontrolle* besonders durch den Staat.

2. Individualkontrolle[124]

a. Übersicht

Eine Kontrolle durch den Betroffenen selbst setzt voraus, dass er überhaupt um die *Existenz* der Personendatenbank weiss, dass er *Auskunft* über die ihn betreffenden gespeicherten Daten erhält und dass er gegebenenfalls ihre *Berichtigung* oder Modifizierung verlangen kann[125].

b. Benachrichtigungspflicht bei der Speicherung?

In der Literatur[126] und in politischen Vorstössen[127] ist verschiedentlich verlangt worden, es müssten die betroffenen Personen bei der ersten Speicherung benach-

124 Verstanden als Kontrolle durch den einzelnen; demgegenüber "Selbstkontrolle" als Kontrolle durch den Datenbankinhaber. (Die Terminologie ist nicht einheitlich.)

125 Vgl. z.B. Burnand, zit. Anm. 3, no. 278 ff.; Auernhammer, zit. Anm. 2, S. 68 ff.

126 Vgl. z.B. Burnand no. 290, 293; Schucan, Diss, S. 75, 78; ders., Vorbereitung, S. 683; Egloff, S. 361 f. und Lehmann, S. VII, alle zit. Anm. 3; letzterer mit praktischen Vorschlägen zur Erfüllung dieser Pflicht. Weitergehend Simitis, zit. Anm. 21, S. 681, der eine Benachrichtigung "in regelmässig wiederkehrenden Abständen" fordert. Vgl. ferner die bei Forstmoser, zit. Anm. 3, S. 224, Anm. 53, aufgeführte Literatur.

127 Vgl. Initiative Gerwig, zit. Anm. 18, Ziff. 6.

richtigt werden. In ausländischen Gesetzen findet sich eine generelle Benachrichtigungspflicht, z.B. im Bundesdatenschutzgesetz für im nicht öffentlichen Bereich verarbeitete Daten[128], während im übrigen eine Benachrichtigungspflicht lediglich für einzelne Fälle[129] vorgesehen ist.

Persönlich stehe ich einer allgemeinen Pflicht zur Benachrichtigung eher skeptisch gegenüber, und zwar nicht nur wegen der damit verbundenen Umtriebe, sondern auch, weil gerade durch diese Mitteilung personenbezogene Informationen Dritten zur Kenntnis kommen könnten. Die Benachrichtigung widerspricht – so scheint mir – dem Postulat nach Datensicherheit[130].

Ich würde es daher vorziehen, den Bestand von Datenbanken offenzulegen[131], und es im übrigen dem Betroffenen zumuten, sich zu erkundigen.

c. *Auskunftsrecht*

Dagegen müsste dem Betroffenen auf Antrag hin[132] *Auskunft über die zu seiner Person gespeicherten Daten* erteilt werden[133].

Dieses *Auskunfts- oder Einsichtsrecht* dürfte dem Grundsatz nach unbestritten sein. Seine Konkretisierung und allfällige *Limitierung* dagegen ist ein Kardinalproblem künftiger Gesetzgebung, das in der politischen Auseinandersetzung im Mittelpunkt stehen wird. Worüber ist im einzelnen Auskunft zu erteilen? Nur über die gespeicherten Daten oder auch über deren Herkunft bzw. über ihre Weitergabe? Und vor allem: Welche überwiegenden öffentlichen oder privaten Interessen stehen dem Recht auf Auskunft entgegen[134, 135]? Mit einer allgemeinen Formulierung ist es hier kaum getan. Vielmehr sollte ein möglichst *präziser Negativkatalog* aufgestellt werden – eine Aufgabe, bei der die gegensätzlichen Interessen und Ansichten zweifellos aufeinanderprallen werden.

128 Vgl. §§ 26 I und 34 I.

129 So § 606 Fair Credit Reporting Act, zit. Anm. 5: Danach ist der Betroffene darüber zu benachrichtigen, dass über ihn ein "investigative report", d.h. ein Bericht aufgrund von Interviews, erstellt worden ist.

130 Durchaus zweckmässig wäre dagegen eine entsprechende Pflicht für Teilbereiche. So könnte etwa ein Hinweis auf die vorgesehene Speicherung und Verarbeitung zwingend vorgeschrieben werden für Formulare, die vom Betroffenen selbst auszufüllen sind.

