Kurzfassung

Erfahrungen zum Datenschutz 1980 - 1998

Autoren: Hans G. Zeger, Ute Verena Widerin, Dieter Kronegger

Aus Gründen der flüssigeren und besseren Lesbarkeit wurde im folgenden Text auf die explizite Anführung von weiblichen und männlichen Formen verzichtet und ausschließlich die männliche Form verwendet. Diese ist als geschlechtsneutral zu beurteilen und steht für beide Geschlechter in gleicher Weise.

Studie im Auftrag des Bundesministeriums für Wissenschaft und Verkehr,
Wien 1998 - 1999, Projektleitung: Hans G. Zeger

Rückmeldungen und Kommentare schicken Sie bitte an hans.zeger@adis.at

Die komplette Studie kann zum Preis von ATS 2.700,- + Ust. bei der ARGE DATEN bestellt werden:
ARGE DATEN, A-1170 Wien, Sautergasse 20,
Tel.: +43/1/4897893, Fax: +43/1/4897893-10
Online: http://www.argedaten.at/studie/dsg80-98

Inhaltsverzeichnis

I. Einleitung

Die Studie analysiert - aus dem Blickwinkel der Betroffenen - die Erfahrungen mit dem österreichischen Datenschutzgesetz. Schwerpunkt war dabei, einerseits die Bandbreite der Datenschutzprobleme auszuloten, andererseits eine Mengenabschätzung zu machen.

Es wurde versucht, die einzelnen Fälle zu systematisieren und bestimmten subjektiven Rechten zuzuordnen. Ausgangspunkt der Analyse war das "Recht auf informationelle Selbstbestimmung", also die Möglichkeit des Individuums weitgehend selbst zu entscheiden, wer in welchem Umfang Einblick in seine private Lebensführung nehmen darf.

Dieses allgemeine und im österreichischen Rechtssystem in dieser Form nicht verankerte Recht wurde in verschiedene Teilaspekte gegliedert. Die wichtigsten dieser Aspekte sind das Recht auf Geheimhaltung von Informationen, das Recht auf Auskunft, wer welche Informationen verarbeitet, das Recht, Informationen aktualisieren und verbessern zu lassen und eine Reihe weiterer Rechte, die es erlauben, abzuschätzen, ob ein Datenverarbeiter Informationen im Sinne und Interesse des Betroffenen verwaltet.

II. Umfang des Datenschutzproblems

Ein wesentlicher Teil der Studie war es, abzuschätzen, in welchem Umfang in Österreich tatsächlich Datenschutzprobleme auftreten. Dazu existieren - mehr als 20 Jahre nach Verabschiedung des Datenschutzgesetzes - bislang überhaupt keine Forschungen und Untersuchungen, und es mußten zum Teil völlig neue Bewertungsansätze gefunden werden.

Weder die Berichte der Datenschutzkommission (hier wurden bis zum 30. Juni 1997 1.175[1] Beschwerdefälle behandelt), noch die Zahl der Datenschutzprozesse (ca. 20 bis 30) ermöglichen eine sinnvolle Aussage über den tatsächlichen Umfang von Datenschutzverletzungen. Im ersten Fall wird ignoriert, daß die meisten Fälle der Datenschutzkommission einen erheblichen Verstärkungseffekt haben, das heißt in vielen Fällen wird zwar nur eine Entscheidung getroffen, betroffen sind aber mehrere tausend oder hunderttausend Personen, die sich in derselben Situation befinden.

In dieser Studie wurde erstmals versucht, den verschiedenen Datenschutzproblemen die Zahl der potentiell Betroffenen gegenüber zu stellen. Basis dieser Studie waren 1.663 Fälle, von denen 1.453 Fälle im Detail ausgewertet wurden. Als Quellen wurden die Aufzeichnungen des Vereins "ARGE DATEN - Österreichische Gesellschaft für Datenschutz", die Entscheidungen der Datenschutzkommission und der Gerichte, Medienberichte, parlamentarische Anfragen und Berichte aus der Fachliteratur herangezogen. Die Analyse wurde durch Recherchen über die Zahl der potentiell Betroffenen ergänzt. In vielen Fällen mußten die Autoren mangels Datenmaterials auf Hochrechnungen und Abschätzungen zurückgreifen.

Ein Ergebnis der Studie ist, daß die Auseinandersetzung mit Datenschutzproblemen, also die Bereitschaft einer Datenschutzverletzung nachzugehen, in den Städten wesentlich höher als im ländlichen Raum ist. In den Städten (Gemeinden ab 11.000 Einwohner) fallen in Relation zur Bevölkerungsverteilung rund sechsmal soviel Datenschutzfälle wie in den ländlichen Regionen an. Das Verhältnis erhöht sich auf 8:1, wenn als urbane Einheit Gemeinden ab 50.000 Einwohner angenommen werden.

Dies bedeutet nicht, daß es im urbanen Bereich mehr Datenschutzverletzungen gibt, sondern es legt den Schluß nahe, daß in den Städten Betroffene eher bereit sind, ihre Rechte wahrzunehmen und zu verfolgen. Darüber hinaus erwartet sich der Stadtbewohner eine erhöhte Respektierung seiner Privatsphäre und Anonymität.

Für Wien wurden rund 40 Fälle je 100.000 Einwohner (EW) dokumentiert, in Vorarlberg rund 17 Fälle je 100.000 EW, ansonsten liegen die Werte zwischen drei und sieben Fällen je 100.000 EW. Das Schlußlicht bildet das Burgenland mit weniger als einem Fall je 100.000 Einwohner.

Bundes- und Landesdienststellen stellen die bei weitem wichtigsten Datenverarbeiter dar, zu denen Datenschutzprobleme dokumentiert sind (45% der Fälle = 659 Fälle).

---

1 Diese Anzahl umfaßt die individuellen Beschwerden und die individuellen Ersuchen und Auskünfte. Quelle: Datenschutzbericht 1997 der DSK

Alle anderen Bereiche folgen mit großem Abstand, wobei folgende Bereiche von größerer Bedeutung sind: Finanzdienstleister 92 Fälle (6%), Adressenverlage 76 Fälle (5%), Vereine und Interessensvertretungen 76 Fälle (5%), Kammern und sonstige Körperschaften des öffentlichen Rechts 69 Fälle (5%).

