ITA manu:script
INSTITUT FÜR TECHNIKFOLGEN-ABSCHÄTZUNG

Beeinträchtigung der Privatsphäre in der Informationsgesellschaft

Gunther Tichy
Walter Peissl

http://www.oeaw.ac.at/ita/pdf/ita_01_01.pdf

ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN

Wien, 12/2001
ITA-01-01
ISSN 1681-9187

http://www.oeaw.ac.at/ita/pdf/ita_01_01.pdf

Dezember/2001
(ITA-01-01)

Beeinträchtigung der Privatsphäre in der Informationsgesellschaft

Gunther Tichy, Walter Peissl

Keywords

Privatsphäre, Privacy, Informationsgesellschaft, Datenschutz, problemorientierte Technikfolgenabschätzung

Abstract

Digitalisierung, Miniaturisierung und Vernetzung haben die Voraussetzungen für eine Informationsgesellschaft geschaffen, die durch Sammlung, Speicherung und Verknüpfung enormer Datenmengen und deren breite Verfügbarkeit gekennzeichnet ist. Das schafft für die meisten Staatsbürger erhebliche Vorteile, die durch Schlagworte wie E-Mail, Internet, E-Commerce, aber auch elektronische Erledigung von Behördenwegen umschrieben werden können. Die verfügbaren Datenmassen entfalten aber auch ein Eigenleben, das in die Privatsphäre der meisten Staatsbürger in vielfacher Weise eingreift; den meisten ist gar nicht bewusst, wieviel Informationen über sie verfügbar sind und z. T. auch gehandelt werden. Im Folgenden sollen zunächst die neuen technischen Möglichkeiten der Informationssammlung, -speicherung und -verknüpfung beschrieben werden; es wird aufgezeigt, welche dieser neuen Möglichkeiten vom wem genutzt werden, und mit welchen Konsequenzen. Dann wird das Janusgesicht der Informationsgesellschaft herausgearbeitet, die kritische Austauschbeziehung zwischen Effizienz und Sicherheit auf der einen Seite, die durch die intensive Informationssammlung und -verarbeitung überhaupt erst ermöglicht wird, und dem daraus resultierenden z. T. tiefen Eindringen in die Privatsphäre auf der anderen. Aus einer Diskussion der bestehenden Datenschutzbestimmungen wird versucht, erste Ansatzpunkte für Lösungen abzuleiten. Das stößt auf zahlreiche Schwierigkeiten: Die Dynamik des Sektors, ein in weiten Bereichen noch mangelndes Problembewusstsein, international erheblich differierende Vorstellungen über Art und Umfang der Schutzbedürftigkeit, aber auch die Tatsache, dass es einer ausgewogenen Kombination gesetzlicher Maßnahmen mit Selbstbeschränkung, also bewusstem Verzicht der Nutzer auf manchen Komfort bedarf.

der Österreichischen Akademie der Wissenschaften
A-1030 Wien, Strohgasse 45/5, Fax: +43-1-710 98 83
http://www.oeaw.ac.at/ita/
ISSN 1681-9187

Inhalt

Ein Vortrag von Gunther Tichy auf der Tagung der Österreichischen Juristenkommission über „Grundrechte in der Informationsgesellschaft“ am 24. Mai 2001 in Weißenbach am Attersee. Der Vortrag beruht auf den ersten Ergebnissen des Forschungsprogramms „Beeinträchtigung der Privatsphäre in der Informationsgesellschaft“ des Instituts für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften; die Autoren danken ihren Kollegen für wertvolle Hilfe bei der Abfassung des Manuskripts.

1 Der traditionelle Datenschutz ist obsolet geworden

In der Vergangenheit, die durch die bestehenden Datenschutzbestimmungen noch immer weitgehend gespiegelt wird, wurden Informationen systematischen Inhalts (zumeist Bestandsdaten), die ein Themenfeld abdecken, durch eine i.d.R. öffentliche Stelle auf gesetzlicher Basis planmäßig erhoben (z. B. Sozialversicherungsdaten, Großerhebungen der Statistik) und durch Zugangsbeschränkungen geschützt. Diese Art von Daten und ihr Schutz sind heute kaum noch Gegenstand der Diskussion;[1] sie haben tendenziell massiv an Bedeutung verloren. Viel typischer für die Informationsgesellschaft – und zugleich viel problematischer – sind einerseits die Zentralisierung und Digitalisierung personenbezogener administrativer Statistiken, die dadurch umfassend und operational wurden (z. B. Melderegister, Schengen-Datenbank, EKIS, Gen-Datenbank), andererseits die weitverbreitete dezentrale Sammlung anfallender Bewegungsdaten, von Daten also, die sich auf bestimmte Handlungen der Betroffenen beziehen:

- Quantitativ am bedeutendsten sind diejenigen ‚neuen' Daten, die als ‚technische Abfallprodukte' etwa im Telekommunikationsbereich oder bei der Nutzung des Internet anfallen.
- Zunehmend an Bedeutung – und Bedrohungspotential für die Privatsphäre – gewinnen systematisch gespeicherte und ausgewertete Daten zumeist eher zufälligen Charakters (‚zufällig' in dem Sinn, dass die Daten über die Personen gespeichert werden, an die die Firmen eben herankommen, z. B. Kundenkarteien, Teilnehmer an Gewinnspielen, usw.), aus denen Interessenprofile potentieller Kunden abgeleitet werden können.[2]
- Am problematischsten sind wohl die Dateien, die durch sogenanntes Data Mining[3] gewonnen werden, durch Verbindung von Daten aus unterschiedlichen Quellen, durch Private für kommerzielle Zwecke, zunehmend aber auch durch öffentliche oder quasiöffentliche Stellen.

Für den Datenschutz bedeutet das, dass er sich vom Schutz von Daten, die in einem Rechenzentrum lagern, zunehmend zum Schutz der Privatsphäre wandeln müsste, vom Schutz statischer Datensammlungen zum Schutz vor der personenbezogenen Verknüpfung und Auswertung von Daten; diese ist bei Verhaltensdaten besonders problematisch, da es die immer dichteren Netze personenbezogener Daten möglich machen, immer aussagekräftigere Profile des Verhaltens von Personen zu generieren, die von diesen Aktivitäten keine Ahnung haben. War die Kontrolle des Einzelnen über diejenigen seiner Daten, die in traditionellen Datenbanken lagern, durch strikte Zutrittsbeschränkungen und Auskunftspflicht möglich, fehlt diese Möglichkeit bei den neuen Formen weitestgehend, sowohl mangels Wissens über Tatsache und Ort der Speicherung und deren Verknüpfung mit anderen Daten, als auch deswegen, weil sich die Bewegungsdaten laufend ändern und demgemäß kontinuierlich kontrolliert werden müssten.

[1] Siehe dazu Abschnitt 5.

[2] Relevant für den Persönlichkeitsschutz sind nicht so sehr statische Datenbestände, die verwaltet werden und überprüfbar sind, als vielmehr laufende dezentrale Bewegungsprofile, die mit Normdaten automatisch verglichen werden.

[3] Unter Data Mining versteht man das Suchen nach Relationen und Mustern in großen Datenbanken, ohne von vornherein irgendwelche mögliche Relationen definiert zu haben.

2 Ein Überblick über die neuen technischen Möglichkeiten

Welches sind nun die wichtigsten dieser neuen Technologien – Hard- und Software wie organisatorische Innovationen – die zur Informationsgenerierung beitragen? Es erscheint zweckmäßig, zwischen solchen zu unterscheiden, bei denen Daten unvermeidlich anfallen, solchen, die die bewusste Suche nach Daten ermöglichen, sowie solchen zur optimalen Datenauswertung.

Zunächst die automatisch – technisch bedingt – anfallenden Daten:

- Unter diesem Titel ist an erster Stelle die *Digitalisierung der Telekommunikation* zu nennen, die systembedingt Gesprächsdaten beim Telefonieren automatisch aufzeichnet. Die Telekom Austria etwa speichert Stammdaten (Name, Titel, Adresse, Bonität) des digitalen Festnetzes bis sieben Jahre nach Ende der Geschäftsbeziehung, Vermittlungsdaten (alle Informationen über alle auch bloß versuchten Verbindungen) bis ein halbes Jahr nach Bezahlung der Rechnung, wogegen Inhaltsdaten im allgemeinen nicht gespeichert werden dürfen. Nach den Allgemeinen Geschäftsbedingungen der Telekom Austria können die Vermittlungsdaten für konzerninterne Marketing- und Werbezwecke verwendet werden.
- Im *Mobilnetz* fallen zusätzlich Daten über den jeweiligen Aufenthaltsort des Teilnehmers an, solange das Gerät eingeschaltet ist, auch wenn keine Gespräche geführt werden; sie werden derzeit nicht gespeichert, könnten aber sehr wohl dann gespeichert werden, wenn nach Einführung der WAP-Technologie entsprechende Dienste in Anspruch genommen werden[4]. Bei der Verwendung von SMS werden die Inhalte gefiltert, somit kontrolliert und zumindest temporär gespeichert. Bei Verwendung des Mobiltelefons für E-Commerce oder Internetdienste (vor allem location based services) fallen weitere Daten an, aus denen der Betreiber ein sehr umfassendes Bild des Nutzers erhalten kann.
- Ebenso unvermeidlich fallen Daten über Ort, Art und Umfang der Transaktionen bei Verwendung von *Kreditkarten* zur Bezahlung an, bzw. von Kundenkarten zu Bezahlung oder Nutzung von Rabatten. Für *E-Commerce* gilt dasselbe, unabhängig von der Art der Bezahlung.
- Das *Internet* ist durch die Vernetzung unzähliger Datenbanken eine enorme Datenerhebungs-, Speicherungs- und Distributionsmaschine: Jeder Nutzer hinterlässt Informationen über die von ihm besuchten Webseiten, die vielfältig genutzt werden können.
- Die *Verfahrenskonzentration* und die Möglichkeit, *Behördenwege elektronisch* zu erledigen, lassen bei den Behörden zwangsläufig z. T. umfangreiche personenbezogene Dateien entstehen.

Zu diesen automatisch anfallenden Dateien treten in zunehmendem Umfang solche aus der *Vernetzung von Datenbanken sowie bewusst gesammelte Daten,* die in der Informationsgesellschaft zunehmend zu einem wertvollen, teuer gehandelten Gut geworden sind:

- Die zunehmende *Möglichkeit der Vernetzung auch sehr großer Datenbanken* gemeinsam mit der Entwicklung maschinenlesbarer Ausweise macht die rasche Zusammenführung personenbezogener Daten und damit eine erhebliche Steigerung ihrer Aussagekraft möglich (z. B. Schengen-Datei).

[4] Die Nennung der nächsten offenen Apotheke oder eine Liste mit nahe gelegenen Restaurants sind Beispiele für ortsbezogene Informationsdienste, mit denen die WAP-Nutzung angekurbelt werden soll. Da diese Dienste auch in Rechnung gestellt werden – und diese beeinsprucht werden können –, lässt sich die Speicherung von ortsbezogenen Daten mit als für die „Verrechnung von Entgelten erforderlich" argumentieren. Damit wird eine technisch bereits bestehende Möglichkeit der Erfassung und Speicherung von Bewegungsdaten, bei der aber bislang aus rechtlichen Gründen eine längere Speicherung nicht zulässig war, zu einer quasi auch konsumentenpolitisch rechtfertigbaren Notwendigkeit (Čas und Peissl 2000, 18).

