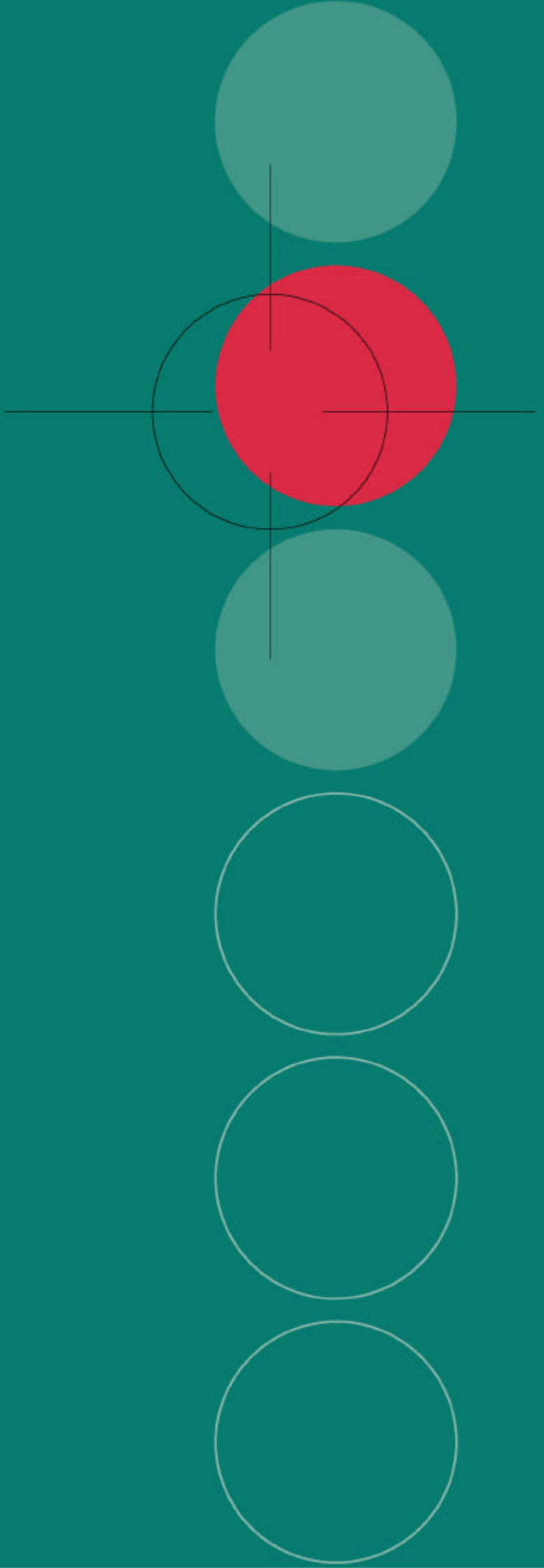
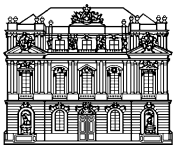
ÖSTERREICHISCHE
AKADEMIE DER
WISSENSCHAFTEN

INSTITUT FÜR
TECHNIKFOLGEN-
ABSCHÄTZUNG

BEEINTRÄCHTIGUNG DER PRIVATSPHÄRE IN ÖSTERREICH

TEIL I
BESTANDSAUFNAHME: DATENSAMMLUNGEN ÜBER ÖSTERREICHERiNNEN





BEEINTRÄCHTIGUNG DER PRIVATSPHÄRE IN ÖSTERREICH

TEIL I
BESTANDSAUFNAHME: DATENSAMMLUNGEN ÜBER ÖSTERREICHERiNNEN

INSTITUT FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
DER ÖSTERREICHISCHEN AKADEMIE DER WISSENSCHAFTEN

Johann Čas
Walter Peissl

unter Mitarbeit von
Telse Jochims

STUDIE IM AUFTRAG DER BUNDESKAMMER FÜR ARBEITER UND ANGESTELLTE

WIEN, OKTOBER 2000

Inhalt

Zusammenfassung

Forschungsprogramm des ITA zum Thema „Beeinträchtigung der Privatsphäre in der Informations-gesellschaft“

Die Entwicklung der sogenannten Informationsgesellschaft eröffnet nicht nur Firmen neue, globale Vermarktungschancen, sondern auch dem Einzelnen ungeahnte Möglichkeiten der internationalen Informationsbeschaffung und auch neue Arten der Unterhaltung. Sie bringt aber auch eine zusätzliche Bedrohung der Privatsphäre mit sich. Das Forschungsprogramm des ITA zum Thema „Beeinträchtigung der Privatsphäre in der Informationsgesellschaft“ nimmt sich deshalb vor, die neuen technologischen Möglichkeiten, ihre Chancen, Bedrohungspotentiale und mögliche Vermeidungsstrategien zu analysieren.