Anhand von 18 exemplarischen und genau dokumentierten Datenschutzverletzungen wurde versucht, eine Abschätzung der Zahl der insgesamt betroffenen Personen zu machen. Schon diese relativ geringe Zahl von 18 analysierten Fällen zeigt, daß mehrere Millionen Menschen von Datenschutzverletzungen betroffen waren. Insgesamt kann davon ausgegangen werden, daß im Laufe der letzten 18 Jahre jeder Österreicher mit hoher Wahrscheinlichkeit mehrere Male von einer durch die DSK festgestellten Datenschutzverletzung direkt betroffen war.

Nachfolgende Tabelle zeigt eine Übersicht dieser exemplarischen Fälle:

Nr.	**Thema**	**betroffene Personengruppe**	**Betroffene**
1.	Übermittlung Maturantendaten an Bank	Schüler	1.200
2.	Kommerzielle Nutzung der Wählerevidenz	Wahlberechtigte	200.000
3.	Unzulässiger Datenabgleich der Wählerevidenz	Wahlberechtigte	90.000
4.	Übermittlung von Ärztedaten	Ärzte	1.600
5.	Übermittlung von Ärzteprivatadressen	Ärzte	12.000
6.	Übermittlung der Geheimnummer	Telefonteilnehmer	360.000
7.	Veraltete Gläubigerschutzdaten	Kontoinhaber Kreditnehmer	780.000
8.	Weitergabe von Gehaltsdaten	Landes- und Bundesbedienstete	120.000
9.	Weitergabe von Urlaubermeldedaten	Urlauber	500.000
10.	Fehlerhafte Arbeitslosendaten	arbeitssuchende Arbeitnehmer	1.500.000
11.	Übermittlung des religiösen Bekenntnisses	alle Bewohner	1.700.000
12.	Unzulässige Meldeerhebungen	alle Bewohner	85.000
13.	Fehlerhafte Meldedaten	alle Bewohner	1.600.000
14.	Unzulässige Berufserhebung	KFZ-Besitzer	40.800
15.	Übermittlung von Wohnungswerberdaten	Wohnungswerber	10.000
16.	Übermittlung von Arbeitnehmerdaten	Arbeitnehmer	50.000
17.	Datenerhebung bei Schülern	Schüler	90.000
18.	Irrtümlicher Eintrag in Verzeichnisse	alle Bewohner	70.000
	Summe		**7,210.600**

Weitere Eckdaten, die das Potential an Datenschutzverletzungen deutlich machen:

Fehlerhafte Adressen bei Directmails

Experten gehen von einer Retourenrate (fehlerhafte Adresse) von 2-10% aus. Bei 592 Millionen persönlich adressierten Massensendungen in Österreich sind dies 10 bis 60 Millionen fehlerhaft verarbeitete Datensätze pro Jahr.

Veröffentlichte Jubilare

Von rund 200.000 Personen werden jährlich (mit oder ohne deren Zustimmung) sogenannte freudige Ereignisse (Geburten, Taufen, Eheschließungen, Alters- und Ehejubiläen) in Zeitungen veröffentlicht. Diese Daten können zu unerwünschten Marketingaktivitäten genutzt werden.

Das Doppelgängerproblem

Die Gefahr, Daten von Doppelgängern zu vertauschen und irrtümlich zu verknüpfen, wird allgemein unterschätzt.
Eine Abschätzung für ganz Österreich (8,08 Millionen Einwohner) ergibt folgende Größenordnungen:

- mindestens 2,9 Millionen Personen haben einen Doppelgänger mit gleichem Familiennamen und gleichem Vornamen,
- mindestens 131.000 Personen haben einen Doppelgänger mit gleichem Familiennamen und gleichem Geburtsdatum,
- rund 1.600 Personen haben einen Doppelgänger mit gleichem Familiennamen, gleichem Vornamen und gleichem Geburtsdatum.

Nicht berücksichtigt wurden dabei Namensähnlichkeiten oder Schreibvarianten.

Einen Doppelgänger zu haben, ist daher ein relativ wahrscheinliches Ereignis und führt bei vielen nur oberflächlich geführten Datenverarbeitungen zu fehlerhaften Verknüpfungen von Daten verschiedener Personen.

Sonstige Fehler in Datenverarbeitungen

Versucht man auf der Basis eines durchschnittlichen Prozentsatzes von 5% fehlerhafter Datensätze eine Abschätzung zu machen, ergibt sich folgende Größenordnung an Fehlern: Derzeit sind rund 81.000 Datenverarbeiter mit insgesamt 293.000 Verarbeitungen offiziell registriert. Wenn als untere Grenze von durchschnittlich 10.000 Betroffenen pro Datenverarbeitung ausgegangen wird, ergibt dies rund 145.000.000 fehlerhafte personenbezogene Datensätze.

Personengruppen, die vom Datenmißbrauch besonders gefährdet sind

- Arbeitslose bzw. Arbeitssuchende
- Fremde, Gastarbeiter und Asylsuchende
- Sozialhilfe- und Notstandshilfeempfänger
- Empfänger von Subventionen und sonstigen Zuwendungen
- Wirtschaftstreibende (besonders Personen, die in Reklamationsverfahren verwickelt sind)
- Kreditnehmer
- Kranke
- Posteinkäufer (Käufer bei Versandhandelsunternehmen)
- Mobilkommunikationskunden
- Kundenkartenbenutzer (inkl. der Benutzer von Finanzdienstkarten, wie Bankomat oder Kreditkarten)

III. Durchsetzung der subjektiven Rechte

Neben den grundsätzlichen Schwierigkeiten, Datenschutzverletzungen als solche überhaupt zu erkennen, richtig zuzuordnen und dann zu verfolgen, bestehen auch einige praktische Hürden.