- Firmen sammeln auf verschiedene Weise (Kundenkarten, Gewinnspiele, etc.) zunehmend *Kundendaten*, die vor allem in großen Konzernen mit einem breiten Produktangebot durch Zusammenführung sehr aussagekräftig werden können.
- *Call centers* können insofern interessante Daten sammeln, als sie unvermeidlich Informationen über Telefonnummer, Interesse des Anrufers und Kundenbeziehung erhalten; durch automatisierte Verbindung mit dem Telefonregister fällt auch die Adresse an. Vor allem wenn ein Call Center für mehrere große Firmen arbeitet, kommt rasch eine gut verwertbare Datei zusammen. Dennoch ist zu fragen, wie es – angesichts der geltenden Datenschutzbestimmungen – einem der großen österreichischen Adressenverlage gelingt, 5 Millionen Adressen mit einer Datentiefe von 50 Merkmalen anzubieten (Čas und Peissl 2000, 16).
- Das *Internet* wird zur Datensammlung benutzt, indem laufend neue Technologien entwickelt werden, mit deren Hilfe das Verhalten des Nutzers ausspioniert werden kann (Tracking). So etwa können sogenannte ‚Web Bugs' (Netzkäfer), die als kleine Skripts in Webseiten eingebaut sind, unbemerkt vom Benutzer auf den Rechner zugreifen.[5] ‚Cookies' sind kleine Dateien, die besuchte Webseiten auf dem Rechner des Besuchers ablegen und bei jedem Wiedereinstieg abgerufen werden können; sie sind dem Surfer in mancher Weise nützlich, liefern dem Auftraggeber jedoch zugleich auch ein Profil des jeweiligen Surfverhaltens.[6]
- Das *Internet* ermöglicht weiters eine *verdeckte Beteiligung Dritter an der Kommunikation* – und damit Überwachung in Form kommunikationsbezogener Detektion; die Daten können automatisch auf bestimmte Inhalte überprüft (Wortfilter) und natürlich auch gespeichert werden.[7]

Nützlich werden die meisten dieser Daten vor allem durch *raffinierte Programme* zu ihrer Auswertung:

- *Software zur datenbezogenen Detektion* ermöglicht es durch Analyse des Datenschattens, den jede Person bei ihren (elektronischen) Aktivitäten hinterlässt, genaue Nutzerprofile zu erstellen, nicht zuletzt durch Vernetzung mehrerer Datenquellen. Dies wird vor allem im Rahmen des so genannten Customer Relationship Management (CRM) eingesetzt.
- Die enorme Speicherkapazität moderner Anlagen gemeinsam mit *effizienten Methoden der Mustererkennung* ermöglichen Fingerabdruck- und DNA-Datenbanken und damit eine biometrische Identifizierung von Personen. Fortgeschrittene Methoden der Mustererkennung ermöglichen auch automatisierte Gesichts- oder Sprechererkennung.

[5] So demonstrierte etwa Gary Clayton (Privacy Council) dem Datenschutz-Ausschuss des US-Senats durch eine präparierte Webseite, wie das komplette Adressverzeichnis des E-Mail-Programms, Outlook-Express' kopiert werden konnte, ohne irgendwelche Spuren zu hinterlassen (FUZO 2001b).

[6] Solange diese bloß dem jeweiligen Unternehmen zugute kommen, sind sie weniger problematisch. Durch weite Verbreitung können sie jedoch sehr problematisch werden, wie etwa das Beispiel ‚DoubleClick' zeigt: DoubleClick ist eine Internet-Werbeagentur, die sogenannte Bannerwerbung vertreibt; sie ist weltweit Marktführer mit ca. 60 % Marktanteil. Wann immer ein User eine Website mit Banner anklickte, wurde ein Cooky gesetzt bzw. ein vorhandenes ausgelesen. Bei Suchmaschinen wurde das gesamte daran anschließende Surfverhalten protokolliert. Angesichts des hohen Marktanteils ist die Wahrscheinlichkeit, auf eine diesbezügliche Site zu stoßen so groß, dass DoubleClick etwa 120 Millionen Profile erstellt haben soll. Zusätzlich kaufte DoubleClick um 1.7 Mrd. $ die Direktmarketing Agentur Abacus mit Daten über 88 Millionen Haushalte (einschließlich deren Internetgewohnheiten); dadurch hätten innerhalb kürzester Zeit einige Hunderttausend bis dahin „anonyme" Surfer identifiziert werden können (Reischl 2001). Das löste allerdings einen Sturm der Entrüstung aus und rief die Aufsichtsbehörde FTC auf den Plan; die Absicht wurde zunächst aufs Eis gelegt.

[7] Zur Bedeutung dieser Überwachungsmöglichkeiten siehe das Verbot von Verschlüsselung digitaler Kommunikation sowie das amerikanische Spionagesystem Echelon Peissl 2000, 10), mit dem europäische Industrieinformationen ausspioniert werden. Einer Untersuchungsdelegation des Europäischen Parlaments wurden von State Department, CIA und NSA Besprechungstermine verweigert (Die Presse 17.5.2001, 7).

- Die Verbindung *hochleistungsfähiger miniaturisierter Videokameras* mit entsprechender Software ermöglicht die Sammlung und auch Speicherung von Bewegungsdaten; Raster-, Screening-, und Profiling-Programme ermöglichen den raschen, systematischen Vergleich unterschiedlicher Daten (Funk 1994, 58)[8] zur 'front end verification'. Menschen, auch verkleidete, können durch ihre Körperbewegung identifiziert und auch über wechselnde Kameras über weite Strecken hin verfolgt werden (Rötzer 2000c, 158).[9]
- Für die Analyse derart gewonnener Daten wie für solche, die weitere Instrumente zur ereignisbezogenen Detektion (Einbruchsmeldeanlagen, szenisch-panoptische Instrumente wie Video, Wärmebildkamera, Nachtsichtgeräte) liefern, gibt es bereits *Verfahren zur algorithmengestützten (automatisierten) Alarmierung* bei Gefahr-verheißenden Szenen (Nogala 2000, 148). An der Universität Leeds wird an der Entwicklung von Software gearbeitet, mit der verdächtiges von normalem Verhalten unterschieden werden kann (Rötzer 2000c, 160).[10]
- *Affective computing* kann schon jetzt viele Körperdaten erfassen und analysieren (Rötzer 2000c**,** 160), und an der Universität Pittsburgh wird zusätzliche Software entwickelt, die auch eine Analyse des Gesichtsausdrucks ermöglicht; damit eröffnen sich völlig neue Möglichkeiten der Mitarbeiterkontrolle.[11]
- Schließlich sollen als Möglichkeiten zur Kontrolle der Privatsphäre noch *Geräte zur substanzanzeigenden Detektion* erwähnt werden, etwa zum Drogennachweis durch Analyse von Flugtickets (Nogala 2000, 146), Sensoren wie z. B. CO_2-Detektoren oder auch
- die *elektronische Fußfessel*.

Viele dieser Geräte und Programme funktionieren noch nicht richtig, doch die Entwicklung läuft rasch weiter; dafür einige Beispiele: Die Instrumente werden immer kleiner, immer leistungsfähiger und vor allem allgegenwärtig (‚Ubiquitous Computing' – UC). Digitale Schaltkreise, Laserbasierte, drahtlose Kommunikation und MEMS (micro electro-mechanical systems) werden zusammengeführt und in Einheiten von etwa fünf Millimeter Länge integriert (‚Smart Dust'); diese miteinander in Verbindung stehenden ‚Micro-Computer' (ausgestattet mit Sensoren für verschiedene Umweltveränderungen) könnten in Zukunft zur flächendeckenden Überwachung von feindlichen Gebieten wie auch von Räumen eingesetzt werden (Flint 2000). In sogenannten ‚smart homes' werden Kommunikationsmittel, Energieversorgung und diverse computerisierte Haushaltsgeräte voll vernetzt. Damit kann etwa die Heizung automatisch (sensor)-gesteuert oder – über einen Abgleich verschiedener Tarife – der optimale Zeitpunkt für das Einschalten der Waschmaschine eruiert werden. Das bringt einerseits Vorteile für Konsumenten[12] wie Gesamtwirtschaft,[13] bedeutet aber andererseits eine weitere Angriffsfläche für die Privatheit, da die kontinuierliche Kontrolle des Strom- und Wasserverbrauchs nicht bloß aufdeckt, wie viele Menschen sich in einem Haushalt wann aufhalten und welche Geräte sie benutzen, sondern auch ihre Fernseh- und anderen Lebens-

[8] OTA (1986) identifizierte bereits in den achtziger Jahren 110 derartige Programme.

[9] Bekannt für den Einsatz von Überwachungstechnologien, die darauf abzielen, ‚deviantes' Verhalten frühzeitig zu erkennen, ist insbesondere Großbritannien, wo etwa 200.000 Überwachungskameras im Einsatz sind.

[10] Etwa Videoanalyse des Verhaltens (Rötzer 2000c), von Beinbewegungen (Rötzer 2000a) aber auch Gesichtsvergleiche in 3D (Rötzer 2000b), so dass nicht einmal die Verwendung einer Sonnenbrille vor Erkennung schützt.

[11] Das Kinderspieltier Furby kann auf die Zuwendung seiner Besitzer reagieren, Weiterentwicklungen können bereits auf recht differenzierte Weise deren jeweilige Verfassung mit berücksichtigen (Sh. Turkle, persönliche Mitteilung).

[12] Vor allem Senkung der Strom- und Heizkosten; wenn die ‚smart homes' via standardisierter Schnittstelle mit Weitverkehrsnetzen (Internet) gekoppelt sind, ist auch das Fernablesen von Gebühreneinheiten oder die Fernwartung von Geräten möglich.

[13] Z. B. verbesserter Lastausgleich in Energienetzen.

gewohnheiten (Schoechle 1995). Die künftige Verwendung des Mobiltelefons als Zahlungsmittel, die zunehmende Verschmelzung von Kunden- und Kreditkarten (Billa-BA-card, ÖBB-Mastercard) oder die Möglichkeit der konzerninternen Verwertung von Kundendaten bei weiterer Konzentration und zunehmend größeren Konzernen eröffnen weitere Möglichkeiten eines immer tieferen Eindringens in die Privatsphäre.

3 Wer nutzt die neuen Möglichkeiten ...

Ob bewusst gesammelt oder als willkommene Folge technischer Möglichkeiten bzw. Notwendigkeiten – die Menge der gesammelten Daten explodiert: Čas und Peissl (2000, 11) schätzen, dass sich der durchschnittliche Österreicher in mindestens 100, wahrscheinlich jedoch eher in 400 Datenbanken finden könnte; nach niederländischen Erfahrungen ist das ein Vielfaches dessen was vermutet wird.[14] Diese neuen Daten ermöglichen vielfältige Nutzung:

1. Zunächst werden sie zur Überwachung genutzt, und zwar keineswegs bloß durch den Staat – Orwells „Großen Bruder" –, sondern, mehr noch, durch viele zumeist gar nicht so „Kleine Schwestern": Private Sicherheitsdienste, Arbeitgeber, Garagenbetreiber, usw.;
2. weiters für administrative Zwecke;
3. für die traditionellen statistischen Zwecke;
4. schließlich für kommerzielle Zwecke, vor allem durch data mining, die Bearbeitung des Datenschattens, den man fast überall hinterlässt, wo man mit Elektronik i. w. S. in Kontakt kommt.

