VERA DELNON

Zwischen Öffentlichkeit und Strafrecht: Datenschutz – Quo vadis?

Inhaltsübersicht

Wissenschaftliches Arbeiten setzt Kenntnis der Tatsachen voraus. Beim Datenschutz wird das schwierig. Die Macht des Faktischen überholt jede Annäherung an das Thema schon vor der Drucklegung.

Datenschutz ist seit einigen Jahren ein vielbesprochenes Thema bei den Behörden des Bundes und der Kantone. Zu reden gibt er namentlich mit Blick auf den polizeilichen Bereich und die Strafverfolgung, die eine Sonderrolle beanspruchen. Gleichzeitig halten die modernen Technologien in rasantem Tempo Einzug bei Wirtschaft und Staat, bei Bürgern und Konsumenten. Von den daraus flies-

senden neuen Möglichkeiten geradezu überwältigt, übersehen wir leicht, in welcher Menge und in welchem Ausmass dadurch in ganz neuen Bereichen Berge von Daten anfallen.

Gesetzliche Regelungen mit Datenschutz-Funktion kennen wir schon lange. Wegen der neuen Technologien werden neue Lebensbereiche der Menschen datenmässig erschlossen. Deswegen haben wir eigens Datenschutzgesetze auf Bundes- und kantonaler Ebene eingeführt. Gleichwohl treten der Allgemeinheit die Bedeutung von Daten, deren Verwendung und die Ausbeutung von verdichteten Datensammlungen in diesen neuen Bereichen erst allmählich ins Bewusstsein.

Für eine Standortbestimmung im Bereich Datenschutz stellen sich folgende Fragen: Was soll mit dem Prinzip des Datenschutzes verwirklicht werden und was geschieht derweil in der realen Umwelt mit Blick auf dieses Ziel?

Die Antwort auf die erste Frage ist einfach. Wir konkretisieren die Verfassung, welche die persönliche Freiheit und die Würde des Menschen schützt.

Die Antwort auf die zweite Frage ist nicht so einfach. Sie verlangt eine Gesamtschau aus der Sicht eines Astronauten, der gleichzeitig alle tatsächlichen Arbeitsabläufe und Arbeitsschritte in allen Arten von staatlicher und wirtschaftlicher Betätigung überblickt und zudem über umfassende Kenntnisse aus der Informatik, der Technik, der Elektronik, aus Handel, Finanzwirtschaft etc. verfügt.

Aufgrund suboptimaler Positionierung und Wissensverdichtung müssen hier bescheidene Teilkenntnisse aus der Froschperspektive genügen. Für uns Strafrechtler ist das nichts Neues.

I. Die Grundidee des Datenschutzes

Zur ersten Frage: Was soll mit dem Datenschutz bewirkt werden?

Die EU-Richtlinie 95/46 vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenenbezogener Daten und zum freien Datenverkehr umschreibt die Grundidee des Datenschutzes am schönsten[1].

Abs. 2 *Einleitungsgründe*

«Die Datenverarbeitungssysteme stehen im Dienste des Menschen; sie haben, ungeachtet der Staatsangehörigkeit oder des Wohnorts der natürlichen Personen, deren Grundrechte und -freiheiten und insbesondere deren Privatsphäre zu achten und zum wirtschaftlichen und sozialen Fortschritt, zur Entwicklung des Handels sowie zum Wohlergehen der Menschen beizutragen.»

[1] Amtsblatt der Europäischen Gemeinschaften vom 23.11.1995, Nr. L 281 S. 31.

Abs. 10 Einleitungsgründe

«Gegenstand der einzelstaatlichen Rechtsvorschriften über die Verarbeitung personenbezogener Daten ist die Gewährleistung der Achtung der Grundrechte und -freiheiten, insbesondere des auch in Art. 8 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten und in den allgemeinen Grundsätzen des Gemeinschaftsrechts anerkannten Rechts auf die Privatsphäre. Die Angleichung dieser Rechtsvorschriften darf deshalb nicht zu einer Verringerung des durch diese Rechtsvorschriften garantierten Schutzes führen, sondern muss im Gegenteil darauf abzielen, in der Gemeinschaft ein hohes Schutzniveau sicherzustellen.»

Art. 1 Abs. 1 Gegenstand der Richtlinie

«Die Mitgliedstaaten gewährleisten nach den Bestimmungen dieser Richtlinie den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten.»

Die Schweizer Gesetzgebung ist dieser EU-Richtlinie um wenige Jahre vorausgeeilt und hat im BG über den Datenschutz vom 19. Juni 1992 (DSG) weitergehend – und in helvetischer Trockenheit – den Schutz der Grundrechte von natürlichen *und* juristischen Personen geordnet, über die Daten bearbeitet werden[2]. Die Botschaft zu diesem Gesetz nennt als Gründe für den erheblich gesteigerten Anfall von Datensammlungen und -verarbeitungen die Erweiterung der Handelsbeziehungen, den Einsatz neuer Verkaufsstrategien, neuer Methoden in der Unternehmensführung sowie die Zunahme und Diversifizierung der Kreditgeschäfte[3]. Vom DSG ausgenommen sind u.a. hängige Zivil-, Straf- sowie Staats- und Verwaltungsverfahren, wo aber dank der neuen Technologien auch immer mehr Datensammlungen anfallen.

Datenschutz ist wie gesagt aber nichts Neues. Datenschutz-Funktion haben die schon lange bestehenden Rechtsvorschriften betreffend das Amts-, Post-, Telefon-, Geschäfts- sowie das Berufsgeheimnis des Geistlichen, Anwaltes, Notars, Revisors, Arztes und Apothekers. Und wo wäre die Schweiz heute ohne ihr einstmals berühmtes Bankgeheimnis?

Hinzu kommen öffentlichrechtliche und privatrechtliche Regelungen, so zum Beispiel die Bestimmungen über das Recht auf Akteneinsicht und deren Beschränkung, ferner die Grundsätze des Persönlichkeitsschutzes, die vertraglichen und nachwirkenden Treuepflichten etc.

[2] SR 235.1; das Gesetz wird ergänzt durch die bundesrätliche VO zum BG über den Datenschutz (VDSG) vom 14.6.1993 (SR 235.11).

[3] Botschaft zum BG über den Datenschutz (DSG) vom 23.3.1988 (BBl 1988 II 413 ff., 416).

Allen diesen Regelungen liegt der Gedanke des ungeschriebenen Verfassungsrechts der persönlichen Freiheit sowie der Wahrung der Privatsphäre im Sinne von Art. 8 Ziffer 1 EMRK zugrunde[4].