Ein Grund, Rechtsverletzungen nicht weiter zu verfolgen, können überlange und bürokratische Verfahren sein. Dies ist häufig im Zusammenhang mit der DSK der Fall. Die DSK sollte aufgrund des Verwaltungsverfahrensrechts spätestens nach sechs Monaten über Beschwerden entscheiden. Von 142 DSK-Entscheidungen standen das genaue Beginn- und Enddatum zur Verfügung. Die durchschnittliche Verfahrensdauer betrug 234 Tage (rund acht Monate), die längste dokumentierte Dauer 3½ Jahre (!). 55% der dokumentierten Verfahren dauerten länger als die maximal zulässige Verfahrensdauer von sechs Monaten.

Ein weiterer Grund für die geringe Zahl an Verfahren können hohe Kostenrisken sein. Ein durchschnittlicher Datenschutzprozeß, den ein Betroffener vor dem Landesgericht (1. Instanz) verliert, kostet den Betroffenen rund ATS 30.000,-. Umgekehrt kann der Betroffene bei Gewinn eines derartigen Verfahrens maximal mit der Feststellung rechnen, daß er eben Recht hatte.

Weiters sind eine Reihe von Bereichen nicht abgedeckt. Neben den fehlenden Regelungen zum Schutz gegen Datenschutzverletzungen im Bereich der Rechtssprechung (Gerichtsbarkeit) und der Rechtssetzung (Parlament) sind auch weitere Bereiche nicht geschützt, z. B. ist der Schutz vor der Anfertigung von Bildern und Videos nicht abgedeckt. Geschützt ist nur die Veröffentlichung, es gibt jedoch keinen Schutz gegen unerwünschtes Anfertigen sowohl im privaten als auch im öffentlichen Raum.

Die subjektiven Rechte könnten wesentlich ausgebaut werden. Insbesondere fehlen die vom Nationalrat schon im Zuge der Beschlußfassung zum DSG geforderten Schadenersatzansprüche für immaterielle Schäden.

IV. Bedeutung der Datenschutzregelungen in der österreichischen Rechtsordnung

Auf verfassungsrechtlicher Ebene ist festzustellen, daß der Verfassungsgerichtshof das Grundrecht auf Datenschutz nur sehr eingeschränkt anwendet. In Fällen, in denen der VfGH über einen Eingriff in die Privatsphäre zu entscheiden hat, zieht der VfGH eher das Recht auf Achtung des Privat- und Familienlebens (Art. 8 MRK) als den Geheimhaltungsanspruch des § 1 DSG heran. Nur in einer Entscheidung[2] wurde die Aufhebung einer einfachgesetzlichen Bestimmung auf § 1 DSG gestützt. – Dagegen hatte der VfGH zweimal[3] Bestimmungen des DSG selbst aufgehoben, wobei jeweils die schwer zu ziehende Trennlinie zwischen "öffentlichem" und "privatem" Bereich wesentlich für die festgestellten Verfassungswidrigkeiten war.

Auf einfachgesetzlicher Ebene existiert vor allem im öffentlichen Recht eine große Zahl von datenschutzrechtlichen Sonderbestimmungen. Einerseits ist dies zu begrüßen, da auch das DSG selbst vorsieht[4], daß die jeweiligen Materiengesetze ausdrückliche Ermächtigungen zur Ermittlung, Verarbeitung und Übermittlung der im jeweiligen Sachbereich benötigten Daten enthalten. Andererseits sind diese Ermächtigungen oft zu allgemein gehalten.

Spezifische gesetzliche Regelungen für die Rechtsträger des Privatrechts fehlen weitgehend. Insbesondere gibt es keine Bestimmungen für die Datenverbundsysteme der Versicherungen und Banken und für die Gläubigerschutzeinrichtungen.

Auf untergesetzlicher Ebene ist festzustellen, daß im öffentlichen Bereich Entscheidungen der Datenschutzkommission in vielen Fällen umgesetzt werden und zu organisatorischen Änderungen auch außerhalb des konkreten Einzelfalls bzw. der vor der DSK belangten Behörde führen. Die Rechtsprechung der DSK hat also zu einem gewissen Datenschutzbewußtsein geführt. Die Studie hat aber auch gezeigt, daß es Fälle gibt, in denen die DSK Verletzungen des Datenschutzes feststellt, ohne daß es zu einer Änderung der Verwaltungspraxis kommt. Es fehlt also eine Stelle, die den festgestellten Datenschutzverletzungen über den Einzelfall hinaus systematisch für alle Betroffenen und bei allen in Frage kommenden Behörden wirksam entgegentritt.

Im privaten Bereich ist das Datenschutzbewußtsein der Verantwortlichen wesentlich geringer. Zum einen existiert praktisch keine Rechtssprechung, zum anderen ist die Motivation, Urteile aus den wenigen Musterprozessen im eigenen Unternehmen umzusetzen, gering. Aufgrund des hohen Klagsrisikos für den Betroffenen riskiert ein Unternehmen wenig, wenn es die Erfahrungen

2 VfGH G 245-250/89, G 268-275/89, 30. Nov. 1989 = VfSlg. 12228/1989

3 Aufhebung des § 5 Abs. 2 DSG durch VfSlg. 12194/1989, des § 14 DSG durch VfGH G 139-141/93, 1. Dez. 1993

4 in §§ 6 und 7 DSG

aus der Rechtsprechung ignoriert. Beispielsweise sei ein Urteil des OGH[5] genannt, in dem klar ausgeführt wird, daß Banken die Daten aus dem Girokontenverkehr nicht für die Bausparwerbung verwenden dürfen. Die verschiedenen Geschäftsfelder sind datenschutzrechtlich sauber zu trennen. Im Gegensatz dazu versuchen viele große Unternehmen, möglichst alle unternehmensintern oder konzernintern verfügbaren Daten in einem Datawarehouse zusammenzufassen und miteinander zu verknüpfen.