Ad 1.: Die verschiedenen Varianten der vielfältigen Nutzungsmöglichkeiten können hier bloß beispielhaft angeführt werden. Die zunehmende *Überwachung durch den Staat* wird mit Vorbeugung wie mit dem zunehmenden Sicherheitsbedürfnis einer wohlhabenden fragmentierten Gesellschaft begründet: Kampf gegen die organisierte Kriminalität oder die Geldwäsche, Observierung der Aktivitäten anderer Staaten (Geheimdienste zunehmend in elektronischer Form; siehe Echelon), Kampf aber auch gegen die übliche ‚kleine' Kriminalität, die die Sicherheit des Bürgers auf der Straße oder in den öffentlichen Verkehrsmitteln bedroht (Video),[15] vielfach als vorbeugender Ersatz für eine Rasterfahndung. Die Vielzahl und die Effizienz der Methoden ließe selbst Metternichs Geheimpolizei vor Neid erblassen.[16]

Neben die Überwachung durch den Großen Bruder Staat tritt zunehmend eine *Überwachung durch eine Vielzahl privater Firmen,* also durch viele Kleine Schwestern, denen zumeist die gleichen Möglichkeiten der elektronischen Sammlung und Speicherung von Daten zur Verfügung stehen wie dem Staat: Private Sicherheitsdienste, Garagenbetreiber, Warenhäuser, Supermärkte, die alle inzwischen Überwachungsanlagen betreiben; mit vielen kann automatisch-softwaremäßig ‚normales' von ‚deviantem' Verhalten unterschieden und eine entsprechende Observierung eingeleitet werden.[17]

[14] Eine Untersuchung des niederländischen Verbraucherverbands kam auf 900 Dossiers je Konsumenten; zwei Drittel der Konsumenten glaubten jedoch, in bloß 25 Datenbeständen erfasst zu sein, nur 4 % in mehr als 100 (Borking 1998, 286).

[15] Siehe Fußnote 8.

[16] Damals war es nicht verboten, Briefe zu versiegeln, wogegen heute gegen die Verschlüsselung der E-Mail ernste Bedenken bestehen.

[17] Es erscheint wichtig, schon an dieser Stelle auf den Doppelcharakter dieser Maßnahmen hinzuweisen: Diejenigen Frauen, die sich in Tiefgaragen fürchten, werden die Überwachung durch Videokameras und

Die Videoüberwachung in Warenhäusern und Supermärkten bezieht sich nicht bloß auf die Kunden, sondern vielfach auch auf die *Arbeitnehmer,* die dadurch ihre Privatsphäre am Arbeitsplatz weitestgehend verlieren. Doch selbst ohne Videoüberwachung hat die Digitalisierung die Kontroll- und Überwachungswerkzeuge des Arbeitgebers ganz generell erheblich verbessert: Gesprächsdaten beim Telefonieren[18] werden nun automatisch aufgezeichnet, und über die Internetnutzung der Mitarbeiter weiß der betriebseigene Netzwerktechniker alles; aus den angewählten Webseiten (Verbindungsdaten) kann der Arbeitgeber recht genaue Rückschlüsse auf die aufgerufenen Inhalte ziehen.[19]

Ad 2.: Ein weiterer großer Bereich der Nutzung ist die *elektronische Speicherung von Daten für administrative Zwecke*, wie z. B. Grundbuch, Steuerdateien, Sozialversicherungsdateien, Passdatei oder zentrales Melderegister.[20] Hier stehen Überlegungen der Effizienz des Verwaltungsablaufs und des Komforts für den Bürger (Grundbuch, Pass) im Vordergrund, doch resultieren daraus unvermeidlich Überwachungsmöglichkeiten; vor allem durch Verbindung mit einer Personenkennzahl, die die Verbindung der verschiedenen Datenbanken ermöglicht (‚Data-Warehousing'[21]), wird der ‚gläserne Mensch' realisiert, nicht zuletzt, weil sich die Zahl der Zugriffsberechtigten erfahrungsgemäß bloß sehr schwer beschränken lässt.

Ad 3.: Ähnliches gilt für die *traditionellen statistischen Zwecke* der Datensammlung durch den Staat: Die großen Vollerhebungen – Volkszählung, Arbeitstättenzählung, Betriebszählung – sollen eingestellt werden. Es ist einfacher und billiger, bestehende administrative Statistiken und Register (Melderegister, Steuerdateien, Unternehmensgründungen, etc.) miteinander zu verknüpfen und eventuell durch Stichprobenerhebungen zu ergänzen. Ein erster Schritt in diese Richtung ist im Rahmen des Bezügegesetzes bereits erfolgt: Zur Erhebung der durchschnittlichen Einkommen (einschließlich Sozial- und Sachleistungen) der gesamten Bevölkerung nach Branchen, Berufsgruppen und Funktionen wurden die Personendaten der Mikrozensuserhebung mit personalisierten Daten aus den Steuerdateien zusammengeführt. Selbst wenn das rechtlich gedeckt sein sollte,[22] erscheint es doch keineswegs unbedenklich, nicht zuletzt angesichts der Ausgliederung des Statistischen Zentralamts aus der öffentlichen Verwaltung.

Erkennungsprogramme mit automatischer Alarmauslösung ebenso schätzen wie die Eigentümer verlorener Kreditkarten Programme zur automatischen Erkennung unüblicher Transaktionen (Nogala 2000, 146); wer auf Grund der automatischen Überwachung grundlos verdächtigt wird und sich – womöglich noch öffentlich – rechtfertigen muss, wird über diese Einrichtungen eine durchaus andere Ansicht haben.

18 Lange Jahre *das* Thema für die Gewerkschaften, bis sich die Betriebsvereinbarungen über die Gesprächsdatenaufzeichnung bei Telefonanlagen durchsetzten.

19 Hierüber besteht bei Nutzern wie bei Arbeitgebern noch kaum ein entsprechendes Bewusstsein – obwohl schon spezielle Softwarepakete auf dem Markt sind, die versprechen, die betriebliche Effizienz der Internetnutzung durch Kontrolle zu steigern.

20 In diesem sollen alle Österreicher gespeichert sein und alle Behörden Zugriff haben. Die für die Volkszählung 2001 eingesetzten ‚Zählorgane' hatten nicht nur die Daten zur Volkszählung zu erheben, die für die Zwecke der Statistik anonymisiert werden, sondern auch persönliche Meldedaten. Theoretisch erheben sie letztere in anderer Funktion – praktisch lässt sich die Verknüpfung (zumindest im Kopf des Zählorgans) wohl nicht vermeiden.

21 Data-Warehousing ist die systematische Zusammenführung und Aufbereitung von Daten aus unterschiedlichen Systemen zur Entscheidungsunterstützung.

22 Das Bezügebegrenzungsgesetz (BGBl I Nr. 64/1997) verlangt in § 8 die Erstellung eines Einkommensberichts. Zu Vergleichszwecken hat der Rechnungshof neben den Berichten der seiner Kontrolle unterliegenden Rechtsträger auch „über die durchschnittlichen Einkommen einschließlich der Sozial- und Sachleistungen der gesamten Bevölkerung – nach Branchen Berufsgruppen und Funktionen getrennt – zu berichten. Solange die hiefür erforderlichen statistischen Daten nicht zur Verfügung stehen, ist dieser Bericht aufgrund von Gutachten von Sachverständigen zu erstatten." (BGBl. I Nr. 64/1997, §8 Abs. 4). Es fällt nicht leicht, in dieser Formulierung die Ermächtigung zur Zusammenführung personalisierter Daten zu erkennen.

Ad 4.: Schließlich die Sammlung, Speicherung und Verwertung von *Kundendaten für kommerzielle Zwecke,* fast schon in Art einer Rasterfahndung. Der Begriff der „Firma" muss seit den Ausgliederungen und Privatisierungen durchaus weit gefasst werden: Vom ehemaligen Statistischen Zentralamt (siehe Abschnitt 6) über die Telekom-Firmen bis zur Gelben Post.[23] Mittels ‚Data-Mining' und ‚Data-Warehousing' kann aus Persönlichkeitsmerkmalen und bisherigem Verhalten mit relativ großer Genauigkeit auf zukünftiges Verhalten geschlossen werden. Im Rahmen des ‚Customer Relationship Management' (CRM) lassen sich unterschiedliche Kundenprofile erstellen und mit relativ hoher Sicherheit Vorhersagen treffen, ob ein Kunde dem Unternehmen treu bleiben wird (‚churn-management') oder potentieller Käufer für bestimmte andere Waren ist; diese Möglichkeiten sind noch keineswegs voll genutzt (Lechner 2000).[24] Je größer und differenzierter diese Firmen, desto mehr Daten über denselben Kunden erhalten sie, und desto genauere Persönlichkeitsprofile können sie erstellen, desto ‚gläserner' wird also ihr Kunde. Drei Probleme erscheinen dabei besonders relevant:

- Erstens die in vielen Fällen geradezu ‚erschlichene' Zustimmung des Kunden zu einer breiten Datenspeicherung und -verarbeitung, versteckt teils in den kleingedruckten Allgemeinen Geschäftsbedingungen, teils in Formulierungen der Zustimmungsklausel, die den Kunden darüber im Unklaren lassen, dass sich seine Zustimmung auf die Verwertung nicht bloß in der jeweiligen Firma bezieht, sondern innerhalb eines riesigen Konzerns, also auch durch Firmen, die er überhaupt (noch) nicht kennt. Bedenklich in dieser Hinsicht erscheint vor allem die zunehmende Verflechtung von Banken mit Versicherungen und Handelsunternehmen.
- Zweitens fehlt dem Betroffenen jede reale Möglichkeit, in die über ihn gespeicherten Daten Einsicht zu nehmen, deren Weitergabe bzw. Nicht-Weitergabe zu kontrollieren[25] und gegebenenfalls deren Löschung zu erzwingen.
- Drittens schließlich ergibt sich – auch ohne Weitergabe der Daten – ein überaus heikles Problem, wenn Firmen fusionieren; angesichts der Informationen, die Kreditkartenfirmen, Banken, Versicherungen, Telekom- oder Internet-Provider über ihre Kunden haben, kann aus solchen Fusionen durch Vernetzung der Daten eine Informationsdichte resultieren, die einen dramatischen Eingriff in die Privatsphäre bedeutet.

[23] Die österreichische Post sammelt intensiv die bei ihr anfallende Daten und bietet sie im Rahmen von „Informell Select" kundenspezifisch selektiert an; im Prospekt werden etwa Adressen von Gartenfreunden erwähnt. Die deutsche Post hat einen Vertrag mit der Kreditkarten-Clearingstelle GZS geschlossen, der zufolge die Rechnungsdaten der Kartenkunden elektronisch an die Post-Tochter PrintCom übermittelt und von dieser ausgedruckt und versendet werden (Die Presse 11.5.2001).

[24] Der Handel selbst nutze die Möglichkeiten der IT-Welt viel zu wenig und kenne daher den Kunden nur ungenau. Telekomfirmen hingegen wüssten längst, dass sie mit all den gesammelten Kundendaten auf einer Goldmine sitzen. (F.P Amesberger, Berater bei Trust Consult in Die Presse vom 17.4.2001, 14).

[25] Siehe Fußnote 5 sowie das vorne erwähnte Problem eines großen österreichischen Adressenverlags, der 5 Millionen Adressen mit einer Datentiefe von 50 Merkmalen anbieten kann.

4 ... und mit welchen Folgen?