Ein Blick auf die leidige Fichenaffäre und die heftige Reaktion der Bevölkerung darauf zeigt, dass es dem Schweizer ernst ist mit seinem Anspruch auf strikte Wahrung seiner Privatsphäre. Als in Zürich das kantonale Datenschutzgesetz vom 6. Juni 1993 zur Abstimmung gelangte, wurde es mit über 70% der Stimmen angenommen, obwohl grosse Parteien wie die FDP und die SVP die Nein-Parole verkündet hatten. Das Schutzbedürfnis des Bürgers wie auch sein Misstrauen im Bereich seiner Privatsphäre sind evident. Was wir mit den Datenschutz-Regelungen erreichen wollen, ist also klar.

Was aber mit Blick auf die Umsetzung dieser Ziele um uns herum geschieht, ist häufig unklar, wenn nicht gar im Dunkeln. Vor diesem Hintergrund hat das Deutsche Bundesverfassungsgericht schon im «Zensus-Urteil» vom 15. Dezember 1983 ein aus dem allgemeinen, durch die Verfassung geschützten Persönlichkeitsrecht fliessendes *Recht auf informationelle Selbstbestimmung anerkannt*: Eine «Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen».

Das Schweizerische Bundesgericht befand erstmals mit Entscheid vom 12. Januar 1990 im Zusammenhang mit verfassungsrechtlichen Fragen: «toute personne doit pouvoir garder la maîtrise des informations qui la concernent»[5]. Dieser Grundsatz ist auch in privatrechtlicher Sache in BGE 120 II 118 ff. E. 3a bestätigt worden. Er gilt natürlich nicht schrankenlos, z.B. nicht bei überwiegenden Allgemeininteressen.

Das Prinzip dieses «informationellen Selbstbestimmungsrechts» hat auch dem Datenschutzgesetz zugrundegelegen: Jedermann soll frei über seine persönlichen Daten sowie über die Aufnahme und Gestaltung seiner Informations- und Kommunikationsbeziehungen entscheiden können[6].

Es versteht sich von selbst, dass dieses Recht auf informationelle Selbstbestimmung zunächst einmal voraussetzt, dass der Bürger überhaupt weiss, wo und wie er mit den im Staat und auf dem Markt verfügbaren Technologien Datenspuren legt, wo diese Daten anfallen und was damit geschieht. Gerade das aber liegt oft im Dunkeln.

[4] Vgl. dazu statt vieler, je mit zahlreichen Hinweisen auf Literatur und Praxis: THOMAS W. SCHREPFER, Datenschutz und Verfassung, eine Untersuchung zur verfassungsrechtlichen Relevanz der Erfassung, Aufbewahrung und Weitergabe personenbezogener Daten, Bern 1985; NIKLAUS OBERHOLZER, Datenschutz und Polizei, in: Festschrift für Mario M. Pedrazzini, Bern 1990, 427 ff.; JÖRG SCHMID, Persönlichkeitsschutz bei der Bearbeitung von Personendaten durch Private, ZBJV 131 (1995) 809 ff.

[5] Semjud 112 (1990) 561 ff., 563, Erw. 2a. Vgl. dazu im Detail die Ausführungen von SCHMID (Anm. 4) 810 f.

[6] Botschaft zum DSG (Anm. 3) 418. SCHMID (Anm. 4) 811.

II. Datenschutz in der Bél-Etage – Dunkelräume im Sous-Sol

Das eigentliche Problem liegt nicht auf der Bél-Etage des gerichtlichen Verfahrens und der transparenten Verhältnisse, sondern im Sous-Sol der geheimen oder der unerkannt ablaufenden Vorgänge. Diesen Sous-Sol teilen sich das weite Feld der polizeilichen Ermittlungen und der intransparenten Verwaltungsvorgänge einerseits und die Wirtschaft mit ihren Geheimnissen andererseits.

Das erwähnte Misstrauen der Bürger bleibt oft in diffusen Gefühlen stekken, da in vielen Bereichen anstelle von offener Information unnötige Geheimniskrämerei vorherrscht. Es entlädt sich daher um so explosiver, wenn im Sous-Sol eine Panne eintritt und ein bisher verdecktes Geschehen plötzlich an der Oberfläche sichtbar wird. Das Malaise wird nicht weichen, sondern gegenteils zunehmen, wenn der beunruhigte Bürger nicht einmal weiss, mit welchen Dunkelräumen im «Sous-Sol» zu rechnen ist. Dabei reichen diese bis weit in unsere alltäglichsten Lebensvorgänge hinein.

Dazu ein Beispiel:

Seit Jahren überfluten mobile Telefone den Markt, ohne dass der Konsument über die Folgen des Gebrauchs aufgeklärt werden muss, geschweige denn aufgeklärt wird. Wer weiss schon, dass man als Halter eines betriebsbereiten Natel-C oder Natel-D pausenlos *Ortungssignale* aussendet, die den Datenempfängern jederzeit den Standort bzw. allfällige Bewegungen des Telefonkunden melden? Wer sind die Datenempfänger und was geschieht mit den Daten? Hat man jemals öffentlich diskutieren können, *was diesbezüglich überhaupt nötig ist*? Und weshalb besteht bei der Zulassung solcher Geräte auf dem Markt *keine Aufklärungspflicht* zuhanden des Käufers, damit er wenigstens entscheiden kann, ob er gewillt ist, solche Datenspuren zu legen?

Noch grotesker wird die Situation beim Natel-D, das als abhörsicher auf dem Markt angepriesen wird. Gerade wegen dieser Anpreisung und wegen seiner Einsatzfähigkeit weitherum in Europa hat das Natel-D viele Benutzer und Umsteiger angelockt.

Selbstverständlich ist das Natel-D nur *relativ* abhörsicher. Der Staat hört schon mit, wenn er will. Das Natel-D verbreitet ebenfalls Ortungssignale, ist aber nicht mehr auf das Gebiet der Schweiz beschränkt. Wenn mit dem Natel-D ins Ausland telefoniert wird, *so fallen bei rund einem halben Dutzend Rechnern im In- und Ausland automatisch die Verbindungsdaten dieses Telefonates an.* Falls wir überhaupt etwas davon wissen, dann wissen wir jedenfalls nicht, *wo* diese Daten anfallen und wer dort was mit diesen Daten macht. Dass ausländische private Telefongesellschaften über Joint-Ventures bereits weitgehend mit den staatlichen PTT-Betrieben verbandelt sind, liefert erst recht keinen Grund zur Entspannung.

Das ist aber noch lange nicht alles:

Über dem deutschen Telefonnetz wacht der Bundesnachrichtendienst zum Schutz von Staat und Verfassung. Er bedient sich dabei neuester Technologie: der computergestützten, automatisierten Spracherkennung. Diese Spracherkennung wird auf einschlägige Worte programmiert, mit deren Hilfe terrorverdächtiges oder organisiertes Verbrecherwerk sofort an der Wurzel erfasst werden soll. Das spielt sich zum Beispiel wie folgt ab:

Ein Schweizer spricht über eine deutsche Datenleitung und verwendet die verdächtigen Worte «Geld», «Konto» oder «Bank». Damit fällt er bereits in den Dunstkreis potentieller Geldwäscherei, welcher international mit allen Kräften Einhalt zu gebieten ist.