131 Dazu hinten S. 53 f.

132 Die Auskunftserteilung erfolgt sinnvollerweise nur auf Antrag; ebenso Schucan, Diss, S. 93; ders., Vorbereitung, S. 684, beides zit. Anm. 3.

133 Ebenso § 13 I BDSG. Aus der Literatur vgl. Schucan, Diss, S. 80 ff., Egloff, S. 361 und Burnand no. 281, alle zit. Anm. 3; ferner die bei Forstmoser, zit. Anm. 3, S. 224, Anm. 52, angeführte Literatur.

134 Vgl. dazu Schucan, Diss, zit. Anm. 3, S. 88 ff.

135 In diesem Zusammenhang ist auch darauf hinzuweisen, dass – im Gegensatz zu Schweden – das schweizerische Verwaltungsrecht kein generelles Einsichtsrecht kennt; ein Einsichtsrecht besteht nur soweit, als es gesetzlich vorgeschrieben ist oder sich aus Art. 4 Bundesverfassung ergibt (so Schucan, Diss, S. 7 f.; ferner Burnand, no. 245, beide zit. Anm. 3).

Weniger brisant ist die Frage, wer die *Kosten* der Auskunfterteilung zu tragen hätte[136]. Meines Erachtens ist es durchaus zumutbar, dem Betroffenen eine angemessene Bearbeitungsgebühr – beschränkt auf den direkten Aufwand für die Beantwortung und ohne Zuschlag für Gemeinkosten – aufzuerlegen[137].

d. Berichtigungs-, Löschungs- und Gegendarstellungsrecht, Recht auf Sperrung

Es versteht sich von selbst, dass dem Betroffenen ein Recht auf *Berichtigung* unrichtiger und auf *Löschung* ungesetzlich gespeicherter Daten zustehen muss[138,139,140]. Bei nicht objektivierbaren Angaben müsste aber vielleicht auch eine Art *Gegendarstellungsrecht* ins Auge gefasst werden. Ferner wäre – im Sinne einer vorsorglichen Massnahme für den Zeitraum der Abklärung – ein Recht auf *Sperrung*[141] vorzusehen.

3. Selbstkontrolle

Im Rahmen des Datenschutzes wird die Selbstkontrolle der eine Datenbank führenden Unternehmen zwar nicht die ausschliessliche, aber eine wichtige Rolle spielen. Zu diskutieren sind zwei Elemente:

a. Registrierung der Verarbeitung und der Zugriffsstruktur

Zunächst ist – damit allfällige Rechtsverletzungen überhaupt festgestellt und rückgängig gemacht werden können – über die Behandlung von Personeninformationen Buch zu führen[142]. Die Zugriffsstruktur[143] muss klar geordnet sein; Einspeicherun-

136 Burnand, zit. Anm. 3, no. 292 f.

137 Nach Lehmann, zit. Anm. 3, S. VII, könnten dem Auskunftsteller Kosten von Fr. 4.– bis 7.– überbunden werden. – Vgl. auch Schucan, Diss, zit. Anm. 3, S. 94 ff.

138 Vgl. statt vieler Lehmann, zit. Anm. 3, S. VII, ferner die bei Forstmoser, zit. Anm. 3, S. 224, Anm. 54, aufgeführten Autoren.

139 Und zwar kostenfrei (so auch Lehmann, zit. Anm. 3, S. VII).

140 Die Tatsache, dass eine Information berichtigt werden musste, ist vom Datenbankinhaber wohl an alle bekannten Empfänger der unrichtigen Information zu melden, soweit der Betroffene daran ein rechtliches Interesse hat (so Schucan, Diss, zit. Anm. 3, S. 102). Vgl. aber zu den praktischen Schranken hinten S. 55.

141 Das BDSG hat eine Sperrung personenbezogener Daten vorgesehen, wenn die "Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt" (§ 14 II S. 1). – Das Institut der Sperrung eignet sich auch für Daten, die der Datenbankinhaber nicht mehr benötigt, wenn deren Löschung für den Betroffenen nachteilig wäre (vgl. dazu Schucan, Diss, zit. Anm. 3, S. 108 f.).

