Ein schweizerisches Datenschutzgesetz?

Von Prof. Peter Forstmoser (Zürich)

Das Thema *«Datenschutz»* — Schutz der Privatsphäre des Einzelnen vor Eingriffen, die durch das Sammeln, die Verwertung und Weitergabe von personenbezogener Information erfolgen — ist seit einiger Zeit auch in der Schweiz Gegenstand intensiver rechtspolitischer Diskussion geworden. Vorarbeiten für *kantonale Erlasse* sind an verschiedenen Orten 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.

Auf *Bundesebene* reichte Nationalrat Bussey schon 1971 eine Motion betreffend die Gesetzgebung über Computer ein. — Der 1974 vorgelegte Entwurf der *Expertenkommission Lüchinger* für eine Neugestaltung des Persönlichkeitsrechts befasst sich in einem eigenen Artikel 28 k mit der Gefährdung der Privatsphäre durch Datenbanken.

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».

In die gleiche Richtung zielt eine *Motion* von Nationalrat Carobbio, die Gesetzesbestimmungen «über die öffentlichen und privaten Informationszentren» verlangt.

Im Rahmen der *Bundesverwaltung* schliesslich wird zurzeit an einer Vereinheitlichung des Datenschutzes in der Verwaltung gearbeitet. Bis zum Herbst 1978 will das Eidgenössische Justiz- und Polizeidepartement zudem einen *Zwischenbericht* zur Frage des Datenschutzes vorlegen.

Problematik und Zielsetzung

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. Man denke etwa an die Auskünfte, welche Versicherungen benötigen, um das zu übernehmende Risiko richtig beurteilen zu können, an die umfassenden Angaben, die erforderlich sind, um geeignete Mitarbeiter auszuwählen. Man denke auch an die moderne Leistungsverwaltung — etwa die Sozialversicherung mit ihren zahlreichen Sparten —, die ohne detaillierte Information über den einzelnen Bürger nicht funktionieren kann.

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.* Dieser ist besonders gravierend, wenn sich Informationen als *fehlerhaft* erweisen sollten, was auf einem menschlichen oder technischen Versagen beruhen kann, allenfalls aber auch bewusst in Kauf genommen wird. Fehlerhaft oder zumindest irreführend kann insbesondere eine Auskunft sein, die auf einem subjektiven Werturteil beruht, etwa eine Aussage über Charaktereigenschaften oder den Gesundheitszustand. Verfälscht sind aber personenbezogene Auskünfte oft auch deshalb, weil sie aus dem Zusammenhang gerissen und verkürzt wiedergegeben werden. Gefahren bringt weiter der *Zugriff durch Unbefugte* mit sich: Gerade bei personenbezogenen Informationen ist es wesentlich, wer der Empfänger ist.

Diese und weitere Gefahren sind zwar keineswegs neu, in einer informationshungrigen Gesellschaft jedoch *aktualisiert.* Hinzu kommen nun aber *bei der elektronischen Datenverarbeitung zusätzliche Probleme,* die sich beim Sammeln und Archivieren mit herkömmlichen Mitteln nicht stellen: Der Unterschied zwischen traditioneller Registrierung und elektronischer Datenverarbeitung ist zunächst *quantitativ:* 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 kann allenfalls ein eigentliches Persönlichkeitsprofil erstellt werden. Durch den Einsatz von Computern werden sodann *faktische Schranken* des Zugriffs und der Verarbeitung *abgebaut.* Weiter ermöglicht die EDV die *Umgliederung und Auswahl* grosser Datenmengen nach den verschiedensten Kriterien mit sehr geringem Aufwand. Endlich dürfte der Einsatz moderner und entsprechend kostspieliger Hilfsmittel zu einer *Konzentration* und *Zentralisierung* personenbezogener Information führen.

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.

Datenschutz im geltenden Recht

Das geltende Recht enthält eine Reihe von Bestimmungen, die — obwohl nicht im Hinblick auf Datenbanken geschaffen — zumindest *teilweisen Datenschutz* gewähren:

Datenschutz im privaten Bereich

Für den privaten Sektor ist vor allem an Art. 28 Zivilgesetzbuch zu erinnern, wonach *jedermann, der «in seinen persönlichen Verhältnissen unbefugterweise verletzt wird», auf Beseitigung der Störung, auf Schadenersatz und allenfalls auf Genugtuung klagen kann.*

Dass diese Norm gerade im Bereich des Datenschutzes bedeutsam werden könnte, zeigt ein neuerer Bundesgerichtsentscheid, der das Verhalten eines Adressenverlages zu beurteilen hatte. Dieser hatte eine Reihe von *«Spezialadressverzeichnissen»* zum Kauf angeboten, darunter die Mitgliederlisten der Freimaurer und Odd-Fellows-Logen, des Lions Club und der Philanthropischen 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 daher das Verbot, diese Verzeichnisse zu vertreiben.

Ein weiterer Schutz liegt in den *Berufsgeheimnissen,* namentlich dem Anwalts-, dem Arzt- und dem Bankgeheimnis.

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.*

Im *Verwaltungsrecht* ist vor allem auf die Pflicht des Beamten zur *Geheimhaltung* und die damit verbundene Schweigepflicht hinzuweisen.