Die Spracherkennung ortet die Gefahr augenblicklich und schaltet automatisch den Mitschnitt des Gesprächs ein, natürlich ohne richterliche Genehmigung. Auch ohne vertiefte Kenntnisse in der Sprachforschung erhellt sofort, dass der Gebrauch von Wörtern wie «Geld», «Konto» oder «Bank» für sich allein keinen Tatverdacht begründen. In der Schweizerischen Juristischen Datenbank SWISSLEX figuriert der Begriff «Geld» 7024 mal, «Konto» 846 mal und «Bank» 6939 mal. Dabei sind die verschiedenen Wortformen (z.B. «Geldes») und die zusammengesetzten Begriffe (z.B. «Trinkgeld», «Gartenbank») noch nicht mitgezählt, welche nochmals ein Mehrfaches davon ausmachen, und die ebenfalls erkannt werden.

Man möchte glauben, Lombroso mit seinen Studien über die Erkennbarkeit des «delinquente nato» sei auferstanden. Wie kann ein Staat derart schwerwiegende Eingriffe in die persönliche Freiheit und die Privatsphäre seiner Bürger tolerieren, wenn schon eine Kosten-/Nutzenanalyse kein vernünftiges Resultat erbringen kann, ganz zu schweigen von der Frage nach der Verhältnismässigkeit? Unbeirrt von solchen Überlegungen halten es Verfassungsschützer offenbar für legitim, 99.99% der mit Deutschland kommunizierenden Bevölkerung abzuhören, um auf gut Glück einer Handvoll möglicher neuer Verbrecher auf die Spur zu kommen, die sich per Telefon der Wörter des allgemeinen Sprachgebrauchs bedienen. Dabei fallen unter den ohnehin unklaren Begriff der «organisierten Kriminalität» offenbar auch schon der Pflanzenschmuggel und das Hütchenspiel[7].

Leider sind *auch in der Schweiz* Bemühungen zur vorsorglichen Abhörung von Telefongesprächen ohne richterliche Genehmigung bereits weit fortgeschritten. Vielleicht scheitern sie noch an einem Vorstoss der Rechtskommission des Nationalrates vom Januar 1996. Der Ständerat jedenfalls hatte in seiner Sommersession die vorsorgliche Überwachung von Post- und Telefonverkehr aus Staatsschutzgründen mit 21 zu 14 Stimmen bereits gutgeheissen[8].

[7] BEAT LEUTHARDT, Leben online, Von der Chipkarte bis zum Europol-Netz, Hamburg 1996, 103.

[8] Gegen den «grossen Lauschangriff» im Staatsschutzgesetz, NZZ Nr. 20 vom 25.1.1996 S. 15.

Berufs- und sonstige Geheimnisträger haben sich bisher ohne weiteres darauf verlassen, dass die ihnen anvertrauten Geheimnisse den besonderen Schutz des Staates geniessen. Auch muss sich jeder Bürger selbstverständlich darauf verlassen können, dass die *Privatsphäre unantastbar* bleibt. Gerade im erwähnten Beispiel des mobilen Telefonverkehrs ist aber ernüchtert festzustellen, dass der *Staat seine Schutzfunktion gegenüber dem Bürger und Konsumenten nicht ernst nimmt.*

Das Misstrauen wird gewiss nicht geringer, wenn brisante Informationen oder Begleiterscheinungen über neue Entwicklungen, welche die Privatspähre des Bürgers tangieren, nicht zum vornherein offengelegt werden, weder im Parlament noch auf dem Markt. Denn dadurch wird dem Bürger und dem Konsumenten nicht einmal die Entscheidung ermöglicht, ob er unter diesen Rahmenbedingungen von den Errungenschaften des modernen Lebens Gebrauch machen will oder nicht, im Gegenteil. Die fehlende Aufklärung unterminiert auch sein Grundrecht auf «informationelle Selbstbestimmung». Dieses Nichtwissen macht ihn manipulierbar. Und das wiederum setzt zu Recht heftige Reaktionen gegen den Staat frei, dessen oberste Pflicht die Wahrung der Verfassung ist.

III. Die divergierenden Interessen im Bereich des Datenschutzes

Erschwert wird eine Klärung der Verhältnisse zunächst einmal durch die Inanspruchnahme teilweise diametral auseinanderklaffender Interessen der verschiedenen Seiten. Je nach Blickwinkel mögen diese Einzelinteressen durchaus verständlich oder vernünftig sein. Nur ist es keineswegs vernünftig, isoliert nur ein Einzelinteresse gesondert zu regeln ohne Blick auf das Gesamte. Leider verstehen sich Verwaltungsbeamte und Parlamentarier oft besser auf den geschärften Blick fürs Kleine statt auf die Erfassung der grossen Zusammenhänge.

Dazu ein Beispiel:

Der Eidgenössische Datenschutzbeauftragte konnte nur mit Mühe verhindern, dass eine weitere deutsche Spezialität Eingang in die Gesetzgebung unseres Landes genommen hat. Bei der Schaffung der kriminalpolizeilichen Zentralstellen des Bundes zur Bekämpfung des organisierten Verbrechens war ursprünglich vorgesehen, dass jedermann zur Ausübung seines Auskunftsrechts über die ihn betreffenden Personendaten zuvor einen «konkreten Tatbestand vorweisen» und ausserdem ein «schützenswertes Interesse» hätte nachweisen müssen.

Das widerspricht ganz klar unserer Verfassung und der Praxis des Bundesgerichts. Wie der Datenschutzbeauftragte zu Recht bemerkte, wäre die Einsichtnahme bei einer solchen Regelung *gerade all den Bürgern versagt, die sich nichts vorzuwerfen haben, und daher nicht fichiert sein sollten* – ein absurdes Ergebnis.

Es ist auch keineswegs einsichtig, weshalb sich diese neuen kriminalpolizeilichen Zentralstellen des Bundes vor dem ohnehin nicht schrankenlos gewährten Einsichtsrecht der Bürger schützen müssten. Das Gegenteil ist doch der Fall: Die neugeschaffenen Bundesstellen bearbeiten u.a. nicht ausgewiesene und teilweise nicht verifizierbare Informationen «aus dem In- und Ausland». Dazu gehören auch Angaben über blosse Ermittlungen und Vorprüfungsverfahren des Auslands oder Informationen von Personen, die unter die Rubrik «Polizeiverbindungsleute» fallen, was immer das heisst. Insbesondere aber gibt das fragliche Bundesgesetz auch die Erlaubnis zur Weitergabe dieser bearbeiteten, *nicht verifizierten Informationen ins Ausland zur «Verhütung» möglicher Straftaten*[9].