Die Einhaltung datenschutzrechtlicher Bestimmungen könnte einerseits gefördert werden, wenn die Rechtsschutzinstrumentarien leichter zugänglich und kostengünstiger wären und es daher mehr Rechtsprechung gäbe. Andererseits könnte ein Datenschutzbeauftragter oder Datenschutzombudsmann eingerichtet werden, der systematisch Verletzungen des Datenschutzes feststellt, sektorspezifische Lösungen fördert und die Einhaltung datenschutzrechtlicher Bestimmungen auch wirksam einklagen kann.

5 OGH 4 Ob 114/91, 25. Feb. 1992 = SZ 65/23

V. Fallanalyse

Insgesamt wurden 1.453 Fälle thematisch analysiert. Aus der Sicht der Betroffenen ergeben sich fünf große Problemkomplexe:

- Einhaltung des Geheimhaltungsanspruchs (616 dokumentierte Fälle)
- Durchsetzung der Auskunftsrechte (622 dokumentierte Fälle)
- Wahrung der Datenintegrität und -qualität (51 dokumentierte Fälle)
- Wahrung sonstiger Informations- und Widerspruchsrechte (4 dokumentierte Fälle)
- Sonstige Rechte (178 dokumentierte Fälle)

Im Detail wurden folgende Einzelthemen behandelt:

	Thema	**Zahl der Fälle[6]**	**Anteil [%]**
	Einhaltung des Geheimhaltungsanspruches "Gefahr des Bruches der Geheimhaltung ..."	**616**	**42,40**
1.	... durch unzulässige ÜBERMITTLUNG von Informationen	207	14,25
2.	... durch unzulässige VERARBEITUNGEN und Auswertungen von Informationen	150	10,32
3.	... im Zuge der ERMITTLUNG von Daten (ohne Wissen des Betroffenen)	88	6,06
4.	... im Zuge der DATENERHEBUNG BEIM BETROFFENEN (RECHTSGRUNDLAGE ist unklar)	39	2,68
5.	... durch unzulässiges Veröffentlichen von Informationen	40	2,75
6.	... im Zuge der DATENERHEBUNG BEIM BETROFFENEN (Erhebung erfolgt auf "freiwilliger" Basis)	34	2,34
7.	... im Zuge statistischer DATENERHEBUNGEN BEIM BETROFFENEN	21	1,45
8.	... im Zuge der DATENERHEBUNG BEIM BETROFFENEN (Erhebung erfolgt auf gesetzlicher Basis)	17	1,17
9.	... im Zuge einer gesetzlich angeordneten VOLKSZÄHLUNG	15	1,03
10.	... durch Abgabe einer zu generell formulierten ZUSTIMMUNGSERKLÄRUNG zur Datenermittlung, -verarbeitung und -übermittlung	16	1,10
	Durchsetzung der Auskunftsrechte	**623**	**42,88**
11.	Probleme, eine korrekte AUSKUNFT gemäß DSG zu erhalten	605	41,64
12.	Probleme, eine korrekte AUSKUNFT gemäß APG zu erhalten	219	15,07
	Wahrung der Datenintegrität und -qualität "Ein Datenverarbeiter verwaltet ..."	**50**	**3,44**
13.	... Daten mit mangelhafter Qualität	28	1,93
14.	... unrichtige Daten	8	0,55
15.	... unnötige Daten	8	0,55
16.	... unvollständige Daten	6	0,41
	Weitere Informations- und Widerspruchsrechte	**4**	**0,28**
17.	Probleme bei der Durchsetzung dieser Rechte	4	0,28

6 Mehrfachnennungen sind möglich.

	Sonstige Rechte	**178**	**12,25**
18.	Probleme im Zusammenhang mit der REGISTRIERUNG von Datenverarbeitungen	53	3,65
19.	Durchsetzung des INFORMATIONELLEN SELBSTBESTIMMUNGSRECHTS	45	3,10
20.	Probleme bei der SICHERHEIT einer Datenverarbeitung	25	1,72
21.	Probleme bei der Genehmigung des INTERNATIONALEN DATENVERKEHRS	23	1,58
22.	Probleme im Zusammenhang mit der Beauftragung eines DIENSTLEISTERS	7	0,48
23.	Sonstige Probleme im Zusammenhang mit dem ZUGANG ZU INFORMATIONEN	12	0,83
24.	Sonstige Probleme im Zusammenhang mit einer Datenverarbeitung	11	0,76
25.	Sonstige Rechtsdurchsetzungsprobleme	3	0,21

VI. Strukturelle Probleme und Branchenprobleme

Die Rechtsdurchsetzung

Die Rechtsdurchsetzung ist im gegenwärtigen Datenschutzgesetz de facto nur im öffentlich-rechtlichen Bereich gegeben. In diesem Bereich besteht zumindest für eine Reihe subjektiver Rechte, die Möglichkeit formlos, kostenlos und damit ohne Verfahrensrisiko und ohne Vertretungszwang Beschwerde zu erheben. Die offenen Probleme dieses Bereiches sind einerseits die Beschränkung der subjektiven Rechte bzw. das Fehlen einer Reihe von Rechten, andererseits die überlange Verfahrensdauer.
Weiters können keine immateriellen Schadensansprüche geltend gemacht werden. Die Entscheidungen der Datenschutzkommission haben daher oft bloß feststellenden und appelativen Charakter. Das ist zu wenig, um Betroffene zu motivieren, gegen erlittenes Datenschutzunrecht Beschwerde zu erheben.

Gänzlich gescheitert ist die Rechtsdurchsetzung im Bereich privater Verarbeiter. Durch die Notwendigkeit, Beschwerden auf jeden Fall vor das jeweils zuständige Landesgericht zu bringen, kommt es zu einem extrem hohen Kosten- und Prozeßrisiko, dem wiederum keine angemessene Schadenersatzmöglichkeiten gegenüberstehen. Insgesamt kam es seit Bestehen des DSG (1980) bloß zu rund 20 bis 30 Verfahren, die fast durchwegs als Musterverfahren geführt wurden. Dabei wurde der jeweilige Betroffene materiell und beratend von einschlägigen Konsumentenschutzorganisationen unterstützt. Praktisch keine Privatperson nahm ausschließlich auf eigenes Risiko ihre Datenschutzrechte wahr.