142 Vgl. z.B. Seidel, zit. Anm. 2, S. 174 f.; Schucan, Diss, zit. Anm. 3, S. 86; Lehmann, zit. Anm. 3, S. VII.

143 D.h. der Kreis der zum Zugriff Berechtigten.

gen und Mutationen sind zu protokollieren, ausnahmsweise und unter bestimmten Voraussetzungen[144] auch die einzelne Abfrage. Die Registrierung mag ein erheblicher Aufwand sein, dürfte aber mehr und mehr ohnehin zu den Grundsätzen einer ordnungsgemässen Datenverarbeitung gehören[145].

b. *"Inspektorat" oder "Kontrollstelle"*

Sollen ausserdem besondere Kontrollorgane zwingend vorgeschrieben werden? In Betracht zu ziehen wären – im Anschluss an die Vorschläge in der Literatur und der ausländischen Praxis[146] – zwei Möglichkeiten: die des unternehmens*internen Datenschutzbeauftragten* (des "Inspektorats") oder die der *externen Datenrevisionsstelle.*

Das deutsche Recht sieht für private Datenbanken, die "mindestens fünf Arbeitnehmer ständig beschäftigen", die Bestellung eines *Beauftragten für den Datenschutz* zwingend vor[147]. Qualifizierung und Funktion dieses Datenschutzbeauftragten haben in den letzten Monaten zu zahlreichen Diskussionen geführt[148] und dürften wohl erst durch die künftige Praxis geklärt werden.

Für die Schweiz ist wohl das Konzept einer *externen Datenrevisionsstelle* vorzuziehen[149]. Ihre Aufgabe wäre wie die der aktienrechtlichen Kontrollstelle zu umschreiben, d.h. sie hätte die Gesetzmässigkeit – nicht aber die Zweckmässigkeit – der Verarbeitung personenbezogener Daten periodisch zu prüfen und darüber Bericht zu erstatten.

Da die aktienrechtlichen Kontrollstellen grösserer Unternehmen heute ohnehin über die nötigen EDV-Kenntnisse verfügen, sollte es zulässig sein und wäre es sogar wünschbar, wenn diese Aufgabe der gesellschaftsrechtlichen Kontrollstelle übertragen werden könnte. Damit dürften sich auch die Kosten in einem vernünftigen Rahmen halten.

144 Die Registrierung jedes einzelnen Zugriffs wäre weder zumutbar noch tunlich: Sie würde bei Banken mit häufigen Abfragen – man denke etwa an den Auskunftsdienst der Telefonbetriebe – zu unzähligen und völlig unüberblickbaren Aufzeichnungen führen. Auch bei der Protokollierungspflicht ist demnach zu differenzieren. Protokolliert werden müsste etwa der Zugriff durch Personen ausserhalb des autorisierten Benützerkreises, ferner der Zugriff auf Intimdaten.

145 Vgl. auch Lehmann, zit. Anm. 3, S. VII.

146 §§ 28 f., 38 BDSG.

147 §§ 28, 26 BDSG. – Dieser betriebliche Datenschutzbeauftragte hat generell für die Beachtung des BDSG und anderer Datenschutzvorschriften Sorge zu tragen (§ 29). Vgl. auch Gerhard Hergenhahn: Die Aufgaben eines betrieblichen Datenschutzbeauftragten, IBM-Nachrichten 25 (1975), S. 240 ff.

148 Vgl. z.B. Bergmann/Möhrle, zit. Anm. 2, § 28 Anm. 2.

149 Von der zwingenden Einführung eines Datenschutzbeauftragten wäre dagegen abzusehen, da es – wie in anderen Rechtsbereichen auch – Sache der Unternehmen bleiben sollte zu entscheiden, wie eine gesetzlich vorgegebene Aufgabe (hier: die ordnungsgemässe Datenverarbeitung) administrativ zu lösen ist; anderer Auffassung offenbar Egloff, zit. Anm. 3, S. 362.

4. Fremdkontrolle und Publizität[150]

a. *Kontrolle durch die Gerichte*

Wie allgemein im Persönlichkeitsschutz so wird auch im Hinblick auf den Schutz vor Datenbanken eine Kontrolle in erster Linie *durch die Gerichte auf Klage der Betroffenen hin* ausgeübt werden.

Grundsätzlich ergeben sich hier keine Besonderheiten. Fragen könnte sich höchstens, ob man *besondere Klagerechte* (etwa von Konsumentenverbänden oder anderen Organisationen[151]) vorsehen sollte.

b. *Konzessions- oder Bewilligungspflicht?*

Abzulehnen und mit unserer liberalen Rechtsordnung unvereinbar wäre es, den Betrieb einer Personendatenbank *konzessionspflichtig* zu machen, es also in das mehr oder minder grosse Ermessen einer Behörde zu stellen, den Betrieb im Einzelfall zu erlauben.