Obwohl also ein erhebliches Fehlerpotential gegeben ist und das Bundesgericht das verfassungsrechtliche Einsichtsrecht ja nicht schrankenlos gewährt, führte unser Parlament ausgiebige Debatten über die vorgeschlagene erhebliche Einschränkung des Auskunftsanspruchs der Bürger. Erst nach der Intervention des Datenschutzbeauftragten verabschiedete es mit einem «indirekten Auskunftsrecht» eine etwas mildere Form der Aushebelung unserer verfassungsmässigen Rechte[10].

Aber auch der Bürger selbst verlegt sich bei der Gewichtung in seiner politischen Willensbildung oft auf persönliche Einzelinteressen oder fällt gefühlsbestimmte Entscheide, weil ihm eine Schau auf die Rahmenbedingungen und ein Überblick über die Konsequenzen fehlt. So hat er ein unbestrittenes Recht auf Wahrung seiner persönlichen Freiheit und pocht auf den Schutz seiner Privatsphäre. Er verlangt aber auch volle Freiheit in jeglicher ökonomischen Betätigung. Besonders unter dem Eindruck medienträchtiger Einzelfälle ruft er nach straffer Verbrechensbekämpfung und -verhütung. Auf grösstmögliche Mobilität und Bequemlichkeit legt er ebenfalls Wert.

Wirtschaft und Staat tun, was sie können, um alle diese Interessen des Bürgers zu befriedigen. Dass dabei aufgrund der heute eingesetzten Technologien laufend EDV-Daten anfallen, ist eine normale Folge dieser Entwicklung. Im Bereich der Wirtschaft aber entstehen noch weit grössere Datenmengen als im Bereich der staatlichen Tätigkeit. Und wo heute noch Lücken bestehen, springt nicht selten der Staat ein – meist unter dem Titel Verbrechensbekämpfung und -verhütung.

Die Zeche bezahlt hüben wie drüben der Bürger, sei es über den Preis der von ihm konsumierten Güter und Dienstleistungen, sei es über die erlegten Steuern. Wem all diese Daten nutzen, wozu sie benutzt werden und wer sie nutzt, das wiederum ist eine Frage, die sich erst beantworten lässt, wenn im Sous-Sol Ordnung geschaffen wird. Bis dahin operieren wir mit verborgenen Dateien in unserem Erkenntnisprozess.

[9] BG über kriminalpolizeiliche Zentralstellen des Bundes vom 7.10.1994 (SR 172.213.71).
[10] Vgl. 2. Tätigkeitsbericht des Eidgenössischen Datenschutzbeauftragten (EDSB) 1994/1995, 12.

IV. Die Fakten: Datenspuren, wo wir stehen und gehen

Bedeutende menschliche Verhaltensweisen lassen sich datenmässig erfassen und werden bereits erfasst. Wir greifen die entscheidenden Bereiche heraus:

Der Bürger konsumiert, er kommuniziert, und er bewegt sich.

1. Allgemeine Personendaten und deren Spuren

Bevor sich eine Person in amts- und wirtschaftsrelevanter Weise betätigt, wird sie erfasst, mit Personaldokumenten sowie mit einer AHV-Nummer versehen.

2. Personaldokumente

Die neue Identitätskarte IDK 95 ist maschinell lesbar. Sie ermöglicht die vollautomatische Erfassung und Überprüfung ihres Trägers auf eine allfällige Ausschreibung im RIPOL (automatisiertes Fahndungssystem)[11]. Nach Versicherung des Eidgenössischen Datenschutzbeauftragten in seinem Tätigkeitsbericht soll der in der Identitätskarte enthaltene Code keine Informationen über den Träger aufführen, die nicht auch in lesbarer Form sichtbar sind. Ferner werden die im RIPOL enthaltenen Datensätze nach Revokation einer Ausschreibung wieder gelöscht und nicht nur als «revoziert» im System belassen, wie es aufgrund der Formulierungen in der VO über das automatiserte Fahndungssystem vom 19. Juni 1995 angenommen werden könnte. Gelöscht werden auch die durch die maschinelle Einlesung der Identitätskarte gewonnenen Daten[12].

Der Europäische Pass der EU-Bürger ist ebenfalls maschinell lesbar und codiert. Wie es sich mit der Verwendung und Archivierung der maschinell erfassten Ein- und Ausreisedaten verhält, richtet sich nach den Bestimmungen der einzelnen Länder. Falls die Daten aufbewahrt werden dürfen, so zeigt sich hier bereits ein bedeutender Unterschied gegenüber früher: Bisher wurde ein Pass gestempelt, verblieb aber bei seinem Träger. Nur bei einer entsprechenden Rechtsgrundlage konnten der Pass eingesehen und so die Bewegungen seines Trägers überprüft werden. Bei der alten Identitätskarte erfolgte nicht einmal eine Stempelung. Sind die Grenz-Kontrolldaten aber in einer Datensammlung abgelegt, so kann der Staat die Bewegungen jedes Reisenden jederzeit und ohne besonderen

[11] VO über das automatisierte Fahndungssystem vom 19.6.1995 (SR 172.213.61).

[12] Vgl. 1. Tätigkeitsbericht 1993/94 des Eidgenössischen Datenschutzbeauftragten, 15.

Grund einsehen oder zum Beispiel bei Interpol-Anfragen ohne formelle Rechtshilfe, d.h. insbesondere ohne Nachweis eines Tatverdachts oder einer angehobenen Strafuntersuchung, ins Ausland abgeben.

3. AHV-Nummer

Wer in der Schweiz lebt, hat seine persönliche AHV-Nummer. Viele Menschen wissen nicht, dass diese Nummer einen sprechenden Code darstellt. Er besteht aus einer Verschlüsselung des Familiennamens, des Jahrgangs, des Geschlechts und der Herkunft. Dank ihrer Genauigkeit ermöglicht eine AHV-Nummer die Identifikation der zugehörigen Person. Sind umgekehrt die vorerwähnten Angaben einer Person bekannt, kann auf deren AHV-Nummer geschlossen werden.

Da die AHV-Nummer ein eindeutiges Zuordnungskriterium für Personendaten darstellt, bauten die amtlichen Datensammlungen seit jeher auf ihr auf. Sie können daher auch über die AHV-Nummer personenbezogen abgefragt werden.

Werden Steuererklärungen vom Amt versandt, ist die AHV-Nummer durch das Adressfenster leicht ablesbar. In militärischen Angelegenheiten figurierte sie bis vor kurzem sogar aussen auf dem Couvert.