Die Diskussion um die rasch wachsenden Möglichkeiten der Datenerhebung, -speicherung und -auswertung, ihre bedenklichen Folgen und deren Begrenzung führt unvermeidlich zu der normativen Frage: Wen stört das und warum? „Wer nichts zu verbergen hat, braucht auch nichts zu fürchten“ ist ein häufig gebrauchtes Argument, um die gängigen Praktiken zu rechtfertigen. Dieser normative Aspekt ist außerordentlich wichtig, kann in dem gegebenen Rahmen allerdings nicht einmal ansatzweise behandelt werden. Bloß ein paar Schlagworte zur Illustration: Das menschliche Bedürfnis nach einem ‚privaten‘ Bereich resultiert aus einem für alle Gesellschaften typischen Schamgefühl sowie aus der Angst vor sozialer Kontrolle (Gridl 1999, 19 FN 19).[26] Dieses Schamgefühl „... ist eine Angst vor der sozialen Degradierung, oder, allgemeiner gesagt, vor den Überlegenheitsgesten Anderer; ... der Konflikt, der sich in Scham-Angst äußert, ist nicht nur ein Konflikt des Individuums mit der herrschenden gesellschaftlichen Meinung, sondern ein Konflikt, in den sein Verhalten das Individuum mit dem Teil seines Selbst gebracht hat, der diese gesellschaftliche Meinung repräsentiert; ... er selbst erkennt sich als unterlegen an.“ (Elias 1979, II397). Es geht also um Nonkomformität, um das Bewusstsein vom Durchschnitt in bestimmten Punkten abzuweichen. Das Interesse daran, diese Abweichung nicht öffentlich zu machen, sie zu ‚verbergen‘, mag damit zusammenhängen, dass man daraus tatsächlich Nachteile erwartet, dass man sich der Abweichungen schämt, sie aber nicht zu ändern vermag,[27] oder aber auch daraus, dass man nicht gewillt oder nicht in der Lage ist, seine Nonkonformität und deren Gründe mit anderen zu diskutieren oder gar sie gegenüber anderen zu rechtfertigen.

Problematisch für den Schutz der Privatsphäre ist, dass Art und Umfang des Bedürfnisses nach einem privaten Bereich zwischen den Gesellschaften, innerhalb derselben Gesellschaft im Zeitablauf wie zwischen den einzelnen Individuen außerordentlich stark variiert; beispielsweise sei geographisch auf die diesbezüglichen Unterschiede zwischen Skandinavien und dem deutschsprachigen Raum verwiesen,[28] zeitlich-historisch auf die von Elias erwähnten mittelalterlichen Hochzeitsnacht-Bräuche[29] oder die hierarchisch bedingten Scham-Differenzen.[30] Das erschwert es, die Privatsphäre allgemeingültig abzugrenzen und bestimmte Daten diesem Bereich als schutzwürdig zuzuordnen. Unter den theoretischen Ansätzen, die solches versuchen, seien die Sphärentheorie, die

[26] Dass jeder Mensch einen Bereich braucht, in dem er alleine ist, wird auch dadurch untermauert, dass etwa Kinder in einer psychiatrischen Anstalt der dauernden Überwachung durch auffälliges Verhalten und die daran anschließende Bestrafung – durch Isolation in Einzelzimmern – zu entgehen versuchen (Egger 1990, 67 FN 2).

[27] Z. B. körperliches anders Sein.

[28] In Österreich lassen sich die Ursachen für das grundlegende Spannungsverhältnis zwischen Datenschutz und Informationsfreiheit und die Systematik der Auskunftsverweigerung in der Entstehungsgeschichte der Amtsverschwiegenheit finden: Die österreichische Bürokratie entstand unter Maria Theresia und Joseph II zur Verwaltung des Finanzwesens; Amtsverschwiegenheit wurde als wesentliches Mittel der Abschottung gegen außen, aber auch als Pressionsmittel gegen kritische Beamte eingesetzt (Egger 1990, 14f). Anders verlief die Entwicklung in Schweden und den USA, wo eine lange Tradition der Offenheit und Informationsfreiheit besteht. In den USA wird das „right of privacy” als integrale Komponente der „informational autonomy” angesehen. „Das ‘right of privacy’ und das ‘(public) right to know’ sind komplementäre Bestandteile der Selbstbestimmung der Bürger.“ (Funk 1994, 577). Offenheit und Transparenz ermöglichen sowohl die Teilhabe des Einzelnen an gesellschaftlichen Entwicklungen als auch eine Kontrollfunktion der Bürger gegenüber der Bürokratie.

[29] „Der Zug ins Brautgemach erfolgte unter Vortritt aller Brautführer. Die Braut wurde von den Brautjungfern entkleidet; sie musste allen Schmuck ablegen. Das Brautbett musste dann in Gegenwart von Zeugen beschritten werden, sollte die Ehe gültig sein. Man legte sie zusammen.“ (Elias 1978, I 243).

[30] „Die Entblößung des Höherstehenden in Gegenwart von sozial Niedrigerstehenden, also etwa die des Königs vor seinem Minister, unterliegt hier begreiflicherweise noch keinem sehr strengen gesellschaftlichen Verbot, so wenig etwa, wie in einer noch früheren Phase die Entblößung des Mannes vor der sozial schwächeren und daher sozial niedriger rangierenden Frau; ... sie kann sogar ... als ein Zeichen des Wohlwollens für den Niedrigerstehenden gelten. Die Entblößung des Menschen von minderem Rang vor dem Höherstehenden wird mehr und mehr als ein Zeichen der Respektlosigkeit aus dem gesellschaftlichen Verkehr verbannt.“ (Elias 1978, II 403).

Mosaiktheorie und der rollenspezifische Ansatz erwähnt. Die *Sphärentheorie* versucht verschiedene Sphären voneinander abzugrenzen, die in unterschiedlichem Maße schutzbedürftig sind; etwa Individualsphäre – Privatsphäre – Geheimsphäre (Hubmann 1967, 269) oder Öffentlichkeitssphäre – Sozialsphäre – Vertrauenssphäre – Intimsphäre – Geheimsphäre (Seidel 1972, 65). Problematisch dabei ist nicht bloß die Grenzziehung zwischen diesen Sphären als solche, sondern mehr noch die Definition der jeweiligen Intim- oder Geheimsphären wegen der erheblich unterschiedlichen individuellen Einschätzungen der Betroffenen. Nach der *Mosaiktheorie* (Egger 1990, 57) gewinnen Daten vor allem in Verbindung mit anderen Daten – als ‚Mosaiksteinchen' – an Aussagekraft. Demgemäß sind nicht nur Daten aus ‚sensiblen' Sphären zu schützen – wie immer diese definiert werden –, sondern auch die Verknüpfung von Daten. Dieser Punkt erscheint deswegen als zentral, weil die Datenverarbeitung – wie vorne beschrieben – gegenüber der Datenerfassung zunehmend an Relevanz gewinnt; da der Einzelne kaum nachvollziehen kann, wer welche Daten an wen weiterleitet und verarbeitet,[31] entzieht sich das eigene ‚virtuelle' Bild weitgehend der eigenen Steuerung, womit zwangsläufig schutzwürdige Interessen verletzt werden. Der *rollenspezifische Ansatz* schließlich betont, dass die Privatsphäre aus zahlreichen unterschiedlichen Bildern besteht und es dem Einzelnen überlassen bleiben muss, welche davon er wem preisgibt.

Außer der Verletzung – wie immer definierter – schutzwürdiger Interessen ergeben sich aus der zunehmenden Nutzung personenbezogener Daten durch öffentliche Stellen wie Private erhebliche Probleme, von der bloß lästigen Überschwemmung durch ‚Informationen' über De-Kontextualisierung, mögliche Risikoselektion, Beeinträchtigung der Privatsphäre durch Nutzung der Daten durch Unberechtigte und Zwang zur Verhaltensanpassung bis zur tendenziellen Aufhebung der Unschuldsvermutung.

Relativ noch am wenigsten problematisch ist *die Belästigung* (Schoenmacker und Starre 2000); doch führen auch die unaufgeforderten Werbeaktivitäten zu überquellenden E-Mail Postfächern ('spam') und Postkästen, zu Telefon-Marketing-Anrufen am Abend, die alle Kosten, Zeitaufwand (Entsorgung) und Ärger verursachen; Belästigungen, die das Leben beeinträchtigen und andere Aktivitäten stören.

Deutlich ernster ist das Problem der *De-Kontextualisierung*, das daraus resultiert, dass die Daten zumeist für ganz andere Zwecke erhoben wurden als für die, nach denen sie ausgewertet werden. Dadurch können falsche Bilder entstehen, selbst dann, wenn die Daten ‚richtig' sind. Eine Internetrecherche beispielsweise zu einer schweren Krankheit (etwa um einem Freund zu helfen), kombiniert mit einer zeitlich nahe liegenden Internetrecherche zu Versicherungsbedingungen und Tarifen, kann ohne Wissen um die Kontexte der Entstehung zu einem höheren Versicherungstarif führen. Besonders anfällig für solche Fehlinterpretationen sind natürlich die automatischen Überwachungssysteme: ‚Deviantes' Verhalten in Tiefgarage oder Supermarkt mag auf Vergesslichkeit, das Interesse für Hitler-Bücher auf wissenschaftlich-zeitgeschichtlichem Interesse beruhen.

Problematisch ist auch die mögliche *Risikoselektion* auf Grund großer Datensammlungen und immer raffinierterer Auswertungsprogramme. Mit Hilfe von Data-Mining-Programmen wird das Verhalten ‚vorausgesagt', wodurch Risiken prognostiziert, Risikogruppen lokalisiert und individualisierte Angebote erstellt werden können. Werden die vermuteten Risiken als groß eingeschätzt, kann es zum Ausschluss von Leistungen kommen,[32] mit möglicherweise weitreichenden Folgen, jedenfalls aber zu höheren Tarifen. Problematisch dabei ist vor allem, dass die Entscheidung nicht auf Grund *existierender* Risken getroffen wird, sondern auf Grund von solchen, die nach bestimmten Merkmalskombinationen *automatisch-modellmäßig vermutet* werden – das Problem der De-

[31] Eine Untersuchung von 750 Websites durch Consumers International, eine Vereinigung von 260 Verbraucherschutzorganisationen zeigte, dass eine erschreckend große Zahl von Anbietern Daten ohne Wissen der Surfer sammelt. Weniger als ein Fünftel der Websites, die persönliche Informationen sammeln, halten die Mindeststandards beim Datenschutz ein (Die Zeit 18, 26.4.2001, 27f).

[32] Das gilt keineswegs bloß für Versicherungen; auch weniger kaufkräftige Kunden im Handel werden bei Beschwerden in der Hotline automatisch nachgereiht, d. h. länger hängen gelassen.

Kontextualisierung wird auch hier schlagend. Neben diesen konkreten Auswirkungen wirft die automatische Risikoselektion durch Data-Mining aber auch grundlegende Fragen auf: Fragen der Gleichbehandlung von Menschen, der Aushebelung des Versicherungsprinzips durch eine exzessive Risikoselektion, aber auch der möglichen Gegenwehr des Konsumenten, der über die Daten und die Programme und damit über die Gründe für seine Behandlung nicht informiert ist.

Wohl am problematischsten jedoch ist der *subtile Zwang zum Konformismus*: Dass aus der Kontrolle ‚devianten' Verhaltens längerfristig eine Verhaltensanpassung im Sinne eines Zugs zu Angepasstheit und ‚Wohlverhalten' resultieren kann, eine Verinnerlichung der Kontrolle durch Selbstdisziplinierung (Foucault 1977).[33] Vielfalt ist jedoch eine Grundbedingung für Demokratie und Zivilgesellschaft wie für die gesellschaftliche, kulturelle und wirtschaftliche Entwicklung. „Grob gesprochen, kann man panoptische Methoden als Mittel betrachten, die Bevölkerung zu normalisieren – etwa den Konsum zu maximieren. ... Sie schaffen Situationen, in denen, wie gesagt, die gewünschten Ergebnisse immer wahrscheinlicher werden." (Lyon 1997). Konformismus verringert einerseits zwar die Fehlplanungen der Unternehmen, da das Verhalten angepasster Konsumenten leichter zu prognostizieren ist, er behindert aber andererseits auch Innovation und damit Wachstum.