Zunahme der Bedrohung der Privatsphäre durch viele Datensammlungen und verbesserte Datenauswertungs-programme

Der vorliegende Bericht ist ein erster Schritt zur Aufarbeitung der empirischen Basis für weitere tiefergehende Analysen. Er zeigt auf, dass Daten über jede ÖsterreicherIn in einer *Vielzahl von Datensammlungen* gespeichert sind. Die Annahmen reichen von etwa 100 bis zu mehreren Hundert Datenbanken. Es ist jedoch nicht die Anzahl der Datensammlungen allein, die zu Beeinträchtigungen der Privatsphäre – diese reichen von vermehrter Belästigung durch persönlich adressierte Werbesendungen bis zu verstärkter Überwachung – führen können.. Durch die zunehmende Vernetzung und vor allem durch *verbesserte Datenauswertungsprogramme* (Data-Mining) können auch auf rein statistischer Ebene bessere Aussagen über Kleingruppen und mit hoher Prognosewahrscheinlichkeit auch über Einzelpersonen gemacht werden, als sich aus den gesammelten Daten allein ergäben.

Wie aus einer Gegenüberstellung von persönlichen Daten und verschiedenen Institutionen deutlich wird, zählen öffentliche Institutionen, Arbeitgeber, Finanzdienstleister und vor allem die Telekommunikationsbranche zu jenen Bereichen, wo am dichtesten Daten generiert werden. Ganz allgemein läßt sich eine *Dynamisierung* feststellen: nicht mehr nur statische Daten in Datensammlungen bilden die Grundlage für eine Bedrohung der Privatsphäre, vielmehr entstehen bei der Nutzung neuer Medien neue, sich bei jeder Mediennutzung verändernde Daten wie Kommunikations- und Inhaltsdaten, die eine umfassende Überwachung bzw. Verhaltensanalyse ermöglichen.

Sonderstellung der Telekommunikations-branche

Da sich zeigt, dass die *Telekommunikationsbranche* ein besonders heikles Feld darstellt, ist diesem Bereich ein umfassender Abschnitt in diesem Bericht gewidmet. Technische Entwicklungen wie Digitalisierung der Netze, Aufbau von Mobilkommunikationsnetzen und die boomende Internetnutzung, gemeinsam mit veränderten – deregulierten – Marktbedingungen eröffnen völlig neue Bedrohungsbilder für die reale und virtuelle Integrität.

Kommunikations- und Bewegungsprofile werden möglich

Durch die Digitalisierung werden Vermittlungsdaten – wer kommuniziert wann mit wem – automatisch generiert und gespeichert; durch die Mobiltelefonie kommen zusätzlich Bewegungsprofile hinzu – wo hält man/frau sich wann auf –; und durch die Kommunikation und Informationsbeschaffung über das Internet werden zumindest temporär auch Inhaltsdaten gespeichert (E-Mail) und die Inhalte der besuchten Websites lassen Rückschlüsse auf Interessen und Vorlieben der KonsumenInnen zu. Die Anzahl und die Art der Daten, die bei der Nutzung von Kommunikations- und Informationstechnologien anfallen, sind natürlich vom eigenen Verhalten determiniert, und daher auch individuell steuerbar. Die Förderung eines bewussten Umgangs mit den neuen Medien durch informierte BürgerInnen ist daher ein wesentlicher Bestandteil einer die Privatsphäre wahrenden Politik. Allerdings greift diese Maßnahme, auf sich allein gestellt, zu kurz: Mit der zunehmenden Durchdringung des wirtschaftlichen, gesellschaftlichen und privaten Lebens mit elektronischen Medien ist ein Verzicht auf deren Nutzung mit entsprechend geminderten Chancen zur vollen Teilnahme an diesem verbunden. Daher sind zusätzlich rechtliche Vorkehrun-

gen gegen eine missbräuchliche Verwendung von Daten und insbesondere technische Lösungen, welche eine anonyme Nutzung ermöglichen, zu treffen bzw. zu entwickeln.