V. Datenspuren bei jeder Konsumation mittels Plastikkarten

Wenn ein Anwalt morgens um 07.00 Uhr für sich und einen Klienten zwei Flugtickets beim Swissairschalter beziehen und über seine VISA-Karte seinem Zürcher Bankkonto belasten will, sollte er wissen, dass die Details seiner Belastung von einem VISA-Center womöglich *in England* bearbeitet werden, während gleichzeitig die SWISSAIR alle Ticketangaben samt der auf den Flugscheinen vermerkten VISA-Kartennummer *in Indien* verarbeiten lässt. Der Anwalt wird nicht darüber informiert und ist sich wohl kaum bewusst, dass er dadurch einer unbekannten Anzahl von ihm unbekannten Personen Umstände bekanntgibt, die er grundsätzlich geheimzuhalten hätte, und die er auch sonst kaum nach England und Indien weiterleiten möchte.

Der Einsatz von Kreditkarten wie VISA oder Eurocard/Mastercard, Diners oder American Express wird aggressiv beworben. Wer über Kreditkarten Reisen bucht, wird automatisch versichert, kann billiger telefonieren, die Rechnung in Raten abstottern etc. Je mehr die Kreditkarte belastet wird, desto höher sind die Vergünstigungen. Aber er liefert dafür auch etwas: Daten über die Details seiner Konsumationen samt Orts- und Zeitangaben, die Verbindungsdaten seiner Tele-

fonate, Details über seine Bewegungen, Angaben über seine Kaufkraftklasse, sein generelles Konsumationsverhalten, kurz: ein Persönlichkeitsprofil, das einem geschulten Auge mehr über die betreffende Person aussagen kann, als diese selbst schon bemerkt hat.

1. Datensammlungen als Instrumente strategischer Planungen ...

Insbesondere liefern *alle Kartenbenutzer gesamthaft* betrachtet wiederum wichtige Informationen, denn durch die *Verdichtung von Daten in einer Datensammlung* werden ihrerseits wiederum *neue Informationen, Gesetzmässigkeiten und Muster* erkennbar, die aus einzelnen Persönlichkeitsprofilen nicht gewonnen werden können. Die Verdichtung von Informationen liefert bedeutende Erkenntnisse verschiedenster Art, z.B. bezüglich des Kaufverhaltens verschiedener Kaufkraftklassen, bezüglich einzelner Produkte und Dienstleistungen etc. Darin liegt ein besonderer und ökonomisch nutzbarer Wert von Datensammlungen, den aber natürlich nur der Betreiber der Datensammlung nutzen (und ausnutzen) kann. Der Literaturboom in diesem Bereich ist beeindruckend.[13]

Dass dieser besondere Wert von Datensammlungen bekannt ist und auch genutzt wird, ist keine Mär. So wurde vor rund zwei Jahren aus den Niederlanden bekannt, dass anlässlich der Lancierung einer neuen Kreditkarte die involvierte Unternehmung Geschäfte und Shops mit dem Argument zu ködern versucht hatte, ihnen würden die Persönlichkeitsprofile der Kunden zur Verfügung gestellt. Tatsächlich ermöglichen Datenbanken je nach ihrer konkreten Ausgestaltung jede nur erdenkliche Auswertung durch deren Betreiber.

2. ... ohne Bankgeheimnis

Die Kredit-Kartenorganisationen stehen zwischen dem Kunden und dessen Bank und unterliegen daher mit Bezug auf die bei ihnen anfallenden Daten nicht dem Bankgeheimnis. Dasselbe gilt für die von der Kreditkarten-Organisation allfällig mit der Datenverarbeitung unterbeauftragten Gesellschaften. Demnach fehlt hier die den Banken direkt auferlegte Beschränkung, die von den Kunden anvertrauten Daten zu verdichten, sie zu vergleichen und sie für markt- oder konsumrelevante Studien zu nutzen.

Auch die drei Schweizer Grossbanken haben Lizenzverträge mit Kartenorganisationen. So geben SBG und SKA die Eurocard/Mastercard an ihre Bankkun-

[13] Vgl. zum Thema MARC-ANDRÉ PRADERVAND, Die Rolle des Informationsmanagements beim Aufbau strategischer Erfolgspositionen, Diss. Zürich 1995, mit zahlreichen Literaturhinweisen.

den ab, der Schweizerische Bankverein die VISA-Karte. Wer die Trägergesellschaften dieser Kreditkarten sind und wie, wo bzw. durch wen die Verarbeitung der anfallenden Daten erfolgt, gehört nicht zur üblichen Kunden-Information. Im vorliegenden Fall verarbeitet die Telekurs AG alle anfallenden Daten im Zusammenhang mit der Eurocard-Nutzung, während VISA zu diesem Zweck in jedem Land zwar eigene Rechenzentren in ihren VISA-Centers unterhält, in der Schweiz aber das Clearing mit dem Schweizerischen Bankverein ebenfalls durch die Telekurs ausführen lässt.

Die Telekurs AG ist eine gemeinsame Tochter der Schweizer Grossbanken und der Kantonalbanken und führt für diese u.a. Online-Datenbanken.

Je länger je mehr wird der Einsatz von Bargeld durch den elektronischen Zahlungsverkehr ersetzt. Wir müssen uns bewusst sein, dass wir damit Datenspuren legen, deren Ausmass und Verbreitung wir keineswegs überblicken.

VI. Datenspuren bei Geschäftstransaktionen

Da Bank- und Finanzgeschäfte ohne EDV heute nicht mehr denkbar sind, hinterlässt jede geschäftliche Transaktion über die Bank, Post oder Konti aller Art Datenspuren.

1. Staatliche Überwachung von Geschäftstransaktionen

Die Amerikaner, Vordenker der grossen Freiheit, sind auch Vorläufer im Versuch, der grossen Freiheit die totale Kontrolle entgegenzusetzen. In den Vereinigten Staaten ist heute schon *jede einzelne Banktransaktion im Wert ab US-$ 10'000.– von Gesetzes wegen meldepflichtig*. Das betrifft ohne weiteres auch Dollar-Transaktionen innerhalb der Schweiz, da diese regelmässig über die Dollarkonten unserer Banken in den USA abgewickelt werden.

Das ist aber keine spezifisch amerikanische Erscheinung. Gegenteils wird der Druck auf Europa immer grösser, es den USA gleichzutun. Bei jeder Gelegenheit wird uns mit der Einziehung von europäischen Werten auf dem Gebiet der Vereinigten Staaten gedroht. Das jüngste Beispiel stellt die absurde Forderung über 125 Milliarden US-Dollar gegen den Kanton Tessin dar, die nach schweizerischem Rechtsempfinden zwar unsittlich ist, aber gleichwohl Krisensitzungen auszulösen vermag[14].

[14] NZZ Nr. 24 vom 30.1.1996 S. 21, «Groteske Geldforderung der USA an das Tessin».