Während die Schweigepflicht die Weiterleitung von Informationen unterbindet, wird die Datenregistrierung als solche durch den Grundsatz der *Gesetzmässigkeit der Verwaltung* eingeschränkt.

Ungenügen des geltenden Rechts

Obschon damit das geltende Recht nicht zu unterschätzende Sicherheiten bietet, ist heute kaum bestritten, dass die herkömmliche Ordnung allgemein dem Schutz der Persönlichkeit, besonders aber angesichts von Datenbanken, nicht mehr zu genügen vermag.

Nicht zu genügen vermag die geltende Ordnung vor allem im Hinblick auf *Personendatenbanken:*

1. Die einschlägigen Rechtsvorschriften sind *in verschiedenen Erlassen verstreut* und decken den Datenschutz mehr zufällig ab.

2. 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.

3. Gerügt worden ist, dass das geltende Recht *kein Einsichtsrecht des Betroffenen* vorsieht und dass daher die Möglichkeit einer Persönlichkeitsverletzung allenfalls gar nicht feststellbar ist.

4. Sodann *fehlt* im geltenden Recht die *präventive Kontrolle;* es kann praktisch nur eingeschritten werden, wenn Persönlichkeitsrechte bereits verletzt worden sind.

5. Zu wenig beachtet wurde bisher ein weiteres Element: das *Erfordernis, mit der internationalen Entwicklung* im Bereich des Datenschutzes *Schritt zu halten.* Schon heute wird im Ausland — im Anschluss an die steuerrechtliche Terminologie — kritisch von der Möglichkeit von «data haven», «Datenoasen», gesprochen. Ausländische Gesetze und Gesetzesentwürfe sehen bereits Restriktionen für den grenzüberschreitenden Datenverkehr vor für den Fall, dass im Ausland nicht der gleiche Standard des Datenschutzes gewährleistet ist.

Zielsetzung und möglicher Inhalt

Der Schutzzweck

Durch eine künftige Gesetzgebung soll die *Privatsphäre der Person,* und zwar in erster Linie der *natürlichen Person,* im Hinblick auf die Datenspeicherung und Datenverarbeitung geschützt werden.

Damit ist freilich nicht mehr als eine allgemeine Zielsetzung gewonnen. Es fragt sich, ob eine präzisere Formulierung in einem künftigen Gesetz möglich und tunlich ist. Soll etwa nach bestimmten Kategorien differenziert werden, z. B. mit der auch vom Bundesgericht übernommenen Sphärentheorie nach der Vie intime, der Vie privée und der Vie publique? Meines Erachtens sollte der Gesetzgeber von einer solchen Unterscheidung grundsätzlich absehen und sie dem *Richter im Einzelfall überlassen.*

Dieser Grundsatz wäre allerdings in einer Richtung zu modifizieren: Sogenannte *Intimdaten,* «heisse Daten», Informationen, die — in den Worten des Bundesgerichts — «der Kenntnis aller anderen Leute entzogen sein sollen, mit Ausnahme jener Personen, denen diese Tatsachen besonders anvertraut wurden», müssten zusätzlich geschützt werden. Ich denke an ein ausdrückliches *Verarbeitungsverbot* mit genau umschriebenen Ausnahmen.

Dagegen würde ich die Ausklammerung sogenannt *freier Daten* ablehnen, da auch diese in einer die Persönlichkeit verletzenden Art zusammengetragen werden können.

Zu erfassende Datenbanken

Zu regeln sind — wie in Schweden und der Bundesrepublik Deutschland sowie entsprechend der Initiative Gerwig — sowohl der *öffentliche wie der private Bereich,* was freilich nicht heisst, dass private und staatliche Datenbanken notwendig dem gleichen Gesetz zu unterstellen sind.

Keine Rolle spielen darf sodann, ob eine Personendatenbank nur für eigene Zwecke oder für Dritte geführt wird. Ebensowenig kann es meines Erachtens darauf ankommen, ob eine Datenbank mit Hilfe der elektronischen Datenverarbeitung oder aber manuell in konventioneller Form geführt wird.

Schranken der Verarbeitung

Auszugehen ist davon, dass die Speicherung und die Verarbeitung personenbezogener Daten *zulässig* sein müssen, mit der Einschränkung freilich, dass ein *schützenswertes Interesse* zu verlangen ist. Abzulehnen wäre es, die Verarbeitung personenbezogener Information generell von der Zustimmung des Betroffenen abhängig zu machen

Dies schliesst nicht aus, dass — wie bereits angetönt — für *Intimdaten* ein Speicherungsverbot mit Erlaubnisvorbehalt vorgesehen wird.

Rechnung zu tragen ist jedoch dem Umstand, dass bei personenbezogenen Daten der *Empfänger* von Bedeutung ist. Eine *Weitergabe* von Personendaten ist daher nur zuzulassen, wenn und soweit der Betroffene ihr zustimmt oder damit rechnen muss. Für den staatlichen Bereich wäre sodann eine Art *Gewaltenteilung* vorzusehen: Jedes Organ soll nur die Daten erhalten und verarbeiten, die es legitimerweise zur Erfüllung seiner Aufgaben benötigt.