Aus analytischen Gründen ist es auch angebracht, eine stärkere Differenzierung der *Datenkategorien* vorzunehmen. Das Datenschutzgesetz (DSG 2000) unterscheidet nur zwischen „personenbezogenen Daten" und „sensiblen Daten". Dazwischen gibt es jedoch eine Vielzahl von Abstufungen, die auch unterschiedliche „Sensibilität" aufweisen. Dies reicht von weitgehend frei verfügbaren sogenannten „Grunddaten" bis zu „Finanziellen Daten" und „Daten über bestimmte Gewohnheiten".

Datenschutz als Wettbewerbsfaktor

Für die nahe Zukunft sind unterschiedliche Entwicklungen vorauszusehen: einerseits werden Informationen – und damit Daten als deren Grundlage – zunehmend Warenwert annehmen. Die Nutzung personenbezogener Daten wird in Zukunft ein Teil unternehmerischen Handelns sein. Andererseits wird aber *Datenschutz ein Wettbewerbsfaktor* werden. Wer bei steigendem Datenaufkommen der Versuchung widersteht, diese extensiv zu nutzen bzw. von Beginn an offenlegt, wie er Daten zu nutzen gedenkt, wird bei den KonsumentInnen höheres Vertrauen genießen und so einen Wettbewerbsvorteil lukrieren. Zukünftig werden nicht nur gesetzliche Rahmen allein, sondern auch freiwillige Selbstbeschränkungen von Unternehmen und Institutionen – zumindest aber transparente *Datenschutzpolitiken* – notwendig sein, um KonsumentInnen vor allzu wild wuchernden Datenverarbeitungen zu schützen.

Trotz weiter Verbreitung von EDV und Neuen Medien gibt es in Österreich derzeit nur ein geringes Bewusstsein über mögliche täglich entstehende virtuelle Bilder. Ein nicht zu unterschätzender Faktor bildet dabei *individuelles Verhalten*. Mit Hilfe von bestimmten Technologien und auch durch Vermeidungsstrategien können übergroße Datensammlungen hintangehalten werden.

Aufklärungsarbeit notwendig

Es scheint hoch an der Zeit, *Aufklärungsarbeit* über mögliche Bedrohungen zu leisten und den KosumentInnen/BürgerInnen Hilfen an die Hand zu geben, wie sie sich in der Informationsgesellschaft reale und virtuelle Refugien der Ruhe und ungestörten Privatheit schaffen bzw. zurückgewinnen können.

I Einleitung

Das gegenständliche Forschungsprojekt ist Teil eines übergeordneten Forschungsprogrammes des Instituts für Technikfolgen-Abschätzung (ITA) der Österreichischen Akademie der Wissenschaften zum Thema „Beeinträchtigung der Privatsphäre in der Informationsgesellschaft". Durch die Entwicklungen zur sogenannten „Informationsgesellschaft" entstehen völlig neuartige Datensammel- und -verknüpfungsmöglichkeiten. Diese kritisch zu untersuchen, alternative technische Vorsorgemaßnahmen sowie Vermeidungsstrategien und Handlungsmöglichkeiten für Betroffene und Entscheidungsträger aufzuzeigen ist vorrangiges Ziel des Forschungsprogrammes. Der vorliegende Bericht zu „Datensammlungen über ÖsterreicherInnen" stellt eine vorläufige empirische Basis für weitere Analysen und tiefergehende Recherchen dar.

Das Grundrecht auf Privatsphäre ist immer öfter bedroht

In vielen Lebensbereichen hinterlassen KonsumentInnen Datenspuren, immer häufiger werden Daten gesammelt. Den KonsumentInnen ist der Zusammenhang zwischen alltäglichen Verrichtungen, der Inanspruchnahme von Dienstleistungen und den dahinter stehenden Datensammlungen oft nicht bewusst. Das Grundrecht auf Privatsphäre wird sowohl von öffentlichen Stellen wie auch von kommerziellen Anbietern immer öfter bedroht. Im gegenständlichen Forschungsvorhaben wird der Versuch unternommen, auf empirischer Basis aufzuzeigen, in welche Datensammlungen ein „Durchschnittsösterreicher" in den verschiedenen Lebensabschnitten kommen kann. Dies wird anhand der Gegenüberstellung von verschiedenen Daten (Merkmalen) einer Person mit Institutionen einerseits und Tätigkeiten andererseits abzuschätzen versucht. Aus den möglichen Verknüpfungen, den unterschiedlichen Datenklassen und den unterschiedlichen Branchen in denen Daten gesammelt und verarbeitet werden, können im weiteren unterschiedliche Bedrohungspotentiale und Szenarien abgeleitet werden.