Am 1. Januar 1996 trat in Deutschland die Wertpapier-Meldepflicht für alle deutschen Kreditinstitute, Niederlassungen ausländischer Banken sowie die Mitglieder der deutschen Börsen in Kraft. Mitzuteilen sind nicht nur die Aktivitäten in Deutschland, sondern die Transaktionen in allen Effekten oder Termingeschäften, die an einer Börse innerhalb der EU oder eines EWR-Vertragsstaates zum Handel zugelassen sind.

Informiert werden muss auf elektronischem Wege über jedes Geschäft inklusive Zeitpunkt, Preis, Volumen, Kauf oder Verkauf, Eigen- oder Kundengeschäft. So fallen pro Handelstag 200'000 bis 300'000 Geschäftsabschlüsse auf dem Rechner des Bundesaufsichtsamts für den Wertpapierhandel an. Ermitteln die eigens dafür konzipierten Computerprogramme eine «verdächtige» Häufung von Käufen, so wird das Bankgeheimnis unterlaufen. Begründet wurde diese staatliche, zentrale Überwachung des Handels mit Wertpapieren und Derivaten mit der *Aufdeckung von Verstössen gegen das Insiderhandelsverbot*[15].

Bei 220 Handelstagen fallen den publizierten Angaben zufolge also bis zu *66 Millionen detaillierte Meldungen pro Jahr* an, die elektronisch entsprechend aufbereitet, abgeliefert, verwaltet und ausgewertet werden müssen. Die damit einhergehenden Zeit- und Kostenaufwendungen berappen wie immer der «vorsorglich» registrierte Kunde und die übrigen Bürger. Und welcher Nutzen soll diesen Kosten die Waage halten?

Nehmen wir zum Vergleich die in der Schweiz bekannten Zahlen zum verbotenen Insiderhandel. Bei uns ist die Insiderstrafnorm (Art. 161 StGB) seit 1. Juli 1988 in Kraft. Sie bedroht Widerhandlungen mit Busse oder mit Gefängnis bis maximal drei Jahre. Zur Aufdeckung eines spektakulären Falles, bei dem jemand geschädigt worden wäre, ist es seither noch nie gekommen. In Zürich wurden in den bald acht Jahren nur zwei Fälle zur Anklage gebracht, die mit Freisprüchen endeten. Einmal soll es in Genf zur Ausfällung eines Strafbefehls mit Busse gekommen sein.

Aus diesen Zahlen lässt sich nicht schliessen, dass Insidervergehen volkswirtschaftlich von solcher Bedeutung sind, dass sich der erwähnte Zusatzaufwand nebst den ohnehin zur Verfügung stehenden kriminalistischen Mitteln rechtfertigen liesse. Wie aber bereits gesagt wurde, lassen solche immensen Datensammlungen je nach Auswertungskriterien u.U. bedeutende Rückschlüsse auf sonstige Umstände zu, die mit Verbrechensbekämpfung nichts zu tun haben[16].

Was die Kriminalitätsbekämpfung angeht, so besteht merkwürdigerweise in der Öffentlichkeit und sogar in den Parlamenten genau das umgekehrte Bild. Insiderdelikte wie auch etwa Geldwäscherei gelten als Dauerbedrohung. Hartnäckig

[15] NZZ Nr. 302 vom 29.12.1995 S. 27, «Deutsche Wertpapier-Meldepflicht in Kraft».

[16] Vgl. die immense Literatur über die strategischen Möglichkeiten durch «Informationsmanagement» z.B. bei PRADERVAND (Anm. 13) 313 ff.

hält sich auch die Vorstellung, die schwere Kriminalität nehme ständig zu, obwohl, wenn man es differenziert betrachtet, das Gegenteil der Fall ist[17].

Entgegen der vorherrschenden Meinung ist die schwere Kriminalität seit 1980 nicht steigend, sondern *sinkend*, wenn die Betäubungsmittel-Beschaffungsdelikte separat betrachtet werden. Einerseits fällt jeder Suchtkranke, der gewaltsam eine Zwanzigernote an sich bringt, unter den Straftatbestand des Raubes und belastet somit die Statistik zur schweren Kriminalität. Andererseits haben sich das Drogenproblem und insbesondere die damit einhergehenden Beschaffungsdelikte über viele Jahre vor allem deshalb stark ausbreiten können, weil es an der politischen Schubkraft zur tatkräftigen Bewältigung des Drogenproblems und der Szenenbildung gefehlt hat. Stattdessen konzentrierten sich diese Kräfte vor allem darauf, diejenigen Vorstösse zu Fall zu bringen, die die Probleme lösen wollten.

Gleichwohl ist eine Entwicklung im Gange, die unter dem Titel Verbrechensbekämpfung und Verbrechensverhütung ständig neue Datensammlungen und Eingriffe in die persönliche Freiheit aller Bürger vorsieht, obwohl deren *kriminalistischer Wert in homöopathischen Einheiten* gemessen werden muss.

Es kann daher nicht schaden, wenn wir uns inskünftig – bevor wir weiteren Eingriffen in unsere Privatsphäre zustimmen – jeweilen die Mühe einer Kosten-/Nutzenanalyse machen.

VII. Datenspuren bei Kommunikation unter Abwesenden

1. Telefon

Vom wichtigsten Kommunikationsmittel, dem Telefon, war bereits oben im Zusammenhang mit dem Natel und mit der Belastung der Gebühren über die Kreditkarte die Rede.

Bekanntlich schützt uns seit einigen Jahren unser Fernmeldegesetz davor, auf dem detaillierten PTT-Taxauszug, der Fr. 4.80 extra kostet, die Nummern der von unserem Anschluss aus angerufenen Abonnenten vollständig einzusehen. Das ist eine Errungenschaft des schweizerischen Datenschutzes zugunsten derjenigen Personen, die auf unsere Kosten Privatgespräche führen. Dafür fallen wie gesagt dieselben Daten gratis und vollständig an bei Kreditkarten-Organisationen, bei beliebigen in- und ausländischen Rechnern oder beim Einsatz von Telefonkarten oder Hauszentralen. Einer im Jahr 1993 an den Nationalrat gerichteten Petition um Aufhebung dieser Regelung im FMG war kein Erfolg beschieden.

[17] Vgl. VERA DELNON/BERNHARD RÜDY, Untersuchungsführung und Strafverteidigung, ZStrR 106 (1989) 47 ff.

Umgekehrt wurde übersehen und nicht darüber informiert, dass bei der Aufnahme des kommerziellen Betriebes von ISDN im «SwissNet 2» und seiner bedeutend erweiterten Möglichkeiten unverhofft Nachteile für Personen entstehen, welche aus Gründen des Persönlichkeitsschutzes eine nicht eingetragene Telefonnummer erhalten haben oder für Personen, welche anonym eine Beratungsstelle anrufen möchten. Deren Nummern scheinen im Display eines an das ISDN angeschlossenen Apparates auf, ohne dass der Anrufer davon weiss. Eine Rufnummerunterdrückung ist heute nicht möglich[18].