Die Problematik geht über die Erhaltung und Sicherung der Vielfalt weit hinaus: Der digitalen Überwachung liegt zwangsläufig die Tendenz zugrunde, *von der Norm abweichendes Verhalten als ‚deviant' und sogar als gefährlich einzustufen.* Nicht bloß, dass die entliberalisiert-kontrollierte Gesellschaft in aufreizendem Kontrast zur liberalisiert-deregulierten Wirtschaft steht; die automatisierten Überwachungssysteme zielen auch zwangsläufig auf bestimmte vordefinierte Risikokategorien, auf bestimmte Territorien und Populationen (Nogala 2000, 153); Minderheiten, Intellektuelle oder Gruppen mit spezifischen Lebensstilen können dadurch in besonderem Maße gefährdet sein.

Darüber hinaus liegt den zunehmenden Überwachungsaktivitäten die *tendenzielle Aufhebung der Unschuldsvermutung,* eines der Grundwerte des Rechtsstaates, zugrunde: Wer seine E-Mail verschlüsselt, ist verdächtig, wogegen man früher – selbst unter Metternich – seinen Brief sogar im versiegelten Kuvert versenden durfte. Verbrechensprävention ist zwar an sich positiv zu bewerten, sie sollte allerdings früher einsetzen und eher die Gestaltung der gesellschaftlichen Rahmenbedingungen zum Ziel haben als alle in der potentiellen Tatsituation zufällig Vorbeieilenden grundsätzlich zu verdächtigen und zu observieren. Überwachung als technokratischer Versuch, Konflikte zu managen statt zu lösen, kann bloß kurzfristig wirken.

[33] Der englische Philosoph J. Bentham entwarf im 18. Jahrhundert das architektonische Prinzip des Panopticons, ein Gefängnis, in dem alle Insassen von einer zentralen Warte aus jederzeit beobachtet werden können, ohne das selbst erkennen zu können (Nogala 2000, 143).

5 Mangelndes Problembewusstsein

Der Überblick über die technischen Möglichkeiten der Datensammlung, -vernetzung und -auswertung wie über ihre übliche Nutzung zeigt einen bereits beträchtlichen Verlust an Privatsphäre. Die Chance der Anonymität, eine der wichtigsten Formen der Privatheit, ist bereits weitgehend verloren gegangen.[34] „Wirtschaft und Staat arbeiten zusammen, um unsere Wege durch das Netz besser aufspüren und nachzeichnen zu können. Potentiell ist das eine Gefahr für Demokratie und Freiheit" (L. Lessing). Warum äußert sich nicht mehr Widerstand gegen dieses massive Eindringen in die Privatsphäre durch Staat und Wirtschaft? Noch vor einem Jahrzehnt gab es massive Proteste gegen die relativ harmlose Datensammlung der Volkszählung; heute wird nicht einmal mehr gegen die problematische Verbindung von Volkszählung und Melderegister-Erhebung durch ein inzwischen ‚privatisiertes' Unternehmen – Statistik Austria – protestiert! Beim ‚Handy' wird zwar die marginale Strahlung der Masten problematisiert, nicht jedoch die Sammlung und Verwertung der Bewegungsdaten. Verschiedenes mag dazu beigetragen haben:

- Zunächst einmal dürfte tatsächlich ein Bewusstseinswandel breiter Bevölkerungskreise stattgefunden haben: Man scheut sich nicht mehr, Gefühle in der Öffentlichkeit zu zeigen, Intimes physisch und psychisch offen zu legen oder sich sogar freiwillig der Beobachtung durch die Medien auszusetzen.[35] Man könnte den Eindruck gewinnen, dass eine Gewöhnung an Öffentlichkeit stattgefunden hat (Nogala 2000, 139); Anonymität – nicht die Verletzung ihrer Privatsphäre – dürfte vielen zunehmend als Bedrohung erscheinen. Doch selbst wenn sich das Bewusstsein der breiten Masse tatsächlich gewandelt hat, muss Schutz der Privatsphäre – wenn auch bloß als Schutz der Interessen einer Minderheit – gesichert sein.
- Zweitens dürfte ‚die Elektronik' weitgehend als technisch-anonym empfunden werden; der normale Nutzer ist sich der Möglichkeiten des Bloßlegens der Privatsphäre bzw. der Möglichkeiten des Eindringens offenbar nicht bewusst, wie der Irrglaube vom anonymen Surfen im Netz enthüllt, oder auch die vorne aufgezeigte markante Unterschätzung der Zahl der Datenbanken, in der sich der Durchschnittsbürger erfasst glaubt.
- Dazu kommt, drittens, das Doppelgesicht der Überwachungs- und Informationsstrategien: Sie alle dienen – zunächst – einem guten Zweck: Die Überwachung der Gauner dient der Sicherheit, die maßgeschneiderte Information wird als zweckmäßig und bequem empfunden, das Gewinnspiel als lustig, der kürzere Behördenweg als angenehm. Erst wenn gelangweilte Polizisten im EKIS surfen oder gar der Nachbar in seinem Beruf als Finanzbeamter in der eigenen Steuerdatei forscht, dann schlägt das Bewusstsein plötzlich um.
- Viertens wird Überwachung nicht bloß in unserer anonymen Gesellschaft vielfach eher als Schutz- und Ordnungsinstrument empfunden denn als Belästigungs- und Bedrohungspotential (Nogala 2000, 141); der Big Brother wird zunehmend nicht mehr als eine Überschreitung soziokultureller Privatheits- und Zivilisationsschranken und als Entgrenzung des bislang Privaten empfunden, er wird akzeptiert.

[34] Der Wert der Anonymität mag von Einzelnen unterschiedlich eingeschätzt werden; die relativ zum Dorf größeren Möglichkeiten der Anonymität scheinen jedoch zumindest *ein* Erfolgsfaktor der Großstädte zu sein (Rötzer 2000c, 158).

[35] „Die Jungen interessieren sich für die Angebote und lassen Datenschutz Datenschutz sein" (L. Späth auf dem Energieforum der Wiener Stadtwerke am 5.4.2001).

6 Die kritische Austauschbeziehung: Sicherheit, Effizienz und Komfort versus Schutz der Privatsphäre

Der geringe Widerstand gegen die mit der Nutzung der digitalen Elektronik verbundene Gefahr des Eindringens in die Privatsphäre ergibt sich nicht zuletzt aus dem daraus resultierenden Nutzen, m.a.W. aus den kritischen Austauschbeziehungen zwischen Sicherheit, Effizienz und Komfort auf der einen und dem Schutz der Privatsphäre auf der anderen Seite. In Bezug auf Maßnahmen zur Sicherung der Privatsphäre sind das sogar die entscheidenden und kritischen Argumente.

- Das Tradeoff des Schutzes der Privatsphäre mit *Sicherheit* wurde schon weiter vorne ausführlich behandelt; Observierung wird offenbar zunehmend als Königsweg zur Bewahrung von öffentlicher Ruhe und Ordnung betrachtet (Nogala 200, 147). Zwar war die Beobachtung der Übeltäter schon immer ein Anliegen: Vor der Verbreitung der Videokamera sorgte „Gottes Aug' ist überall" wenigstens im Nachhinein für ausgleichende Gerechtigkeit; im Eifer der Sorge um die Observierung potentieller Übeltäter übersehen die Meisten allerdings, dass bei der prophylaktischen Observierung nicht die ‚Übeltäter' als solche observiert werden können, sondern bloß formal-definiert ‚deviantes' Verhalten. Andererseits darf aber auch nicht übersehen werden, dass die strikte Überwachung in Großbritannien Kleinkriminalität und Vandalismus tatsächlich stark zurückgehen ließ, und das Leben für Viele dadurch tatsächlich leichter geworden ist.
- Das Tradeoff mit *Kontrolle* ergibt sich daraus, dass die Notwendigkeit genauer Überwachung und Kontrolle zunehmend mit der Aufdeckung von möglichen Missbräuchen begründet wird; das reicht vom Identifizieren von ‚Sozialschmarotzern' und Steuerhinterziehern[36] bis zur peinlich-genauen Überwachung der Mitarbeiter (Nogala 2000, 152). Die Verhältnismäßigkeit wird dabei zumeist überschritten. Es wird übersehen, dass Datenschutz als solcher ein *Ziel* demokratischer Regierungen ist, Kontrolle und Anti-Missbrauchsmaßnahmen hingegen bloß *Instrumente*, keine Werte an sich (POST 1998).[37] Der Informationseingriff muss auf das unvermeidliche Minimum beschränkt und eine strenge Zweckbindung gefordert werden. Stahlmann (1994) spricht in diesem Zusammenhang von der Notwendigkeit „kalkulierten Nichtwissens".
- Tradeoffs mit *Effizienz* ergeben sich aus dem Konflikt zwischen der grundsätzlich effizienzsteigernden Wirkung der Digitalisierung der Verwaltung einerseits und dem Grundrecht auf Schutz der Privatsphäre andererseits. Das gilt für das Grundbuch, die Datenbank des Hauptverbands der Sozialversicherungsträger über die Erwerbstätigen wie für das zentrale Melderegister. Optimal unter dem Gesichtspunkt der Effizienz der Verwaltung wie der Statistik wäre die totale Vernetzung durch Zuordnung der jeweiligen Statistiken zu konkreten Personen. Aus diesem Grund wird im Datenschutzrat auch eine Debatte über die Einführung einer Personenkennzahl (PKZ) und deren Ausgestaltung geführt. Zu beachten wird dabei nicht bloß der Schutz der Privatsphäre als solcher sein, sondern auch die Tatsache, dass die „Statistik Austria – Die Informationsmanager" als inzwischen aus budgetären Gründen ausgegliedertes Unternehmen, dessen Mitarbeiter nicht mehr dem eher restriktiven Beamtendienstrecht unterstehen, recht intensiv nach zusätzlichen kommerziellen Verwertungsmöglichkeiten ihrer Daten‚schätze' sucht (und das aus finanziellen Gründen wohl auch muss). Ein weiteres aktuelles Beispiel für einen solchen Tradeoff ist die Medcard bzw. Sozialversicherungskarte. Die Speicherung aller Gesundheitsdaten und Arzt-

[36] Siehe etwa die Aktion des Finanzministeriums gegen die Schwarzverkäufe von Bier durch die Wirte.

[37] Es gibt zwar ein Grundrecht auf Datenschutz (§1 DSG 2000 als Verfassungsbestimmung), das auch in Art. 8/1 EMRK zu finden ist („Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs."), nicht hingegen auf Effizienz.

besuche würde für die Administration wie für Notfälle durchaus hilfreich sein, andererseits wäre ohne spezifische Vorsorge aber auch kaum zu verhindern, dass sich zahlreiche Interessenten – von Arbeitgebern bis zu Versicherungen – den Zugang zu diesen Daten erzwingen würden.

- Tradeoffs mit *Komfort* schließlich ergeben sich daraus, dass die Preisgabe der Privatheit vielfältige Vorteile bringt: Rabatte im Fall der Kundenkarte sowie für manche interessante Angebote,[38] rasche Kommunikation im Fall von E-Mail bzw. – oft nicht ganz so rasche – Information durch das Internet, usw. Verzicht auf all das würde ein Mehr an Privatheit um den Preis erheblicher Komforteinbußen bedeuten.