Dagegen wäre es möglich, die *Bewilligung zum Betrieb* – in Analogie zur Gründung von Körperschaften – von der Erfüllung gewisser gesetzlicher *Minimalanforderungen abhängig zu machen.* Eine staatliche Kontrollinstanz hätte dann – ähnlich den Handelsregisterbehörden bei der Gründung von Gesellschaften – summarisch und primär formell zu prüfen, ob den gesetzlichen Vorschriften nachgelebt wurde, ob also zum Beispiel die allenfalls erforderliche "Datenrevisionsstelle" bestellt wurde.

Für kurante und vom Persönlichkeitsschutz her relativ problemlose Datenbanken könnte auch von einer Bewilligungspflicht abgesehen und lediglich die *Anmeldung* und Bekanntgabe gewisser Minimalangaben[152] verlangt werden – eine Lösung, die im Handelsrecht bekanntlich für die Personengesellschaften[153] verwirklicht ist.

c. *Datenbankenregister, Publikation von Personendatenbanken in öffentlichen Blättern?*

Lehnt man eine Pflicht zur Benachrichtigung der Betroffenen ab[154], dann muss auf andere Weise dafür gesorgt werden, dass der einzelne überhaupt in Erfahrung brin-

150 Zusammenfassende Darstellung der verschiedenen Systeme der Fremdkontrolle z.B. bei Burnand, zit. Anm. 3, no. 256 ff.

151 Ähnlich Art. 2 III des Bundesgesetzes über den unlauteren Wettbewerb.

152 Z.B. Identität des Datenbankhalters, Art der geführten Datenbanken, Angabe, ob Verarbeitung für eigenen internen Gebrauch oder zur Weitergabe an Dritte (diesfalls auch Kreis der üblichen Empfänger).

153 Kaufmännische Kollektiv- und Kommanditgesellschaft.

154 Vgl. vorn S. 49 f.

gen kann, ob und welche Personendatenbanken bestehen. Angemessenes Mittel hiezu wäre ein *Datenbankenregister*[155], das öffentlich wäre und dem gewisse minimale Informationen über Personendatenbanken[156] entnommen werden könnten[157]. Als Vorbild könnte das Handelsregister dienen, dem ein Datenbankenregister vielleicht sogar angegliedert werden könnte[158].

Im Interesse der Übersichtlichkeit wäre für jedes Unternehmen nur *eine* Registrierung vorzusehen, auch wenn mehrere Personendatenbanken nebeneinander geführt werden.

Ob – analog der Veröffentlichung im schweizerischen Handelsamtsblatt – die Errichtung einer Personendatenbank ausserdem in *öffentlichen Blättern publiziert* werden sollte[159], möchte ich eher verneinen[160] [161].

d. Datenschutzamt oder Datenombudsman?

Ein besonderes staatliches *Datenschutzamt* dürfte sich in der Schweiz – zumindest vorderhand – erübrigen[162].

Dagegen wäre für den öffentlichen Bereich ein *Datenombudsman*, der vor allem vermittelnd und schlichtend wirken sollte, zu befürworten[163]. Entsprechende Erfahrungen aus Deutschland sind ermutigend[164]. Für den privaten Bereich sollte die freiwillige Einsetzung eines Ombudsmans – etwa für Kreditauskunfteien, Kleinkreditinstitute oder andere Organisationen – geprüft werden[165].

155 Vgl. neben den bei Forstmoser, zit. Anm. 3, S. 224, Anm. 63, aufgeführten Autoren Burnand, zit. Anm. 3, no. 273 f. und Rausch, zit. Anm. 3.

156 Etwa Art der gespeicherten Daten und Zweck der Verarbeitung.

157 Ebenso die Initiative Gerwig, zit. Anm. 18, Ziff. 3.

158 Ausführlich Schucan, Diss, zit. Anm. 3, S. 70 ff.

159 So sieht z.B. § 13 des österreichischen Entwurfes die jährliche Publikation des Verzeichnisses sämtlicher Datenbanken vor.