Ohne Wirkung blieben auch die Vorstösse im Parlament, welche bei richterlich genehmigten Telefonüberwachungen diejenigen Abhörungen automatisch ausgenommen haben wollten, die der Verfolgte mit dem Geistlichen, Arzt oder Anwalt führt.

2. Datennetze

Die Kommunikation via Datennetze boomt. Ständig werden neue Bereiche in der sich eröffnenden virtuellen Welt erschlossen. Telebanking, Teleshopping, Internet-Surfing zu Vergnügungs- und Weiterbildungszwecken – alles ist möglich.

Nichts hingegen geht ohne Hinterlassung von umfangreichen und detaillierten Datenspuren. Bereits mehr als 40 Millionen Benutzer zählt das Internet, welches unbeschränkte Möglichkeiten zur Einholung und zum Austausch von Informationen, zum Güterkauf und zum Bezug von Dienstleistungen bietet. Die Bewegungen in der virtuellen Welt erfährt der Benutzer als unpersönlich, weil er weder sein Gesicht zeigt, noch Stimme oder Handschrift einsetzt. Gleichwohl ist er nicht etwa anonym unterwegs. Bei jedem Server, auf dem er einkehrt und etwas anschaut, können nicht nur seine Koordinaten samt Name registriert werden, sondern sogar die aktuelle Version der von ihm benutzten Kommunikationssoftware. Für den Versand von E-Mails bieten daher neue Dienstleister im Internet einen «Re-Mailer-Service» an: Man schickt seine E-Mail zu diesem Dienst, wo der Absender von der Nachricht abgetrennt und vor der Weiterleitung durch denjenigen des «Remailers» ersetzt wird.

[18] Vgl. 2. Tätigkeitsbericht EDSB 1994/1995, 32 f. sowie Tages-Anzeiger vom 4.7.1995, «Geheime Nummern beschränkt geheim, Datenschutzbeauftragter warnt vor Risiken in der Telekommunikation».

VIII. Datenspuren bei jeder Bewegung

Wer mit der Postcard telefoniert, lässt das Telefongespräch auf dem Postkonto belasten und erhält eine monatliche Abrechnung. Der Datenschutzbeauftragte hat bereits darauf hingewiesen, dass aufgrund der registrierten Daten von Ort, Zeit und angerufenen Nummern ein nicht unbedenkliches *Bewegungsprofil* entstehe[19]. Wird zum Telefonieren die 1995 von der PTT neu lancierte Calling Card «Swiss Telecom Card» benutzt, so läuft dieses Bewegungsprofil samt allen Telefondaten sogar noch über den Rechner des Calling Card-Anbieters und die zugehörige Kreditkarten-Organisation.

Dasselbe gilt natürlich – wie bereits oben ausgeführt – für alle Konsumationen, die der Kreditkarten-Kunde an verschiedenen Orten und zu verschiedenen Zeiten über seine Karte bezahlt. Nebst dem Persönlichkeitsprofil entsteht immer auch ein Bewegungsprofil.

IX. Datenspuren im Verkehr

GPS steht für das von 24 Satelliten getragene Global Positioning System. Damit kann jedes mit einem GPS-Navigator ausgerüstete Objekt auf der Erde genau seine Position feststellen und seine Bewegungen verfolgen. Was ursprünglich rein militärischen Charakter hatte, wird – allerdings mit geringerer Genauigkeit – längst zivil genutzt.

Dank dem Global Positioning System kann der amerikanische Grossbauer inzwischen seine weiten Felder optimal bedüngen, wenn er gestützt auf die erstellten Landschafts-Übersichtsbilder Nährstoffmängel erkannt hat und sich mit dem GPS-Navigator auf seinem Traktor zum richtigen Fleck führen lässt[20]. Das geodätische Institut der ETH Zürich arbeitet seit einiger Zeit mit GPS. Mit besonderer Nachbearbeitung der Daten wird heute eine Genauigkeit von unter 1 cm erreicht. Mercedes hat GPS als Verkehrsleitsysteme versuchsweise schon in Autos eingebaut[21]. Lastwagen, Mietwagen und Taxis werden bereits öfters nachgerüstet.

Die Überlegungen bleiben aber nicht bei den Möglichkeiten der Verkehrs- und Stauplanung stehen. Schon jetzt wird darüber nachgedacht, ob nicht Systeme

[19] Vgl. 2. Tätigkeitsbericht EDSB 1994/1995, 47.
[20] Vgl. Precision farming, Satellitennavigation für die Landwirtschaft, NZZ Nr. 1 vom 3.1.1996 S. 10.
[21] GPS – militärisches Navigationssystem mit zivilem Nutzen, Basler-Zeitung Nr. 279 vom 29.11.1994 S. 3.

mit Peil- bzw. Ortungsmöglichkeit inskünftig serienmässig so in Fahrzeuge eingesetzt werden sollten, dass die jederzeitige Auffindung gestohlener oder verunfallter Fahrzeuge oder die Verfolgung von Kriminellen in Fluchtautos möglich wäre. Satellitentechnologie, GPS, GMS (Global Monitoring System), GSM (Global System for Mobile Communication) etc.: Damit könnte jedes Fahrzeug jederzeit in jeder Bewegung erfasst werden. Heute sind gegen 1'000 Satelliten im Einsatz, davon mehrere hundert in privater Hand. Und zur Genauigkeit: Spionage-Satelliten entziffern die Marke auf einer Zigarettenschachtel. Die Ortung eines betriebsbereiten Natel-D und erst recht des kommenden Natel-E ist schon viel präziser als diejenige noch des Natel-C, die im Kilometerbereich lag.

X. Chipkarten

Im Gegensatz zu Wertkarten, die zum voraus bezahlt und wie Bargeld «verbraucht» werden, ermöglichen *Chipkarten* die nachträgliche Verbuchung von konsumierten Dienstleistungen. Dazu wird der Karteninhaber aber *identifiziert,* und es werden Angaben über Ort, Zeit und Details der konsumierten Dienstleistung erfasst.

Die Chipkarten arbeiten wie Kleinstcomputer. Sie weisen keinen Magnetstreifen mehr auf, sondern einen Mikrochip. Mit ihnen kann nicht nur telefoniert und eingekauft werden. Wie das im neuen Flughafen München demonstrierte Beispiel zeigt, werden Chipkarten erfolgreich für die 20'000 Mitarbeiter mit ihren verschieden weitgehenden Zutrittsberechtigungen eingesetzt. Die Berechtigungs- und die Bewegungsprofile all dieser Personen sind dank Chipkarte einzeln jederzeit verfügbar und abfragbar. Ausschliesslich mit der auf sie persönlich programmierten Benutzer-Chipkarte können die Flughafenangestellten, die Flughafen-Polizisten, die internationalen Stewardessen, das Raumpflege- und Küchenpersonal parkieren, tanken, Zutritts- und Durchgangsschleusen passieren, einkaufen, in der Kantine essen, telefonieren, faxen und ihre Voice-Mail abfragen[22].