Konsumentenschutzorganisationen und Arbeitnehmervertreter fordern daher schon seit längerer Zeit, den Rechtsschutz, wie er für den öffentlich-rechtlichen Bereich existiert, auch auf private Datenverarbeiter auszudehnen, zumindest jedoch für den Zivilrechtsweg das Außerstreitverfahren einzuführen, um das Klags- und Kostenrisiko gering zu halten.

Nach wie vor sind wesentliche Bereiche, in denen Datenschutzverletzungen möglich sind, von einer rechtlichen Regelung ausgenommen. Dies betrifft besonders die Gerichtsbarkeit aber auch die Legislative (u.a. DSK 210.273, 120.495, 120.512). Datenschutzverletzungen des Nationalrates oder anderer gesetzgebender Körperschaften (z.B. DSK 120.480) sind ebenfalls nicht verfolgbar.

Die Interessensabwägung

In vielen Bereichen funktioniert die notwendige Interessensabwägung zwischen verschiedenen Grundrechten nicht oder nicht ausreichend.

Dem berechtigten Interesse des Gläubigerschutzes beispielsweise steht das berechtigte Interesse des Kredit- und Darlehensnehmers auf Achtung seiner Privatsphäre gegenüber. Auch geringfügige Unregelmäßigkeiten bei der Rückzahlung von Schulden führen zu Eintragungen in zentralen Listen

("Unerwünschte Kontoverbindungen", "Kleinkreditkataster", "Wirtschaftsevidenz"), in die eine Vielzahl von Organisationen Einsicht nehmen können. Ebenso fehlen effiziente Kontrollmechanismen, die die Richtigkeit der Eintragungen genau kontrollieren, die Betroffene informieren und auf ihre Rechte aufmerksam machen und Informations- und Schadensersatzmechanismen, die bei Eintragungsfehlern die Betroffenen schadlos halten.

Das Sicherheitsbedürfnis der Bevölkerung macht die Erfassung und Analyse von Tätern, Verbrechen und Tatverdächtigen notwendig. Gleichzeitig ist aber immer auch die Unschuldsvermutung anzuwenden und die Möglichkeit von Fehlern in der Ermittlung und Verarbeitung von Informationen zu bedenken. Die Beschränkung von Grundrechtseingriffen, die daher erforderlich ist, ist im Zusammenhang mit einigen Informationsinitiativen, wie der Sammlung von DNA-Daten, der Aufzeichnung der zwangsweisen Einweisung in psychiatrische Anstalten oder bei der Formulierung der Beweisverwertungsverbote bei Lauschangriff und Rasterfahndung, aber nicht der Fall.

Weitere Beipiele sind Privatversicherungen, die einen potentiellen Versicherungsbetrug frühzeitig erkennen und unterbinden wollen, und statistische und wissenschaftliche Analysen von Informationen, deren Wunsch der Genauigkeit und Flexibilität der statistischen Analyse der Eingriff in das Privatleben gegenübersteht.

Das Konzernproblem

Datenschutzrechtlich sind die Daten jedes Tochterunternehmens völlig getrennt von den Daten der anderen Töchter zu behandeln, sogar die Weitergabe von Daten von einem Geschäftsfeld (Aufgabengebiet) in ein anderes Geschäftsfeld eine Übermittlung, die so wie die Weitergabe von einem Unternehmen an ein anderes zu behandeln ist.[7]

Diese saubere datenschutzrechtliche Trennung verschiedener Aufgabengebiete liegt aber nicht im wirtschaftlichen Interesse von Konzernen, die durch enge Zusammenarbeit mit ihren Töchtern produktive und finanztechnische Synergieeffekte lukrieren möchten, und daher daran interessiert sind, mittels Datawarehouse- oder Datamining-Lösungen möglichst alle konzernintern vorhandenen Daten in einer einzigen Datenbank zusammenzuführen.

Einen besonders problematischen Komplex bilden dabei Unternehmen, die in den drei Geschäftsfeldern Versandhandel, Adressenverlag und Bank gleichzeitig tätig sind. Als Adressenverlage können diese Unternehmen Handel mit fremden Daten treiben, als Banken haben sie direkten Zugriff auf die Informationen des Verbundsystems der Banken. Die Verknüpfung dieser verschiedenen branchenspezifischen Möglichkeiten ermöglicht es solchen Firmen, die Datenschutzbestimmungen weitestgehend zu umgehen.

7 So hat etwa der OGH im Urteil 4 Ob 114/91, 25. Feb. 1992 = SZ 65/23 festgestellt, daß die Weiterverarbeitung von Girokontendaten für Zwecke der Bausparwerbung unzulässig ist.

Informationsverbundsysteme

Verschiedene Datenverarbeiter, wie Banken, Versicherungen und auch das Informationsverbundsystem des BM für Inneres betreiben Informationsverbundsysteme, in die verschiedene Datenverarbeiter ihre Daten einbringen und alle anderen Teilnehmer diese Daten abrufen können. Für den Betroffenen hat dies die Konsequenz, daß die Zuständigkeit für die Datenverarbeitung ungeklärt ist und daß eventuelle Fehler sehr rasch bei vielen Stellen verbreitet werden.

Die fehlende Rechtsgrundlage

Eine Reihe von Unternehmen, die mit sehr sensiblen Daten agieren, handelt ohne direkte Geschäfts- und Vertrauensbeziehung zum Betroffenen. Diese Einrichtungen haben in der Regel keinen Rechtsanspruch auf personenbezogene Daten (z.B. Inkassobüros).

Damit diese Einrichtungen trotzdem zu den für ihre Tätigkeit notwendigen Daten kommen, agieren sie in einem Graubereich und versuchen durch verschiedene psychologische Tricks und falsche Behauptungen Auskünfte zu erhalten. So treten diese Einrichtungen immer wieder pseudoamtlich auf ("wir ermitteln in einer Rechtssache", "für ein Verfahren", "hieramts notwendige Untersuchung"), oder sie versuchen Arbeitgeber, Hausbesorger und -verwalter, Verwandte oder Mitbewohner schlicht zu überrumpeln.