160 Ebenfalls kritisch Schucan, Diss, S. 70, wohl noch bejahend Vorbereitung S. 683 (beides zit. Anm. 3).

161 In diesem Zusammenhang ist auch das quantitative Problem zu erwähnen: In Schweden z.B. sprach man anlässlich der Gesetzgebungsarbeiten von etwa 5'000 anmeldepflichtigen Datenbanken. Tatsächlich wurden bis heute schon ca. 20'000 Anmeldungen vorgenommen, wobei noch nicht alle Datenbanken angemeldet sind. Ferner besitzen z.B. allein die Bundesbehörten der USA ca. 7'500 Datenbanken.

162 Anderer Meinung Burnand, zit. Anm. 3, no. 266, der ein fünfzehnköpfiges "Commissariat fédéral de l'informatique" fordert. Dieses hätte den Vollzug des Datenschutzgesetzes zu überwachen.

Freilich wird man ohne eine zusätzliche Behörde bzw. ohne die Erweiterung von Kompetenzen bestehender Ämter nicht auskommen, wenn man – wie es hier vorgeschlagen wird – die Offenlegung der Verhältnisse in erster Linie durch ein Datenbankregister anstrebt. Die Aufgaben und Kompetenzen der Registerbehörden gingen aber weniger weit als diejenigen, die einem eigentlichen Datenschutzamt nach den in der Literatur geäusserten Vorstellungen zukämen.

163 Aus der Literatur statt vieler Seidel, zit. Anm. 2, S. 182 f. – Hessen kennt seit 1970 einen Datenschutzbeauftragten (§§ 7 ff. des hessischen Datenschutzgesetzes).

164 Vgl. 5. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten, Hessische Landestags-Drucksache 8/2475.

165 Näher zu prüfen wäre vielleicht auch die Einführung einer *nebenamtlich tätigen Kommis-*

D. Sanktionen

1. Berichtigungs- und Löschungspflicht

Es versteht sich von selbst, dass eine unrichtige Angabe zu berichtigen, eine widerrechtlich gespeicherte zu löschen ist[166]. Wünschbar wäre es, die Berichtigung und Löschung auch denjenigen mitzuteilen, an die unrichtige oder ungesetzlich gespeicherte Informationen weitergeleitet worden sind[167]. Dies ist aber nur soweit möglich, als die Weitergabe registriert worden ist, was die Ausnahme sein dürfte.

2. Wiedergutmachung (Schadenersatz und Genugtuung)

Ist durch rechtswidrige Speicherung, Verarbeitung oder Weitergabe personenbezogener Daten dem Betroffenen *Schaden* erwachsen, so ist dieser zu *ersetzen.* Überwiegend wird die Einführung einer *Kausalhaftung* im Sinne einer Gefährdungshaftung postuliert, da Personendatenbanken für die Betroffenen eine besondere Gefahr darstellten[168].

Schaden ist nach schweizerischem Recht stets Vermögensschaden[169]. Aus Verletzungen der Privatsphäre wird jedoch häufig nicht Schaden im Sinne eines materiellen Verlustes resultieren, sondern *immaterielle Unbill.* Diese ist durch *Genugtuung* abzugelten. Für den Schutz gegenüber Personendatenbanken dürfte sich dabei eine besondere Regelung aufdrängen: Nach allgemeinen Rechtsgrundsätzen ist eine Genugtuung nur geschuldet, wenn sowohl die erlittene Verletzung wie auch das *Verschulden* des Verletzers *besonders schwer* wiegen[170]. Für erhebliche Persönlichkeitsverletzungen im Rahmen der Datenverarbeitung wäre dagegen eine *Genugtuung auch bei leichtem Verschulden,* vielleicht sogar *unabhängig vom Verschulden*[171] des Verletzers zu diskutieren.

sion, welche die Entwicklung zu verfolgen, Berichte über den Stand der Praxis, Richtlinien zur Behandlung offener Fragen und Empfehlungen für die Fortentwicklung dieses Rechtszweiges auszuarbeiten hätte.