Die Tatsache, dass die rasch zunehmenden Möglichkeiten der Datensammlung, -vernetzung und -auswertung auch verschiedentlich erhebliche Vorteile mit sich bringen, darf über die damit verbundenen beträchtlichen Eingriffe in die Privatsphäre nicht hinwegtäuschen. Auch die bis jetzt ausgebliebene ‚Rebellion der Betroffenen' gegen ihre Durchleuchtung und Überwachung sollte nicht vorschnell als Zustimmung interpretiert werden. Derzeit herrscht noch sehr wenig Bewusstsein über die tatsächlichen Abläufe und Verknüpfungen bei Kundenkarten, E-Cash-Systemen, Mobilkommunikation, etc. Die Stimmung kann rasch umschlagen, wenn Massenmedien die ‚realen' Rückwirkungen des ‚virtuellen' Verhaltens aufzeigen und problematisieren. Soll man mit Gegenmaßnahmen solange warten? Vieles spricht dafür, die laufende Entwicklung als bedenklich anzusehen und keineswegs abzuwarten: Die verschiedenen Nachteile, die aus der Verletzung der Privatsphäre resultieren, wurden bereits ausführlich besprochen. Dazu kommt die Gefahr, dass das System aus Bequemlichkeit und vordergründigen Interessen in eine Situation schlittert, in die man gar nicht kommen wollte; in die Situation des Zauberlehrlings, der die von ihm gerufenen Geister nicht mehr los wird, weil sich das ganze System auf deren Tätigkeit eingestellt hat. Nicht bloß im Fall eines politischen Systemwechsels, auch bei Umschlagen der Stimmung – vom benign neglect der Überwachung zu ihrer Ablehnung – könnten diese Abhängigkeiten äußerst unangenehm werden. Zu diesen ‚Geistern' mit Eigendynamik gehören zweifellos auch die kommerziellen Interessen der ‚Sicherheitsindustrie', die durch Schüren der Angst immer raffiniertere Überwachungsanlagen zu rechtfertigen und zu verkaufen sucht.

7 Ansätze zum Schutz der Privatsphäre in der Informationsgesellschaft

Welche Schlussfolgerungen ergeben sich aus all diesen Überlegungen über die neuen technischen Möglichkeiten der Informationssammlung, -speicherung, -vernetzung und -auswertung für den Datenschutz in der Informationsgesellschaft? Zunächst sollte betont werden, dass die Geschichte des Datenschutzes weit zurück reicht, Elemente des Datenschutzes somit sehr viel älter sind als die digitalen Datenbanken. Die Wurzeln des Datenschutzes liegen in den Verschwiegenheits- bzw. Standesregeln: Der Eid des Hippokrates stammt bereits aus dem 5. Jahrhundert vor Christus; umfassende ‚Persönlichkeitsrechte' wurden allerdings erst gegen Ende des 19. Jahrhunderts intensiver diskutiert, auch wenn einzelne, wie etwa das Briefgeheimnis, schon in der Aufklärung allgemein anerkannt wurden (Gridl 1999, 19f). Warren und Brandeis wehrten sich 1890 in der Publikation

[38] Z. T. ist das nichts anderes als der elektronische – billigere und weniger treffsichere – Ersatz der traditionellen Beratung durch den geschulten Verkäufer, der die Buchinteressen seiner Stammkunden sehr viel besser abschätzen kann als das digitale System von Amazon.

"The Right to Privacy" gegen die Übergriffe der Sensationspresse auf das Privatleben und leiteten aus dem damaligen Rechtsbestand der USA ein "right to be let alone" ab. Bereits in dieser ersten Privacy-Debatte spielten neue Technologien wie Photoapparat, mechanische Druckereien und neue Übermittlungsmethoden eine wesentliche Rolle (Gridl 1999, 20). Datenschutzgesetze i.e.S. haben allerdings erst mit der Verbreitung der elektronischen Datenverarbeitung Eingang in die Rechtsordnung gefunden: In Österreich begann die Diskussion in den sechziger Jahren, ein erster Gesetzentwurf lag 1973 vor und wurde 1978 beschlossen (Egger 1990, 87ff).

Das bestehende Datenschutzrecht geht – wie erwähnt – von Datenschutz im unmittelbaren Sinn des Wortes aus, also dem Schutz von Daten. Das entsprach den Bedürfnissen der siebziger Jahre des vergangenen Jahrhunderts: Große Rechenanlagen in eigens eingerichteten und physisch abgeriegelten Rechenzentren. Dort konnten die Dateien als solche geschützt und damit der eigentliche Schutzzweck erreicht werden – die Verhinderung ihres Missbrauchs. Bereits mit der Verbreitung der Personal Computer (PC) und der Dezentralisierung der Informationstechnik konnte Datenschutz als ‚zentralistisches' Schutzrecht nicht mehr adäquat greifen, umso weniger, als die PCs immer stärker vernetzt wurden, zuletzt weltweit im Rahmen des Internet.

Der traditionelle Datenschutz in Form eines Schutzes vor Missbrauch von Daten durch physische Separierung (Funk 1994, 581) war nie sehr schlagkräftig und ist heute durch die technische Entwicklung überholt. Die meisten Datenschutzgesetze basieren allerdings nach wie vor auf der inzwischen obsoleten Unterscheidung von Erhebung, Speicherung und Weitergabe von Daten sowie von sensiblen und nicht-sensiblen Daten; sie differenzieren nicht zwischen 'data storage' und 'data flow' (Noam 1992) und leiden vor allem darunter, dass dezentralisierte "very large systems are very hard to document, monitor, diagnose, fix, and replicate" (Coates 1992). Zwar gibt es überall in Europa Datenschutzbeauftragte, doch sind sie weitgehend ohne Macht.[39] Neue Ansätze sind dringlich. Ein wichtiger Schritt in diese Richtung war das im deutschen Volkszählungsurteil (1983) festgemachte „informationelle Selbstbestimmungsrecht", das Recht des Individuums selbstbestimmt zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte preisgegeben werden. „Zugrunde liegt all diesen Ansätzen der Gedanke, dass dem Einzelnen ein von der öffentlichen Sphäre abgesonderter Bereich privater Lebensführung zukommt, in dem dieser frei von staatlichen und gesellschaftlichen Zwängen als autonomes Subjekt über seine Person und sein Eigentum bestimmen kann." (Funk 1994, 562). Das geht über die traditionellen statischen Datenschutzregelungen weit hinaus, ist in Österreich jedoch bis heute nicht verwirklicht.

Der Begriff des informationellen Selbstbestimmungsrechts stellt insofern einen wesentlichen Leitgedanken der Datenschutzdebatte dar, als er die *aktive* Rolle des jeweils Betroffenen betont; eine solche wird tatsächlich zunehmend wichtig, da legistische Schutzmaßnahmen *allein* die Probleme kaum lösen können – schon aufgrund der Unübersichtlichkeit und Unkontrollierbarkeit der dezentralen Datensammlung und –speicherung. Das eigene ‚virtuelle' Bild entzieht sich zunehmend der eigenen Steuerung.[40] Hieraus könnte der Schluss gezogen werden, der beste Datenschutz wäre Datenvermeidung. Eine solche Strategie stößt jedoch rasch an Grenzen. Denn die Netze werden nicht bloß immer dichter, die Nutzung häufiger und die generierbaren Profile aussagekräftiger, auch die Teilnahme an den Aktivitäten, die eine Preisgabe persönlicher Daten implizieren, lässt

[39] Die USA kennen keine Datenschutzbehörden. Die einzelnen Gesetze eröffnen vielmehr dem Individuum Zugang zu „seinen" Daten. Das Prinzip der „informational autonomy" vereint einerseits das Recht auf Kontrolle über das eigene informationelle Bild, andererseits aber auch Zugang zu allen relevanten Informationen, die eine Beteiligung der Bürger an gesellschaftlichen Entscheidungsprozessen ermöglichen. Diese Öffentlichkeitsprinzip wird als wichtiges Schutzschild gegen behördlichen Machtmissbrauch angesehen. „Sunlight is said to be the best disinfectant" (vgl. Funk 1994, 575f).

[40] Das steht in diametralem Gegensatz zur informationellen Selbstbestimmung. Demgemäß müssen Rahmenbedingungen geschaffen werden, die die Selbststeuerung erleichtern, wie der Ausbau bestehender Auskunfts und Informationspflichten, grundsätzliches Verbot der Weitergabe von Daten (opt-in, also Zustimmungspflicht statt opt-out – Verweigerungsmöglichkeit), etc.).

sich immer weniger vermeiden. Eine Strategie der Verweigerung könnte vielleicht noch auf Kredit- und Bankomatkarten verzichten, auf Mobiltelefon und Surfen im Internet. Doch der Preis einer derartigen Sicherung der Privatsphäre wäre eine erhebliche Einbuße an Bequemlichkeit und Lebensqualität, bis hin zu Kontaktverlust und Vereinsamung. Für einzelne Individuen mag eine solche Verweigerungsstrategie möglich sein – wenn auch, im Extremfall um den Preis, dass sie sich gerade dadurch verdächtig machen; der normale Staatsbürger jedoch, als Arbeitnehmer, Gehaltsempfänger, Steuerpflichtiger, Krankenversicherter, Transferleistungsempfänger oder Verdächtiger der Polizei, eingebettet in vielfältige soziale Beziehungen, Gruppen, Organisationen und Kommunikationsnetzwerke, ist den Informations- und Kommunikationstechnologien hilflos ausgeliefert.[41].

Allerdings: Auch wenn es der bewussten und aktiven Mitarbeit der Betroffenen bedarf, ist ein gesetzlicher Rahmen unverzichtbar, da allein er dem Einzelnen die Möglichkeit gibt, sein informationelles Selbstbestimmungsrecht auch durchzusetzen. Dabei geht es nicht um Verhinderung bestimmter Techniken, sondern um den Rahmen für eine Entwicklung, die im Einklang mit demokratischen Grundrechten stattfindet und diese nicht aushöhlt; es geht um die Schaffung entsprechender Sicherheit und entsprechenden Vertrauens in das System als Voraussetzung für die Akzeptanz durch die Nutzer und damit auch für den wirtschaftlichen Erfolg (z. B. bei E-Commerce).

Es kann allerdings nicht Aufgabe dieses Beitrags sein, einen solchen gesetzlichen Rahmen zu entwickeln, zum Teil, weil unser Forschungsprogramm am ITA erst begonnen hat, vor allem aber, weil diese Probleme noch kaum das Bewusstsein breiterer Bevölkerungskreise – und damit in das Bewusstsein der Politik – erreicht haben, die öffentliche Debatte bestenfalls in ihren Anfängen steht. Sehr wohl aber lassen sich einige Grundsätze ableiten und einige Instrumente diskutieren. Dabei darf allerdings nie vergessen werden, dass es endgültige Lösungen auf diesem Gebiet nicht geben kann: Die Dynamik rasch aufeinanderfolgender technischer und organisatorischer Innovationen läßt laufend neue Probleme entstehen,[42] und die Tradeoffs, die Einschätzung der relativen Austauschbeziehungen zwischen den einzelnen Zielen – etwa Komfort versus Preisgabe persönlicher Daten – ändern sich zwangsläufig.

7.1 Grundsatz der Verhältnismäßigkeit

Er ergibt sich aus dem Janusgesicht der Digitalisierung, den im vorigen Abschnitt ausführlich besprochenen kritischen Austauschbeziehungen zwischen dem Schutz der Privatsphäre auf den einen Seite und Sicherheit, Komfort und Effizienz auf der anderen; es muss zu einer Güterabwägung kommen: Nicht alles was machbar ist, darf auch getan werden. Verhältnismäßigkeit ist in diesem Zusammenhang in dreierlei Dimensionen zu beachten: Verhältnismäßigkeit zwischen dem Wert der ungestörten Privatsphäre auf der einen Seite und (1) dem Wert des jeweils verfolgten Ziels als solchem, (2) dem Erfolg bei seiner Verfolgung, und (3) dem damit verbundenen materiellen Aufwand auf der anderen.