Der empirischen Analyse der Situation in Österreich lagen folgende Fragen zugrunde:

Forschungsfragen

- Welche Datensammlungen entstehen im Alltag?
- Welche könnten zusätzlich entstehen?
- Wie sieht ein bewusster Umgang mit den Neuen Medien aus?

Anders ausgedrückt, entstehen folgende Forschungsfragen: Wie sieht der „typische" Minimaldatensatz eines/r jeden Österreichers/in aus? Was hat sich in den letzten 10 Jahren verändert, was wird sich ändern? Was produzieren KonsumentInnen selber „freiwillig", wird das mehr? Anleitungen zur Datenvermeidung!

2 Datenschutz: Zum Wandel eines Begriffs

Der Begriff Datenschutz ist, wenn auch eingeführt, so doch missverständlich. Es geht keineswegs um den Schutz von Daten, sondern vielmehr um den Schutz von Menschen vor den Folgen missbräuchlicher Datenverwendung. Ein Weg dazu war lange Zeit tatsächlich der physische Schutz von Daten in Rechenzentren. Die unglückliche Benennung hat vor allem historische Gründe. In den Anfängen waren die Datenverarbeitungsmaschinen zentrale Großrechner, in denen Daten gespeichert waren. Indem man diese schützte, waren auch missbräuchliche Verwendungen hintangehalten. Wenn man ein „Rechenzentrum" abschirmte und den Zutritt auf speziell geschultes und verantwortungsvolles Personal beschränkte, konnte (mit) den Daten nichts passieren. Völlig anders stellt sich die Situation heute dar. Natürlich werden auch heute noch viele Anwendungen der Massendatenverarbeitung in Großrechenanlagen von Banken, Versicherungen, anderen Dienstleistungsunternehmen und bei öffentlichen Institutionen bearbeitet. Durch die Miniaturisierung, die Entwicklung von PC und Laptop und vor allem durch die Vernetzung derselben entstehen jedoch völlig neue Anforderungen an den Datenschutz.[1] Weg von zentralistischen, relativ leicht realisierbaren Sicherheitskonzepten verlagert sich der Schutz immer weiter Richtung Sicherung der Endgeräte und der Verbindungswege. Damit kommt es zu einem Zusammenwachsen der Bereiche IT-Sicherheit und Datenschutz. Verfahren der IT-Sicherheit wie Verschlüsselung und Signierung können auch zum wirksamen Schutz der Privatsphäre eingesetzt werden. Zusätzlich zu den bestehenden gesetzlichen Rahmenbedingungen sind von den Institutionen öffentliche Datenschutzpolitiken einzufordern, in denen diese definieren, wie sie mit KonsumentInnendaten umgehen, für welche Zwecke sie diese verarbeiten und wie sich ihr Verhältnis zur informationellen Selbstbestimmung ihrer KundInnen generell darstellt. Wenn Preise und Dienstleistungen vergleichbar sind und KonsumentInnen ein steigendes Datenschutzbewusstsein an den Tag legen werden, wird eine verantwortungsvolle Datenschutzpolitik einen Wettbewerbsvorteil gegenüber anderen Anbietern im e-commerce darstellen.

Begriffsbestimmung: vom Datenschutz zur informationellen Selbstbestimmung

In der Diskussion von Datenschutzfragen wird immer öfter der englische Begriff "privacy" verwendet. Privacy (Zurückgezogenheit, Privatsphäre) wird oft auch mit „Recht auf informationelle Selbstbestimmung" übersetzt. In Anlehnung an eine Definition von Katsh, E.[2] werden darunter zwei Dimensionen subsumiert:

- Die Ebene der informationellen Selbstbestimmung, d. h. das Recht zur Kontrolle von Informationen über einen selbst, sowie
- das Recht in Ruhe (alleine) gelassen zu werden.