Nebst der Sicherheit im Betrieb wird mit dem Einsatz solcher Mittel auch die lückenlose Überwachung und Arbeitskontrolle aller Mitarbeiter nicht nur möglich, sondern auch abspeicherbar.

[22] LEUTHARDT (Anm. 7) 164 f.

XI. Kein Datenschutz ohne Datensicherheit

Datenschutz setzt Datensicherheit voraus. Datensicherheit wiederum ist ein weites Feld, das den Rahmen dieser Arbeit bei weitem sprengen würde. Einige kurze Anmerkungen sind aber nötig:

Datensicherheit bedeutet zunächst einmal Sicherheit über die Richtigkeit und die Aussagekraft von Daten. *Informationen entstehen nicht nur an der Quelle.* Elektronische Einlesungen werden auch in zehn Jahren noch fehleranfällig sein.

Mit der Erhebung und Bearbeitung von Daten sind nicht «unfehlbare Ämter» oder «bestrenommierte Unternehmen» befasst, sondern die dort beschäftigten Tausende von Menschen mit unterschiedlichstem Ausbildungsniveau, Verantwortungs- und Pflichtbewusstsein und wechselnder Tagesform. Ständiger Personalabbau, Budgetrestriktionen und steigender Stress auf den verbleibenden Mitarbeitern nehmen Einfluss auf Sorgfalt und Genauigkeit in der Arbeit und damit auf die Qualität der Datenbewirtschaftung. Auch aus diesen Gründen ist die Überprüfung erhobener und verwendbarer Daten so wichtig. Zu Recht schützt unsere Verfassung das Einsichts- und Auskunftsrecht des Betroffenen, und dabei sollte es wenn immer möglich bleiben.

Datensicherheit bedeutet aber auch Sicherheit vor nachträglicher Verfälschung von Daten oder unzulässiger Vernichtung, Sicherheit vor unzulässiger Einsichtnahme oder Datenklau. Diese Probleme verschärfen sich erheblich bei elektronischen Systemen im Vergleich zu den herkömmlichen Registern[23].

Unter das Thema Datensicherheit fällt auch die Frage der Verschlüsselung von Datenübermittlungen und Telefongesprächen. Dafür existiert heute ein eigenständiger, jedem zugänglicher Markt.

Bereits seit 1993 unternimmt die US-Regierung Bemühungen, das Verschlüsselungswesen an sich zu ziehen und den *Clipper Chip* für alle Kommunikationsgeräte und Computer vorzusehen. Der Clipper Chip soll die Kommunikation zwischen zwei Geräten verschlüsseln zum Schutz vor Dritten, allerdings mit der Einschränkung, dass der Staat in jedem Fall über den Schlüssel verfügt. Natürlich ist die sichere Verschlüsselung eine Fiktion. Das ist in den USA erkannt und diskutiert worden. Zu Recht erschraken viele ob der Vorstellung, dass alle Menschen nur einen bestimmten Schlüssel benützen dürfen, dessen Doppel sich in der Hand des Staates befindet. Als dem Clipper Chip Sicherheitsfehler nachgewiesen werden konnten, geriet das Projekt in den USA vorübergehend in den Abwind. Kürzlich wurde aber der *Clipper Chip II* vorgestellt, welcher nun ganz sicher «ganz sicher» sein soll.

[23] Der im Januar 1996 in Schweizer Kinos ausgelaufene amerikanische Computer-Thriller «The Net» mit Sandra Bullock gibt einen interessanten Einblick in dieses Thema.

In den Köpfen europäischer Regierungen wird die Idee des Clipper Chip mit wachsendem Interesse verfolgt. In einer Empfehlung des EU-Ministerrates vom 11. September 1995 nimmt sie erste Formen an.

XII. Von den zukünftigen Möglichkeiten

Die Chipkarte, welche Personalausweis, Fahrausweis, Versicherungsausweis, medizinische Daten, Schlüssel, Kontoberechtigungen und Zahlungsmittel in einem enthält, ist nicht nur denkbar, sondern auch machbar. Sie steht als konkrete Möglichkeit im Raum. Bereits heute lernen wir aus der Werbung, wie lästig die Verwendung von vielen verschiedenen Karten sei.

Parallel laufen intensive Bemühungen zur Schaffung einer Einheitswährung in Europa. Von der Einheitswährung weg – hin zur *blossen Kontoberechtigung* ist ein immerhin denkbarer Weg. Alle kostenrelevanten Angelegenheiten müssten dann ausschliesslich über Banken (oder eventuell die Post) abgewickelt werden.

Die Vorstellung, dass unsere jederzeitige Ortung im Verkehr aus Sicherheits-, Gesundheits- oder aus Verkehrsplanungsgründen für unerlässlich erklärt werden könnte, gerät zum Albtraum.

In den Offenbarungen des Johannes, 13, 17, heisst es: «Kaufen oder verkaufen konnte nur, wer das Kennzeichen trug: den Namen des Tieres oder die Zahl seines Namens.» Keine Utopie.

XIII. Schlussfolgerungen

Die persönliche Freiheit und das Recht auf Wahrung der Privatsphäre schützen die Würde des Menschen. Zu Recht beanspruchen sie Verfassungsrang. Der Mensch entscheidet, ob die modernen Technologien ihm dienen sollen, oder ob er sich dadurch zum kontrollierten Objekt macht. Er hat es in der Hand, vorweg festzusetzen, ob und welche Daten elektronisch überhaupt aufgezeichnet und welche davon behalten werden sollen. Das sind rein praktische und technische Fragen. Wir können und müssen sie in Zukunft differenzierter angehen und unsere Bedingungen festlegen.

Ein Eingriff in die Privatsphäre durch Erfassung, Speicherung und Auswertung von personenbezogenen Daten bedarf einer überzeugenden Begründung. Eine Datenerhebung muss nötig und unumgänglich sein. Die Abwägung zwischen den verfassungsmässig geschützten Rechtsgütern und einem kriminalistischen Bedarf

soll nur dann zulasten der Grundrechte gehen, wenn der Eingriff zwingend notwendig ist zum Schutz klarer, höherwertiger Allgemeininteressen.

In jedem anderen, insbesondere im privatwirtschaftlichen Bereich, sind Verfassungsverletzungen nicht zu rechtfertigen. Der epidemische Anfall von personenbezogenen Datensammlungen im Gefolge neuer Technologien, Marktentwicklungen und Dienstleistungen ist zu unterbinden.