[41] „Die gesellschaftliche und technische Abhängigkeit des Einzelnen macht ihn bis in den letzten Winkel der privaten Lebensgestaltung zum Objekt unterschiedlicher Formen der Identifizierung. In der Verschränkung von Datenverarbeitung und Gentechnologie beispielsweise wird selbst der Körper als letzte ‚natürliche Grenze' aufgelöst." (Funk 1994, 564) Dies führt dazu, eine"genetic privacy" einzufordern, die ethische, gesellschaftlich politisch anerkannte Grenzen der Identifizierung, des Mapping, des Screening und darauf basierender (unsicherer) Vorhersagen definiert. Die Gefahr des „genetic labelling" (die Kategorisierung von Menschen aufgrund ihrer Gen-Konstitution) ist im Prinzip die stärkste Form der ‚Risikoselektion'.

[42] Überdies ist zu beachten, dass Folgen für die Privatsphäre ja nicht nur beim Missbrauch, sondern auch beim ‚normalen', bestimmungsgemäßen Gebrauch der Daten entstehen können.

Für den Komplex der *Sicherheit* bedeutet Verhältnismäßigkeit, dass Überwachung so sparsam als möglich eingesetzt werden sollte, stets einer spezifischen Genehmigung bedarf, und dass generelle Überwachung bloß in Sonderfällen möglich sein sollte. Generelle Videoüberwachung aller Staatsbürger und komplexe Programme der Verfolgung einzelner über weite Gebiete überschreiten wohl nach allen drei Kriterien den Grundsatz der Verhältnismäßigkeit. Gleichermaßen ist Verhältnismäßigkeit auch bei der Überwachung durch Verknüpfung persönlicher Daten in jedem Einzelfall zu beachten. Auch bei der Bekämpfung der Cyberkriminalität, die vor allem von der EU-Kommission in letzter Zeit forciert wird; besteht die große Gefahr, dass dabei die Vermeidung von Delikten, die die Privatsphäre verletzen, mit einem unverhältnismäßig starken weiteren Eindringen in die Privatsphäre erkauft werden müsste (Čas 2001, 7).

Weniger problematisch erscheint der Tradeoff zwischen Schutz der Privatsphäre und *Komfort,* da es zumeist um eine Entscheidung des Betroffenen selbst geht. Allerdings muss dafür gesorgt sein, dass sich der Betroffene der Folgen seiner Entscheidung voll bewusst ist, denn die kommerziellen Anbieter der diversen elektronisch-digitalen Dienste versuchen bekanntlich die verschiedenen Nachteile nach Möglichkeit zu verschleiern.

Sehr viel schwieriger, nicht zuletzt weil vielfältiger, stellt sich das Problem der Verhältnismäßigkeit bei dem Tradeoff mit *Effizienz*, am häufigsten im Bereich der öffentlichen Verwaltung und des Sozialwesens i. w. S. Wie später noch gezeigt wird, ist in manchen Fällen eine zumindest teilweise Lösung durch die Gestaltung der Zutrittsbedingungen denkbar. Das gilt allerdings nicht für die bereits erwähnten Probleme im Bereich der Statistik: Die großen Grundzählungen wie Volkszählung, Betriebszählung, Arbeitsstättenzählung usw. sind teuer und mit erheblichen Fehlermargen behaftet – also ineffizient; die benötigten Informationen sind in administrativen Statistiken zumeist bereits vorhanden. Allerdings müssten diese bereinigt, u. U. zentralisiert, miteinander verbunden und laufend aktualisiert werden. Aktuelle Beispiele mit solcher Zielsetzung mit allen ihren problematischen Folgen sind die Einkommensstatistik gemäß Bezügegesetz, die Zentralisierung des Melderegisters und die Personenkennzahl. Einem bestimmten Datensatz soll jeweils eine ganz bestimmte Person zugeordnet werden können. Dabei gehen die Probleme über diejenigen der Zugriffsberechtigung weit hinaus. Neben den in Abschnitt 6 ausgeführten Gefahren aus der potentiellen Verwertung der Daten durch ein inzwischen ausgegliedertes Unternehmen „Statistik Austria“ geht es vor allem um die Verbindung und Weiterführung der Daten: Die Verbindung ermöglicht ein, sehr genaues Bild der jeweiligen Person zu zeichnen (siehe Mosaiktheorie), und die Daten veralten rasch, wenn sie nicht laufend aktualisiert werden, was umfangreiche Meldepflichten, – und daraus resultierend Überwachungsmöglichkeiten – voraussetzt.

7.2 Grundsatz der Forcierung nicht-speichernder Alternativtechnologien

Dieser Grundsatz beruht auf der Erkenntnis, dass es keine ‚neutrale‘ Technik gibt. Technische Systeme werden auf die Erreichung bestimmter Ziele hin entwickelt; es kommt stets auf den Zweck der Anwendung und die darauf gerichtete Gestaltung an. Marktkräfte sorgen dafür, dass die verschiedenen Informationstechnologien kommerziellen Rentabilitätsanforderungen genügen, kaum je jedoch dafür, dass sie die Privatsphäre entsprechend schützen – ganz im Gegenteil: Die Sammlung von persönlichen Daten, das möglichst tiefe Eindringen in die Privatsphäre, ist kommerziell zumeist höchst rentabel, der Widerstand des Einzelnen für ihn selbst hingegen ‚unrentabel‘, weil in den seltensten Fällen zielführend. Die sozialverträgliche Gestaltung muss deshalb eine gesamtgesellschaftlich-staatliche Aufgabe sein. Ein diesbezügliches Instrument ist die Forcierung des Angebots von nicht-speichernden Alternativtechnologien: Etwa anonyme Telefon-Wertkartensysteme, anonyme Zahlungskarten (E-Cash, Quick-Karte), oder anonyme Maut-Abbuchung beim Road pricing.

Die kommerziellen Mobilkommunikations-Provider bieten solche Systeme zwar durchaus an, da sie damit zusätzliche Kundenschichten erschließen können, sie lassen sich den Verzicht auf den Zugang zu personenbezogenen Daten allerdings zumeist recht teuer abgelten. Bei der Diskussion über die Einführung alternativer Systeme zur Einhebung der Straßenverkehrsabgabe hingegen wurde die Frage des Schutzes der Privatsphäre durch anonyme, nicht-speichernde Einhebungsformen nicht einmal diskutiert.[43]

7.3 Grundsatz der Minimierung der Speicherung und der begrenzten Vernetzbarkeit

Dieser Grundsatz muss als Folge eines der eher seltenen Fälle gefordert werden, in denen neue Techniken als solche tatsächlich zusätzliche Regulierungen erfordern, der Zwang zur Regulierung also direkte Technikfolge ist: Während beim analogen Telefonsystem jede Verbindung nach Beendigung ‚spurlos' verschwunden war,[44] eine Speicherung der Daten daher technisch speziell eingerichtet werden musste und primär Kosten verursachte, *müssen* die Verbindungsdaten bei digitalen Systemen technikimmanent zwischengespeichert werden. Um denselben Schutz der Privatsphäre zu erreichen wie beim analogen System muss nicht bloß Ausmaß und Zeitdauer der Speicherung reguliert, sondern auch organisatorisch-technisch Vorsorge für die Löschung der Daten getroffen werden.[45] Mit ihrer automatischen Verfügbarkeit steigen zugleich auch die Begehrlichkeiten nach der Verfügungsmacht über diese Daten, wie die Wünsche nach Schnittstellen für die ‚gesetzlich ermächtigten Behörden' zeigen.[46] Das European Telecommunication Standards Institute (ETSI) hat spezifische Schnittstellen definiert, die es gesetzlich ermächtigten Behörden ermöglichen, den Telefon- und Internetverkehr auch *ohne Wissen der Betreiber und anderer Behörden* abzuhören.

Gleichermaßen Technikfolge, nämlich Folge der Verbilligung und der enorm ausgeweiteten Möglichkeiten der Datenspeicherung und des data mining, ist das Interesse der Wirtschaft an Persönlichkeits- und Verhaltensdaten ihrer Kunden. Eine dem Betroffenen nicht bekannte Vernetzung von Dateien ist jedoch nicht bloß im kommerziellen sondern auch im öffentlichen Bereich ein massiver Eingriff in die Privatsphäre. Alles was eine solche Vernetzung erleichtert ist daher aus der Sicht des Datenschutzes überaus bedenklich. Im besonderen Maße gilt das für die verschiedentlich vorgeschlagene Personenkennzahl oder unterschiedlichen Formen von Bürgerkarten – es sei denn, dass der Betroffene mit ihrer Hilfe die Zugriffsmöglichkeiten auf seine Daten selbst steuern kann.

[43] Ganz im Gegenteil wurde zuletzt ein ‚Road pricing per Handy' entwickelt und auf der Südautobahn getestet, das über das Satellitennavigationssystem den jeweiligen Standort des LKW ermittelt und an einen Zentralrechner mitteilt; Mautpreller sollen durch ‚Enforcement cars' identifiziert werden, die beim Vorbeifahren an dem LKW dessen Daten abrufen und mit denen der Datenbank vergleichen. (Die Presse 16.5.2001, 23). Vor allem bei der wohl zu erwartenden Ausdehnung der Maut auf PKW wäre mit diesem System eine weitere, ganz beträchtliche Einengung der Privatsphäre verbunden.

[44] Eine Überwachung und Speicherung durfte nur erfolgen, wenn sie gerichtlich angeordnet wurde, und erforderte eine spezifische technische Ausstattung für die Speicherung.

[45] Das Telekommunikationsgesetz unterscheidet Stamm-, Vermittlungs- und Inhaltsdaten, für die jeweils unterschiedliche Vorschriften bestehen. Da die Speicherung billig und eine spätere kommerzielle Verwertbarkeit durchaus möglich ist, werden gerade sensible persönliche Daten ohne gesetzliche Verpflichtung bloß unzureichend gelöscht.

[46] Das ist ein eigener Komplex, der in diesem Rahmen nicht behandelt werden kann. Kurz gesagt geht es darum, dass in europäischen Standardisierungsforen technische Standards zum Abhören geschaffen werden, die in weiterer Folge durch Europaratsentschließungen und nationale „Überwachungsverordnungen" politisch sanktioniert werden.