Es ist für die einzelne KonsumentIn durchaus von Belang zu wissen, wenn auch zunehmend schwieriger nachzuvollziehen, wer welche Daten über sie gespeichert hat. Die Belästigung – die zweite Dimension – wird möglicherweise in Zukunft von noch größerem Gewicht sein.

Es zeigt sich also ein Wandel des Begriffs vom Datenschutz zur informationellen Selbstbestimmung vom statischen, techno-zentrierten Ansatz der siebziger Jahre zur dynamischen Sichtweise im Zeitalter von WWW und Mobilkommunikation.

---

[1] Wiewohl natürlich auch für moderne DV-Systeme die §§ 14 und 15 DSG 2000 gelten, die den Auftraggeber und Dienstleister Datensicherungsmaßnahmen (technisch und organisatorisch) und die Geheimhaltung von Daten vorschreiben.

[2] zit. nach Schoechle 1995, 445.

Zu untersuchen ist auch, inwieweit die Gefährdung von Privatheit schon fortgeschritten ist. Wieviel Privatheit ist im sogenannten „Informationszeitalter" noch aufrecht zu erhalten und wie können teilweise bereits verlorene Rückzugsrefugien in realen und virtuellen Welten zurückgewonnen werden? Wenn man weiters davon ausgeht, dass eine moderne Lebensführung ohne Nutzung digitaler Medien nicht mehr sinnvoll denkbar bzw. in vielen Bereichen auch nicht wünschbar erscheint, muss man sich im Zuge von Datenschutzüberlegungen auch Gedanken zur Aufrechterhaltung von Daten-Integrität (siehe http://www.bigbrother.awards.at/2000/awards/) in der Informationsgesellschaft machen. Wenn Datenvermeidung in manchen Bereichen nicht realisierbar ist, weil man bestimmte Funktionen der neuen Medien gerne nutzt, so sollte doch sichergestellt werden, dass zumindest keine virtuellen Bilder entstehen, die einem im realen Leben schaden können.

Klassischer Datenschutz

Klassischer Datenschutz

Die o. a. Entwicklungen bedeuten nicht, dass gesetzliche Regelungen obsolet geworden sind. Vielmehr ist gerade in Hinblick auf die neuen Herausforderungen darauf hinzuweisen, dass der Schutz der Privatsphäre ein Grundrecht darstellt. Diese grundrechtliche Absicherung ergibt sich aus den einschlägigen Paragraphen des DSG 2000, wie auch aus MRK § 8 sowie einschlägiger Nebengesetze. Näheres dazu auch unter
http://www.austria.gv.at/regierung/VD/V3.htm;
http://www.kronegger.at/; http://www.ad.or.at/office/)

Rechtsgrundlagen

§ 1 des DSG 2000 bestimmt:

> "(1) Jedermann hat, insbesondere auch in Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht.
>
> ...
>
> (3) Jedermann hat, soweit ihn betreffende personenbezogenen Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, d. h. ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen
>
> 1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;
>
> 2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten."[3]

Damit, sowie durch die Bestimmungen über die Verwendung von Daten (§§ 6 bis13 DSG 2000) ist der Schutzzweck des DSG 2000 definiert und rückt den Schutz der Privatsphäre in den Mittelpunkt.

Zusätzliche Herausforderungen

Wie bereits weiter oben ausgeführt, haben sich die Rahmenbedingungen für Datenschutz durch technische Entwicklungen wesentlich verändert. Darüber hinaus kommen noch andere Entwicklungen hinzu, die eine verstärkte Bedrohung der Privatsphäre plausibel erscheinen lassen und entsprechende Abwehrstrategien des Einzelnen und der Gesellschaft erforderlich machen.

---

[3] DSG 2000, BGBl. I Nr 165/1999.

Die Art der Gefährdung dynamisiert sich. Während es im „klassischen Datenschutz“ um missbräuchliche Verwendung von Daten aus anderen Entstehungskontexten oder auch um illegale Datenübermittlungen geht, entstehen zusätzlich neue Überwachungs- und Kontrollpotentiale.