Vergleichbar zu behördlichen Ermittlungen müßte für derartige Einrichtungen eine Informations- und Aufklärungspflicht (mit begleitenden Strafsanktionen) eingeführt werden, die diese Einrichtungen verpflichtet, Auskunft über die rechtlichen Grenzen und Grundlagen ihrer Auskunftsersuchen zu geben.

Wissenschaftliche Forschung

Ein Standardproblem stellen Erhebungen zum Zwecke wissenschaftlicher Forschung dar. Oft werden diese Arbeiten von Behörden oder sonstigen Organisationen in Auftrag gegeben, zu denen die befragten Personen in einem Abhängigkeitsverhältnis stehen (Schüler/Schule, Mütter/Tagesheime, Angestellte/Arbeitgeber, ...). Vielfach lassen die Erhebungen die notwendige Sensibilität bezüglich des Grundrechtseingriffes vermissen. Aus Sorge nicht genügend Datenmaterial zu bekommen, wird zu wenig oder überhaupt nicht auf die Freiwilligkeit der Mitarbeit hingewiesen oder nicht auf eine effektive Anonymisierung geachtet. Bei einer gewissen Sensibilisierung wäre es jedoch für die erhebenden Stellen ein leichtes, entsprechende Settings zu gestalten, die einen unerwünschten Grundrechtseingriff vermeiden.

Innerkirchliche Angelegenheiten

Aus historischen Gründen, insbesondere aufgrund des Konkordats, wird die Mitgliederverwaltung der Religionsgemeinschaften vom Staat unterstützt, indem das Religionsbekenntnis als Bestandteil des polizeilichen Meldezettels (früher: der

Haushaltslisten) verwaltet wird. Ist strittig, ob eine Person ein bestimmtes Religionsbekenntnis hat, kann die Religionsgemeinschaft dazu ein Feststellungsverfahren vor der Bezirksverwaltungsbehörde beantragen.

Diese Sonderstellung steht im Konflikt mit datenschutzrechtlichen Regelungen. Art. 8 der EU-Datenschutzrichtlinie stuft Daten über religiöse oder philosophische Überzeugungen als besonders sensible Daten ein, die prinzipiell nicht verarbeitet werden dürfen (wobei für die Mitgliederverwaltung der religiösen Organisation selbst eine Ausnahme vorgesehen ist).

Eine Lösung dieses Problemkreises ist mittelfristig nur durch eine Anpassung der rechtlichen Sonderbestimmungen an ein modernes Religions- und Staatsverständnis zu erwarten.

Überschießende Erhebungen

Generell nutzen Gemeinden sehr häufig amtliche Bürgerkontakte (z.B. Meldeverfahren, Antrag für Parkberechtigungen, Anträge für Förderungen, ...), um über das notwendige Maß hinausgehende Daten zu erheben.

Betroffene, die in der Regel bloß rasch die unbedingt notwendigen Behördenwege erledigen wollen, haben sehr oft nicht genügend Zeit und auch Wissen, um die rechtlichen Details einer Datenermittlung abschätzen zu können und geben persönliche Informationen (etwa Familien- und Einkommensverhältnisse, Berufs- und Ausbildungsinformationen) preis, die sie bei genauer Kenntnis des rechtlich unbedingt notwendig Informationsumfanges auf keinen Fall gegeben hätten.

Hier wird die Zukunft zeigen, inwieweit die Vorgabe der EU-Datenschutzrichtlinie, bei Erhebungen auszuweisen, welche Daten verpflichtend gegeben werden müssen und welche auf freiwilliger Basis gegeben werden können, greifen wird.

Der "halb"öffentliche Raum

Wir bewegen uns vielfach in Bereichen, die zwar von vielen Personen benutzt werden, die jedoch durch die sozialen oder sonstigen Rahmenbedingungen nur von einer bestimmten gleichartigen Gruppe frequentiert werden. Beispiele sind etwa die Schulen und Universitäten, die eigentlich nur von Schülern/Studierenden und Lehrenden frequentiert werden, die Krankenhäuser, in denen sich Patienten, Ärzte und Verwandte aufhalten, Privatpensionen, aber auch kleinere Gemeinden.

Alle diese Räume schaffen eine private, zumindest geschlossene Atmosphäre, bei der der einzelne das Gefühl gewinnt, "unter seinesgleichen" zu sein. Nichtsdestotrotz handelt es sich um klassische öffentliche Bereiche, bei denen veröffentlichte Informationen in falsche Hände gelangen können.

Noch immer lassen etliche Einrichtungen die entsprechende Sensibilität vermissen:
- Auflegen der Gästebücher
- Aushang von Patientenblättern
- Aushang von Prüfungsergebnissen
- Aushang von Kirchen- und Gemeindenachrichten

Manuelle Datensammlungen

Bisher waren manuelle Akten- und Karteisammlungen nur unzureichend von den Datenschutzrechten erfaßt. Dies führte unter anderem dazu, daß bei besonders sensiblen Sachverhalten ganz bewußt auf den "Handakt" ausgewichen wurde.

Die neue EU-Datenschutzrichtlinie soll diese, bloß technisch begründete Regelungslücke schließen. Die Durchsetzung von subjektiven Rechten darf nicht von der technischen Form der Datenermittlung und -verwaltung abhängen.

Zu allgemeine gesetzliche Datenverarbeitungsbestimmungen

Auch im zwanzigsten Jahr des Datenschutzes besteht noch eine Fülle gesetzlicher Regelungen, die nicht im Detail die notwendigen Datenarten, Ermittlungs- und Übermittlungsermächtigungen beschreiben, sondern ganz generell bloß auf alle "notwendigen" Daten abzielen.

Laufend führen unklare Übermittlungsermächtigungen nicht dazu, die Betroffenenrechte klarzustellen, sondern dazu die Übermittlungen zu erleichtern (z.B. Gesetzesnovelle zur Erleichterung des Datenaustausches zwischen Sozialversicherungen und AMS/ AMV).