7.4 Grundsatz der strengen Limitierung der Zugriffsberechtigungen

Die breiten – und sich im allgemeinen automatisch rasch weiter ausweitenden – Zugriffsmöglichkeiten auf Datenbanken mit persönlichen Daten sind die häufigste Quelle der Verletzung der Privatsphäre. Dafür sind nicht bloß kommerzielle Interessen und Neugier verantwortlich, sondern vielfach auch Interesse an Effizienz: Die Beispiele reichen von den verschiedenen Formen des E-Government – One-Stop-Shop oder Ausstellung des Passes außerhalb der Wohnsitzgemeinde – über eine Medcard, die Zutritt zu allen Gesundheitsdaten ermöglicht, bis zur Bürgercard. Bei der Regelung der Zutrittsbedingungen bestehen allerdings durchaus unterschiedliche Optionen mit unterschiedlichen Folgen für den Schutz der Privatsphäre: Der jeweilige Beamte, Arzt, usw. kann Zugriff auf alle notwendigen Dateien haben, womit deren Missbrauch programmiert ist, selbst wenn die Zugriffsmöglichkeiten limitiert sind und protokolliert werden müssen. Als Privacy-freundliche Alternative dazu kann der grundsätzlich zugriffsberechtigte Beamte, Arzt, usw. im konkreten Fall auf personenbezogene Datenbestände bloß dann zugreifen, wenn der Bürger seinen ‚Schlüssel' dafür (z. B. Chipkarte) zur Verfügung stellt. Allerdings funktioniert selbst dieses Verfahren bloß dann, wenn zuvor eine entsprechende Aufklärung den Bürgern ihre Rechte bewusst macht, also klarlegt, dass sie den Zugriff sehr wohl verweigern können. Die Zugriffsberechtigung müsste allerdings auch bei diesem Verfahren streng limitiert und kontrolliert werden, um Unberechtigten – etwa Arbeitgebern, Versicherungen etc. – den Zugriff selbst mit Zustimmung des Betroffenen (Druck zur Ausfolgung der Karte!) zu verweigern.

7.5 Einrichtung eines Datenschutzbeauftragten mit Pouvoir

Angesichts der Dynamik des Systems und der Unmöglichkeit einer strikten gesetzlichen Regelung erscheint die Schaffung eines Bundesbeauftragten für den Datenschutz mit entsprechender Infrastruktur und Ausstattung zur Kontrolle unverzichtbar; die derzeit bestehenden Einrichtungen, Datenschutzrat (DSR) und Datenschutzkommission (DSK) reichen dafür keineswegs aus. Neben der bisher vorherrschenden starken Orientierung auf juristischen Sachverstand sind vor allem technische Expertise und dauerhaft zur Verfügung stehende Ressourcen notwendig, um die komplexen Entwicklungen proaktiv analysieren und steuernd eingreifen zu können. Selbst auf der Ebene darunter, der einfachen Informationsbereitstellung für interessierte Bürger, können die österreichischen Einrichtungen nicht mit der Zeit Schritt halten: Als Beispiel sei nur angeführt, dass (anders als die deutschen Bundes- und Landesbeauftragten für den Datenschutz) weder die DSK noch der DSR eine eigene website mit Tipps und einschlägigen Hinweisen hat! Die einzigen österreichischen Sites kommen von der ARGE Daten (http://www.ad.or.at/office) und von einzelnen engagierten Juristen (http://www.kronegger.at/ und http://normative.zusammenhaenge.at/inhalt.html.

7.6 Grenzen einer nationalen gesetzlichen Regelung des Datenschutzes

Abschließend muss auf zwei bedauerliche Begrenzungen nationaler Regelungen zum Schutz der Privatsphäre hingewiesen werden, nämlich die Internationalisierung der Information und die Notwendigkeit des bewussten Umgangs der Staatsbürger mit ihren persönlichen Daten.

Die Information entzieht sich einer *nationalen Steuerung* noch viel stärker als andere wirtschaftliche Aktivitäten, vor allem seit sie durch den elektronischen Datenverkehr an Mobilität erheblich gewonnen hat. Diese Mobilität ermöglicht 'jurisdiction hopping', die Trennung von Transaktionen und Datenbanken und deren Verlagerung in das Gebiet mit der jeweils lockersten Regulierung: „Banking auf den verschwiegenen Bahamas, Datenspeicherung im liberalen Finnland, Steuerzahlung auf den großzügigen Barbados." (Fischermann 2001, 14). Anders als die Steuerparadiese beruhen die ‚Datenbankparadiese' allerdings weniger auf dem egoistischen kommerziellen Bemühen exotischer Kleinstaaten, Firmen anzulocken, als eher auf unterschiedlichen Einstellungen gegenüber Amtsverschwiegenheit/Datenschutz versus Öffentlichkeitsgrundsatz/Informationsfreiheit. Wie weiter vorne erwähnt, sind die diesbezüglichen Systeme in Skandinavien und auch in den USA völlig anders gewachsen und dementsprechend auch anders gestaltet als etwa in Österreich oder Deutschland. Das bedeutet, dass die unbedingt erforderliche Regelung auf einer übernationalen Ebene auf ganz besondere Schwierigkeiten stößt.

Die zweite Begrenzung eines umfassenden gesetzlichen Schutzes der Privatsphäre ergibt sich aus der unbedingt erforderlichen Mitwirkung der Betroffenen. Das setzt allerdings umfassende Maßnahmen der Bewusstseinsbildung voraus, da die Gefahr besteht, dass mangelnde Kenntnisse und Bequemlichkeitsdenken den Einzelnen wie die Gesellschaft in eine Situation schlittern lassen, in die diese nicht geraten wollten. Es gilt, 'Awareness' in Bezug auf bewusste Nutzung der digitalen Angebote zu schaffen; die Gefahr eines 'Digital Divide' besteht nicht nur als Folge ökonomischer Unterschiede und Zugangsbarrieren, sondern auch in Form eines ‚qualifikatorischen Digital Divide' in ‚Unbedarfte' und ‚Bedarfte' betreffend die Möglichkeiten des Schutzes der Privatsphäre.

8 Literatur

BORKING, J. (1998): 2008 – Ende der Privatheit? In: H. Bäumler, Hg, Der neue Datenschutz, Neuwied: Luchterhand, 283–93.

ČAS, J. und W. PEISSL (2000): Beeinträchtigungen der Privatsphäre in Österreich. Teil I Bestandsaufnahme: Datensammlungen über ÖsterreicherInnen, Wien: ITA.

ČAS, J. (2001): Der Preis der Bekämpfung der Cyberkriminaität. ITA-News März 01, 7–8.

COATES,V. T. (1992): The future of information technology. Annales AAPSS 522, 45–56.

EGGER, E. (1990): Datenschutz versus Informationsfreiheit – Verwaltungstechnische und verwaltungspolitische Implikationen neuer Informationstechnologien. In: Schriftenreihe der Österreichischen Computer Gesellschaft, Bd. 52, Wien, München: OCG, Oldenbourg.

ELIAS, N. [^{2}1969] (1978): Über den Prozeß der Zivilisation. Soziogenetische und psychogenetische Untersuchungen. Band I: Wandlungen des Verhaltens in den weltlichen Oberschichten des Abendlandes; Band II: Wandlungen der Gesellschaft. Entwurf zu einer Theorie der Zivilisation, Suhrkamp Taschenbuch.

FISCHERMANN, Th. (2001): Flucht in den Cyberspace. Die Zeit 17, 19.4.2001, 11–14.

FLINT, J. (2000): Smart Dust. In: Schulzki-Haddouti, C., Hg, Vom Ende der Anonymität. Hannover: Heinz Heise, 105–107.

FOUCAULT, M. (1977): Überwachen und Strafen. Die Geburt des Gefängnisses. Frankfurt/Main: Suhrkamp.

FUNK, A. (1994): Öffentlichkeit und Privatheit im Zeitalter technischer Kommunikation – Ein Vergleich amerikanischer und deutscher Regelungsstrukturen. Leviathan (4), 560–592.

FUZO (2001a): Gadgets auf der Jagd nach Verbraucherdaten. [Aufgerufen am: 01-04-11 2001], <http://futurezone.orf.at/futurezone.orf?read=detail&view=bw&id=60108&tmp=94259>.

FUZO (2001b): ‚Web-Bugs" bedrohen Privatsphäre. [Aufgerufen am: 01-04-11 2001], <http://futurezone.orf.at/futurezone.orf?read=detail&view=bw&id=59352&tmp=72473>.

GRIDL, R. (1999): Datenschutz in globalen Telekommunikationssystemen. In: Frankfurter Studien zum Datenschutz, Bd. 12, Hg S. Simitis, Baden-Baden: Nomos.

HUBMANN, H. (1967): Das Persönlichkeitsrecht Köln: Böhlau.

LECHNER, M. (2000): Konsumentenwünsche sind vorhersehbar. Standard, B1.

LYON, D. (1997): Chipkarten und Technopolizei. Interview; [Aufgerufen am: 4.5. 2000] <http://www.heise.de/bin/tp/issue/dl-artikel.cgi?artikelnr=8025&mode=html>.

NOAM, E., (1992): Telecommunications in Europe. New York, Oxford: ...

NOGALA, D. (2000): Der Frosch im heißen Wasser. In: Schulzki-Haddouti, C. H., Hg, Vom Ende der Anonymität, Hannover: Heinz Heise, 139–155.

OTA (1986): Electronic Uses and Individual Privacy. Washington.

PEISSL, W. (2000): Überwachung total: ECHELON. ITA-News, April 2000, 10–11.

PEISSL, W., ČAS, J. (2000): Beeinträchtigung der Privatsphäre – Datensammlungen über ÖsterreicherInnen. Oktober 2000, Wien: ITA <http://www.oeaw.ac.at/ita/ebene5/d2-2a24a.pdf>.

POST (1998): Data Protection – Online Discussion, Report. Nr. E-1, December 1998, London: POST <http://www.parliament.uk/post/e1.pdf>.

REISCHL, G. (2001): Gefährliche Netze. Wien: Ueberreuter.

RÖTZER, F. (2000a): Man ist, wie man geht. In: Schulzki-Haddouti, C. H., Hg, Vom Ende der Anonymität, Hannover: Heinz Heise, 108–109.

RÖTZER, F. (2000b): Verkleidung zwecklos. In: Schulzki-Haddouti, C. H. Hg, Vom Ende der Anonymität, Hannover: Heinz Heise, 112–113.

RÖTZER, F. (2000c): Wer gut und böse ist. In: Schulzki-Haddouti, C. H. Hg, Vom Ende der Anonymität, Hannover: Heinz Heise, 157–168.

SCHOECHLE, T. D. (1995): Privacy on the information superhighway – will my house still be my castle? Telecommunications Policy 19 (6), 435–452.

SCHOENMACKER, M., STARRE, G. v. d. (2000): Personal data in the information society. Report to Parliament, September 2000, The Hague: Rathenau Institute.

SEIDEL, U. (1972): Datenbanken und Persönlichkeitsrecht. Köln: Schmidt.

STAHLMANN, G. (1994): Präventionsstaat und Sozialdatenschutz. [Aufgerufen am: 29.3. 2001] <http://www.fh-fulda.de/fb/sw/projekte/sozdat/praevstaat.htm>.

WARREN, S. D., Brandeis, L. D. (1890): The Right to Privacy. Harvard Law Review IV (5), 193ff.

Bisher erschienene manu:scripte

ITA-01-01 Gunther Tichy, Walter Peissl (12/2001): Beeinträchtigung der Privatsphäre in der Informationsgesellschaft. <http://www.oeaw.ac.at/ita/pdf/ita_01_01.pdf>

ITA-01-02 Georg Aichholzer(12/2001): Delphi Austria: An Example of Tailoring Foresight to the Needs of a Small Country. <http://www.oeaw.ac.at/ita/pdf/ita_01_02.pdf>

ITA-01-03 Helge Torgersen, Jürgen Hampel (12/2001): The Gate-Resonance Model: The Interface of Policy, Media and the Public in Technology Conflicts. <http://www.oeaw.ac.at/ita/pdf/ita_01_03.pdf>

ITA-02-01 Georg Aichholzer (01/2002): Das ExpertInnen-Delphi: Methodische Grundlagen und Anwendungsfeld „Technology Foresight“. <http://www.oeaw.ac.at/ita/pdf/ita_02_01.pdf>

ITA-02-02 Walter Peissl (01/2002): Surveillance and Security – A Dodgy Relationship. <http://www.oeaw.ac.at/ita/pdf/ita_02_02.pdf>