166 Lehmann, S. VII; Schucan, Diss, S. 99, beide zit. Anm. 3.

167 Gleicher Meinung Schucan, Diss, zit. Anm. 3, S. 102; vgl. auch vorn Anm. 140.

168 Vgl. Burnand, zit. Anm. 3, no. 300; Simitis, Schwierigkeiten, zit. Anm. 3, S. 8; ebenfalls eine Kausalhaftung sieht der Entwurf Lüchinger (vgl. Anm. 17) in OR 49bis III vor. Immerhin ist darauf hinzuweisen, dass der Einsatz moderner technischer Mittel wirkungsvollere Sicherungsvorkehren ermöglicht als die, welche bei konventioneller Bearbeitung möglich waren. Insofern erscheint die Einführung einer Kausalhaftung als nicht unproblematisch, führt sie doch in Verbindung mit einer gesetzlichen Verpflichtung zu Sicherungsmassnahmen (dazu vorn S. 48) zu einer doppelten Verschärfung gegenüber dem heutigen Zustand.

169 Vgl. Oftinger, zit. Anm. 123, S. 53 f.

170 OR 49. – Vgl. BGE 101 II 199 E 6c; Grossen, Recht der Einzelpersonen, zit. Anm. 33, S. 360 (mit weiterer Judikatur); Tuor/Schnyder: Das Schweizerische ZGB (9.A. Zürich 1975), S. 86.

171 So Simitis, Schwierigkeiten, zit. Anm. 3, S. 9.

Zu überlegen wäre sodann, ob das Risiko durch eine obligatorische *Haftpflichtversicherung* gedeckt werden müsste, wie es dem Wesen der Kausalhaftung entspricht[172].

Endlich fragt es sich, ob die Stellung des Betroffenen durch eine *Umkehr der Beweislast* verbessert werden sollte: Es wird nämlich in der Praxis oft fast unmöglich sein, den Nachweis des Kausalzusammenhangs zu erbringen, etwa darzutun, dass ein Kreditbegehren tatsächlich wegen einer falschen Auskunft und nicht aus andern Gründen abgelehnt wurde. Dem könnte Rechnung getragen werden, indem in solchen Fällen ein Sachzusammenhang von Gesetzes wegen vermutet würde, so dass der Schädiger den Gegenbeweis anzutreten hätte.

3. Strafrechtliche Sanktionen?

Strafrechtlich zu ahnden wäre die Verletzung von *Berufsgeheimnissen.* Darüber hinaus sollte in der Einführung von Strafnormen Zurückhaltung geübt werden, da sich eine extreme Pönalisierung nur negativ auswirken kann[173, 174].

4. Verwaltungsrechtliche Sanktionen

Mit Bezug auf private Datenbanken könnte – bei wiederholten und schwerwiegenden Verletzungen – ein *Bewilligungsentzug,* verbunden mit der Pflicht zur Auflösung der Datenbank[175], vorgesehen werden. Wiederum könnte sich der Gesetzgeber an der geltenden Ordnung im Handelsregisterrecht orientieren.

Im öffentlichen Bereich kämen die allgemeinen *beamtenrechtlichen Sanktionen* sowie die allfällige *Staatshaftung* zum Zug. Besondere Vorkehren für Personendatenbanken drängen sich nicht auf.

172 Vgl. Lehmann, zit. Anm. 3, S. VII; allgemein Oftinger, zit. Anm. 123, S. 40.

173 Für eine umfassende strafrechtliche Regelung Burnand, no. 298, ferner Egloff, S. 362, beide zit. Anm. 3; vgl. auch Lehmann, zit. Anm. 3, S. VII.

174 Immerhin wären wohl Ordnungsstrafen vorzusehen etwa für Rechtsverletzungen hinsichtlich der Registrierung von Datenbanken, der Meldepflichten, der Einsichtsrechtsgewährung usw. Ferner sollten wohl der unerlaubte Zugriff und das unerlaubte Kopieren, die nicht autorisierte Mitbenützung von Anlagen und ähnliches unter Strafe gestellt werden.

175 Nach § 22 des schwedischen Datalagen muss eine ohne Bewilligung betriebene Datenbank vernichtet werden.

V. Schlussbetrachtungen

Ich habe versucht, die möglichen Elemente eines Datenschutzgesetzes *vollständig* und *umfassend* aufzuzeigen, unter Einbezug der im Ausland realisierten wie der in Literatur und rechtspolitischer Diskussion vorgeschlagenen Instrumente. Dadurch ist vielleicht – zu Unrecht – der Eindruck entstanden, ich spreche einer umfassenden und perfekten *Maximalordnung* das Wort. Es seien daher abschliessend die Grundsätze zusammengefasst, an denen sich der Gesetzgeber nach meiner Ansicht bei der Entwicklung einer Datenschutzgesetzgebung zu orientieren hätte:

- Anzustreben ist nicht die "beste aller Welten", kein alle irgendwie denkbaren Gefährdungen erfassendes Supergesetz, sondern eine *praktikable und möglichst einfache Ordnung,* die den heute bekannten oder voraussehbaren Missbräuchen steuert. Die skizzierten Möglichkeiten des Datenschutzes wären daher nicht einfach zu kumulieren. Vielmehr wäre eine *vernünftige Auswahl und Kombination* zu treffen[176].
- Eine Datenschutzgesetzgebung hat naturgemäss zum Ziel, die Datenverarbeitung zu *beschränken.* Doch ist stets im Auge zu behalten, dass die Verarbeitung personenbezogener Daten grundsätzlich *legitimen Interessen dient und wünschbar ist.* Es ist daher die Möglichkeit der Informationsverarbeitung zu gewährleisten, zugleich aber die Privatsphäre zu schützen durch Offenlegung der Verhältnisse und eine Reihe weiterer spezifischer gesetzlicher Schutzvorkehren.
- Die möglichen Elemente eines künftigen Gesetzes sind durch *Gesetzgebung und Gesetzesentwürfe des Auslands* weitgehend vorgegeben. Vor einer unkritischen Übernahme und Kopie ist jedoch zu warnen: Im Bereich des Persönlichkeitsschutzes ist *nationalen Besonderheiten* Rechnung zu tragen, hat jeder Rechtskreis besondere Probleme. Auch ist man im Ausland – so scheint mir – bis heute zu sehr von dogmatischen Konzepten ausgegangen und wurden die Realien zu wenig geklärt[177]. In der Schweiz sollte dagegen eine gründliche *Erforschung der Rechtstatsachen* ebensosehr Grundlage der Gesetzgebung sein wie die theoretische Auseinandersetzung.
- Ein künftiges Gesetz soll *flexibel* genug sein, um Raum für die *Rechtsfortbildung durch den Richter* zu lassen. Das Gesetz darf auch nicht durch eine allzu detaillierte Ordnung auf den heutigen Stand der Technik festgelegt werden. Vielmehr soll es eine *Berücksichtigung künftiger technischer Entwicklungen* ermöglichen.

176 Was den Umfang eines Datenschutzgesetzes betrifft, könnten vielleicht das die Persönlichkeit im Wirtschaftsleben schützende Bundesgesetz über den unlauteren Wettbewerb mit 23, allenfalls auch das Kartellgesetz mit ebenfalls 23 Artikeln als Richtschnur dienen.

177 Vgl. das vorn Anm. 161 angeführte Beispiel.

- Ist die *Zeit für eine Datenschutzgesetzgebung überhaupt gekommen?* Kritiker werden dies bezweifeln mit dem Hinweis darauf, dass im Bereich der Verarbeitung von Personendaten keine unhaltbaren Zustände herrschen und keine grossen Skandale zu registrieren sind. Gerade dies ist aber nach meiner Auffassung Grund genug, um die Gesetzgebungsarbeit zu beginnen: Datenschutz ist eine Materie, die emotional anspricht und sich für demagogische Übersteigerungen eignet. Es ist daher Sorge zu tragen, dass die Arbeit *nüchtern an die Hand genommen wird,* nicht im Affekt und unter dem Eindruck hochgespielter Missstände.
- Immer ist zu beachten, dass Datenschutz *Ausgleich legitimer Interessen* – der Interessen des einzelnen an seiner Privatsphäre und der Dritter an personenbezogener Information – bedeutet[178]. Als Richtschnur können dabei die folgenden Ausführungen des Bundesgerichts dienen:

> "Ein Schutz der Privatsphäre ist nur möglich, wenn das Informationsbedürfnis der Öffentlichkeit grundsätzlich hinter dem Anspruch des einzelnen, für sich sein zu können, zurücktreten muss ... Nur ein besonders gewichtiges Interesse an Information darf daher höher bewertet werden als der Anspruch auf ein ungestörtes Privatleben."[179]

Im Zweifel ist daher stets dem Schutz der *Persönlichkeit der Vorrang zu geben.*

178 Weitere Problemkreise, die Gegenstand eigener Untersuchungen sein müssten, seien angedeutet mit den Schlagwörtern "Informationsgleichgewicht" und "Informationsinteresse der Öffentlichkeit".

179 BGE 97 II 105.