VII. Entwicklung des Datenschutzes in Hinblick auf die technologische Entwicklung

Im Zusammenhang mit Datenverarbeitungen zeichnet sich eine Reihe globaler Trends ab, die bisher nicht oder ungenügend in die Datenschutzgesetzgebung eingeflossen sind.

Internationaler Datenverkehr

Das bisherige Datenschutzgesetz geht im wesentlichen von abgeschlossenen Datenverarbeitungen bei meist lokal oder auf innerstaatlicher Basis operierenden Organisationen, Behörden oder Unternehmen aus. Die Übermittlung von personenbezogenen Daten wird als genehmigungspflichtige Ausnahme in der Verarbeitungspraxis angesehen. Diese Position widerspricht dem generell arbeitsteiligen Trend und dem Trend zur Globalisierung. Auch Datenverarbeitungen werden heute weltweit arbeitsteilig organisiert.

Offene Netze

Bis zur Mitte der 90er Jahre waren in Österreich praktisch nur proprietäre und/oder abgeschlossene Datennetze bekannt. Dies bedeutet, daß für die Sicherheit und auch für die Einhaltung der verschiedenen gesetzlichen Bestimmungen klare Verantwortlichkeiten herrschten. Meist war der Netzbetreiber ident mit dem datenschutzrechtlich Verantwortlichen, oder der Netzbetreiber konnte alle Teilnehmer über einheitliche Verträge an die Einhaltung der entsprechenden Bestimmungen binden. Diese Situation ist bei offenen Netzen, wie dem Internet, nicht mehr gegeben.
Das datenschutzrechtliche Problem besteht darin, daß für den Betroffenen vielfach nicht mehr erkennbar ist, wer Verantwortlicher einer bestimmten Datenverarbeitung ist, wer für sein Datenschutzanliegen zuständig ist bzw. aufgrund welcher gesetzlichen Bestimmungen jetzt seine persönlichen Daten verarbeitet werden.

Personenbezogene Prozeßdaten

Immer mehr Datenverarbeitungen erlauben es, in Echtzeit Informationen zum Benutzerverhalten zu speichern. Es sind dies Informationen, wer wann welchen Dienst in Anspruch genommen hat, wer sich an welchem Ort aufgehalten hat und wer mit wem in Kontakt getreten ist. Diese Informationen, die zum überwiegenden Teil zur Aufrechterhaltung des Betriebs einer Dienstleistung notwendig sind, können auch zur Feststellung des Benutzerverhaltens (Erstellung von Benutzerprofilen) verwendet werden und gegen die Interessen des Betroffenen gerichtet sein.
Die datenschutzrechtlichen Probleme ergeben sich nicht aus den einzelnen Datensätzen, sondern aus den daraus abgeleiteten Auswertungen und Interpretationen. Der Informationswert der Prozeßdaten erschließt sich erst aus der Auswertung und dem Vergleich großer Datenmengen. Damit ein Betroffener erkennen kann, welche Schlußfolgerungen aus seinen Prozeßdaten gezogen werden, wäre es daher notwendig, die Informations- und Richtigstellungsrechte auch auf die Auswertungen auszudehnen.

Neue Techniken in der Büroautomation

Im Zuge der Einführung des Faxes gab es durch Fehlzustellungen laufend ungewollte Datenschutzverletzungen. Der Anteil der dadurch offenbarten Informationen dürfte nach wie vor relativ hoch sein.
Wesentlich verstärkt wird diese Problematik derzeit beim Einsatz von electronic Mail. Neben der dort ebenfalls gegebenen Gefahr der schlichten Fehlzustellung einer Nachricht durch die Angabe eines falschen Empfängers können weitere Datenschutzverletzungen erfolgen (z.B. durch das Anführen aller Empfänger einer E-Mail können unerwünscht Kommunikationsbeziehungen offenbart werden).

Datamining-Tools

Die Grundgedanken von "datamining" sind nicht neu und werden seit rund 30 Jahren unter Schlagwörtern wie "Management Information System (MIS)" propagiert. Neu ist heute, daß einerseits diese Technologien ausgereift, weit verbreitet und billig sind, andererseits daß durch das rasche Anwachsen der Prozeßdatenbestände auch genügend auswertbares Material vorhanden ist.
Die bestehenden rechtlichen Regelungen zum Datenschutz ignorieren diese Entwicklung vollständig, da alle Regelungen immer von in sich geschlossenen Datenverarbeitungen ausgehen, welche Daten zu einem bestimmten Zweck ermitteln, verarbeiten und übermitteln. Die ständige Neuverwertung und Neubewertung von Informationen sind dabei nicht vorgesehen.

Öffentlich zugängliche Datenbanken

Sowohl über das Internet, über Onlinedienste und mittels CD-ROM erhält eine immer breitere Öffentlichkeit Zugang zu personenbezogenen Informationen.
Die zentralen Probleme sind dabei weniger die abzurufenden Daten selbst sondern die erweiterten Möglichkeiten, diese Informationen mit anderen Datenbanken zu verknüpfen und nach anderen Kriterien als ursprünglich vorgesehen zu recherchieren und auszuwerten.

VIII. Schlußfolgerungen

Die Studie hat deutlich gezeigt, daß es bei folgenden Punkten im derzeitigen Datenschutzgesetz noch große Mängel und Verbesserungsmöglichkeiten gibt.

Verbesserte begriffliche Klarheit

Im Datenschutzgesetzes sollten Begriffe verwendet werden, die für die Betroffenen und für die Datenverarbeiter möglichst klar und operativ umsetzbar sind. Dabei muß das Datenschutzgesetz der üblichen juristischen Präzision folgen. Besonderes Augenmerk ist dabei auf die genaue Abgrenzung und Definition einzelner Begriffe zu legen (z.B. die Begriffe "Auftraggeber" oder "Dienstleister").

Außerdem ist auf die spezialisierte Terminologie der Datenverarbeitungsbranche einzugehen. Dies ist sicher nicht einfach, da dieser Bereich dramatischen und raschen Änderungen unterworfen ist. Trotzdem dürfen die Begriffe weder zu spezifisch sein, sie würden sonst zu rasch veralten, noch zu allgemein, sie würden ansonsten nicht leicht umsetzbar sein.