Einführung besonderer Berufsgeheimnisse?

Gegenüber der öffentlichen Verwaltung bietet das *Amtsgeheimnis* Schutz vor der unerwünschten Weitergabe personenbezogener Information.

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. Ein Anfang hiezu wurde 1971 bei der Revision des Bankengesetzes gemacht: Das Bankgeheimnis soll nach neuer Formulierung nicht nur auf Organe und Angestellte von Banken Anwendung finden, sondern auch auf «Beauftragte».

Pflicht zur Datenrichtigkeit

Ungenaue und lückenhafte Personeninformationen können schwerwiegende Folgen haben. Es ist daher zu verlangen, dass Personendaten *richtig und vollständig* sind.

Richtigkeit und vor allem Vollständigkeit lassen sich allerdings 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.*

Pflicht zur Datensicherung

Weiter ist zu fordern, dass personenbezogene Daten durch angemessene *technische und organisatorische Massnahmen* vor Entwendung, Verstümmelung und Missbrauch *geschützt* werden. 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.

Die Kontrollstruktur

Die Einhaltung der gesetzlichen Vorschriften ist angemessen 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.

Eine *Kontrolle durch die Betroffenen selbst* setzt dreierlei voraus:

1. Sie müssen von der *Existenz* der Personendatenbank erfahren. Angemessenes Mittel hierzu wäre ein *Datenbankregister,* das öffentlich wäre und dem gewisse minimale Informationen über Personendatenbanken entnommen werden könnten.

2. Weiter müssen die Betroffenen *Auskunft über die zu ihrer Person gespeicherten Daten* erhalten. Dieses Auskunfts- oder Einsichtsrecht dürfte dem Grundsatz nach unbestritten sein. Seine Konkretisierung oder 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? 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.

In der Literatur und in politischen Vorstössen ist verschiedentlich verlangt worden, es müssten die betroffenen Personen bei der ersten Speicherung *benachrichtigt* werden. Eine generelle Benachrichtigungspflicht sieht das deutsche Bundesdatenschutzgesetz vor. Persönlich stehe ich dieser Lösung 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.

3. Schliesslich muss dem Betroffenen ein Recht auf *Berichtigung* unrichtiger und auf *Löschung* ungesetzlich gespeicherter Daten zustehen. Bei nicht objektivierbaren Angaben — etwa über Charaktereigenschaften — müsste 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* vorzusehen.

Im Rahmen des Datenschutzes wird die *Selbstkontrolle der Unternehmen,* die Personendatenbanken unterhalten, eine wichtige Rolle spielen.

1. Zunächst ist — damit allfällige Rechtsverletzungen überhaupt festgestellt und rückgängig gemacht werden können — über die Behandlung von Personeninformationen Buch zu führen. Die Zugriffsstruktur muss klar geordnet sein; Einspeicherungen und Mutationen sind zu *protokollieren,* ausnahmsweise und unter bestimmten Voraussetzungen auch die einzelne Abfrage.

2. Weiter fragt es sich, ob besondere Kontrollorgane zwingend vorgeschrieben werden sollten. Das deutsche Recht sieht für private Datenbanken, die mindestens fünf Arbeitnehmer ständig beschäftigen, die Bestellung eines *Beauftragten für den Datenschutz* zwingend vor. Für die Schweiz wäre das Konzept einer *Datenrevisionsstelle* zu diskutieren. 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 würde.

Wie allgemein im Persönlichkeitsschutz, so müsste auch im Datenschutz eine *Fremdkontrolle* in erster Linie durch die *Gerichte* auf Klage der Betroffenen hin ausgeübt werden.

Fraglich ist, ob zusätzlich eine *präventive Kontrolle* eingeführt werden sollte. 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. Denkbar wäre es dagegen, die Bewilligung zum Betrieb von der Erfüllung gewisser gesetzlicher Minimalanforderungen abhängig zu machen.

*

Ist die *Zeit* für eine Datenschutzgesetzgebung überhaupt gekommen? Kritiker werden dies bezweifeln mit dem Hinweis darauf, dass keine unhaltbaren Zustände herrschen und bisher keine Skandale zu registrieren waren. Gerade dies ist aber nach meiner Auffassung Grund genug, um die Gesetzgebungsarbeit an die Hand zu nehmen: Datenschutz ist eine Materie, die emotional anspricht und sich für demagogische Uebersteigerungen eignet. Es ist daher Sorge dazu zu tragen, dass die Arbeit nüchtern an die Hand genommen wird, nicht im Affekt und unter dem Eindruck hochgespielter Missstände. Dabei ist stets zu beachten, dass Datenschutz *Ausgleich legitimer Interessen* — der Interessen des Einzelnen an seiner Privatsphäre und der Dritter an personenbezogener Information — bedeutet. Als Richtschnur können dabei die folgenden Ausführungen des *Bundesgerichts* dienen:

> «Ein Schutz der Privatsphäre ist nur möglich, wenn das Informationsbedürfnis der Oeffentlichkeit 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.» (BGE 97 II 105)

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