Konzept der strukturellen Datenschutzprobleme

Es muß ein Mechanismus gefunden werden, der es erlaubt, wirksam strukturelle Datenschutzprobleme zu beseitigen. Dazu ist es notwendig, neben dem individuellen Beschwerderecht, das immer nur eine bestimmte Datenschutzverletzung beseitigen kann, auch die Möglichkeit der Verbandsklage durch entsprechende Organisationen und Einrichtungen zu schaffen.

Vereinfachte Verfahren zur individuellen Rechtsdurchsetzung

Datenschutzverfahren müssen rascher durchgeführt werden und für die Betroffenen einfacher und transparenter als bisher zu führen sein. Die Trennung verschiedener Rechtsdurchsetzungswege für "private" und "öffentlich-rechtliche" Datenverarbeitungen muß fallen.

Der erweiterte Schutzbegriff

Die strategische Orientierung des Datenschutzes muß zu einer Umformung der subjektiven Rechte des Betroffenen führen. Aus dem simplen "Geheimhaltungsanspruch" muß das Recht auf "informationelle Selbstbestimmung" werden.

Damit wird die Durchführung von Datenverarbeitungen vereinfacht, wenn der Betroffene dieser Verarbeitung zugestimmt hat; die Datenverarbeitungen werden aber auch eingeschränkt, da ein erweitertes Schutzrecht nicht nur auf die einzelnen Daten, sondern auch auf die gesamte Verarbeitung inkl. zusätzlichen zulässigen Verarbeitungen und den Verarbeitungsergebnissen abzielen muß.

Widerspruchsrechte könnten ausgebaut und systematisch in eine Reihe von Rechtsmaterien eingebaut werden (z.B. im Zusammenhang mit der Weitergabe von Wählerevidenzdaten). Auch im Bereich von Stellenbewerbungen bzw. von

Personalberatungsfirmen oder beim AMS wäre ein Widerspruchsrecht angesichts der oft raschen Veränderungen in den Anstellungsverhältnissen, der Berufserfahrungen und der Qualifikationen sinnvoll.

Informations- und Aufklärungsstelle zur Vermeidung formeller Datenschutzverfahren (Bundesdatenschutzbeauftragter)

Die fehlende Möglichkeit, daß eine unabhängige Stelle behauptete Datenschutzverletzungen aufgreifen und überprüfen kann, kann als Mangel des Gesetzes angesehen werden. Gerade bei der Verletzung des Datenschutzes, in der Regel bei der Verletzung des Grundrechts auf Geheimhaltung, hätte ein Betroffener ein gesteigertes Interesse, daß sein Fall mit größtmöglicher Schonung behandelt wird. Dazu wäre die Recherche durch einen unabhängigen Dritten, einen Datenschutzbeauftragten oder einen Datenschutzombudsmann ein geeignetes Instrument.

In diesem Zusammenhang erwarten sich die Betroffenen auch (a) eine aktive Informationspolitik, etwa wenn ihr aufgezeigtes Sachverhalten einen Systemmangel offenlegt und (b) eine aktive Rolle bei der Führung von Verfahren durch einen Datenschutzbeauftragten, wenn ein nicht rechtskonformer Sachverhalt festgestellt wird.

Ebenso könnten zu generelle, teilweise sittenwidrige Zustimmungserklärungen wirksam über einen Datenschutzbeauftragten mit generellen Klags- und Einwirkungsvollmachten bekämpft werden. Dieser könnte über Unterlassungsklagen die Verwendung nachteiliger Zustimmungserklärungen oder umfassender Frage- und Erhebungsbögen bekämpfen.

Geschädigte bzw. vermeintlich Geschädigte haben derzeit nur die Alternativen, ein formelles Verfahren anzustrengen, nichts zu tun, sich mit dem Fall an eine informelle, jedoch kompetenzlose Beschwerdestelle zu wenden oder an die Öffentlichkeit zu gehen[8].

Technologische Begleitung

Aufgrund der Dynamik des Technologiezweiges Informationsverarbeitung und der fortschreitenden Konvergenz der Bereiche Medien, Telekommunikation und Datenverarbeitung ist die systematische Beobachtung, Analyse und Hilfestellung im Zusammenhang mit Sicherheitsrisken der Informationstechnologie wichtig.

---

8 Im informellen Bereich sind derzeit folgende Stellen tätig:
(a) die Schlichtungsstelle der Datenschutzkomission im BKA, eine sozialpartnerschaftlich besetzte Stelle ohne Kontroll-, Entscheidungs- und Erhebungskompetenz,
(b) die ARGE DATEN - Österreichische Gesellschaft für Datenschutz, eine als privater Verein organisierte Vereinigung, die über Spenden, Mitgliedsbeiträge und Referentenhonorare finanziert wird, auch hier fehlen Erhebungs- und Kontrollkompetenzen, es kann also immer nur eine Beratung von Betroffenen und Datenverarbeitern durchgeführt werden, bei Mitglieder werden auch Vertretungen vor Behörden übernommen,
(c) der Verein für Konsumenteninformation, eine sozialpartnerschaftlich besetzte Konsumentenschutzvereinigung, die dann als Anlaufstelle geeignet ist, wenn Datenschutzverletzungen Teil eines Konsumentenschutzproblems sind,
(d) die Medien, deren Einschaltung in der Regel die größte Wirksamkeit bei der Behebung von systemischen Datenschutzmängeln erreicht.

Es geht dabei weder um eine gesellschaftspolitische Risikoabschätzung, noch sollte diese Stelle die Umsetzung von Datenschutzbestimmungen kontrollieren, überwachen oder durchsetzen.
Diese Stelle sollte als technologienahe Anlaufstelle Beratung und Information über ganz konkrete Sicherheitsrisken ermöglichen. Sie sollte somit gleichermaßen Anlaufstelle für datenverarbeitende Organisationen, für Betroffene aber auch für die eigentlichen Datenschutzkontrollstellen sein.