Zu analytischen Zwecken erscheint es deshalb sinnvoll, zwischen eher *statischen* und *dynamischen Datensammlungen* zu unterscheiden. Unter die statischen Datensammlungen fallen die klassischen Datenbanken. Dynamische Datensammlungen entstehen vor allem durch die neuen Kommunikationsmedien. Insbesondere durch die Digitalisierung der Festnetztelefonie, durch den Aufbau der Mobiltelefonie sowie durch die verstärkte Internetnutzung entstehen wesentliche neue Gefährdungen. In den klassischen Datenbanken konnte durch Einsichtnahme ein falsches Datum erkannt und korrigiert werden. Bei den dynamischen Datensammlungen fallen nicht nur einmal erhobene Daten an, die auch richtiggestellt werden können, vielmehr entsteht bei jeder Nutzung ein Datenstrom über Kommunikationsbeziehungen und auch über ausgetauschte Inhalte. Damit wird Verhalten kontrollierbar. Im TKG wird deshalb zwischen *Stammdaten*, *Vermittlungsdaten* und *Inhaltsdaten* (§ 87 TKG) unterschieden.[4]

Neue Qualität: dynamische Datensammlungen

Das DSG 2000 unterscheidet im § 4 nur zwischen *„Daten“ („personenbezogenen Daten“*) und *„sensiblen Daten“ („besonders schutzwürdige Daten“).* Wobei personenbezogene Daten Angaben über Betroffene sind, deren Identität bestimmt oder bestimmbar ist. Sensible Daten sind solche über rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse und philosophische Überzeugung, Gesundheit oder Sexualleben natürlicher Personen. An diese Unterscheidung knüpfen sich unterschiedliche Bestimmungen über die zulässige Verwendung der Daten. Die der rechtmäßigen Verwendung zugrundeliegenden verschiedenen „schutzwürdigen Geheimhaltungsinteressen“ werden in den §§ 8 und 9 dargestellt. Der besondere Schutz der sensiblen Daten ist ein wesentlicher Punkt der aus der DSRL direkt in das DSG 2000 eingeflossen ist. Im Alltag entstehen jedoch eine Menge Daten, die diesen strengen Kriterien nicht unterliegen und doch aussagekräftiger sind als die weitgehend „öffentlichen“ Daten wie Name und Adresse. Zur weiteren Analyse möglicher Bedrohungsszenarien durch Datenmissbrauch erschien es deshalb angebracht, weitere Kategorien einzuführen. Wir unterscheiden dementsprechend zwischen[5]: *Standard Grunddaten, erweiterten Grunddaten, Privaten Lebenslaufdaten, Daten aus dem Privatleben, Versicherungsdaten, Gesundheitsdaten, finanziellen Daten, Vermögensdaten, Kriminaldaten, Kontakten und Gewohnheiten.*

Datenkategorien

Ein weiteres Unterscheidungsmerkmal ist die Eigentümerschaft von Datensammlungen (*öffentlich* versus *privat*). Und schließlich muss in der Analyse zwischen *vermeidbaren* und weitgehend *unvermeidbaren* Datensammlungen bzw. Daten generierende Handlungen unterschieden werden. Beispiele dafür sind etwa:

- *öffentlich*
  unvermeidbar → Standesamt, Melderegister, Schulbehörde, SV, Gesundheitssystem, Finanzbehörden, ...
  (teilweise) vermeidbar → alle KriminalDBs wie EKIS (Elektronisches Kriminalpolizeiliches Informationssystem) u. a., Förderstellen,

---

4 Näheres dazu im Abschnitt über die Telekommunikation.

5 Die genauen Inhalte dieser Kategorien können der Tabelle weiter unten entnommen werden.

- *privat*

  unvermeidbar → Arbeitgeber, Bank, zumindest ein Telekom-Unternehmen, ...

  vermeidbar → Versicherungen, mehrere Telekom-Unternehmen, Internetprovider[6], KundenClubs, Medien, Vereine, Kirchen etc..

Jede(r) hinterlässt eine Vielzahl von Datenspuren

Wie diese Beispiele zeigen, geht die Bedrohung der Grundrechte von Meinungsfreiheit, Datenschutz und Privatsphäre in der sog. „Informationsgesellschaft" nicht nur vom „Netz der Netze" aus. Vielmehr hinterlassen alle BürgerInnen in unterschiedlichsten Bereichen Datenspuren und sind demgemäss zunehmend der Bedrohung durch Überwachung ausgesetzt. Immer mehr Tätigkeiten in verschiedenen Lebensbereichen werden elektronisch unterstützt oder vollständig elektronisch abgewickelt. Der Einkauf, der Behördenweg, die Arbeit, unterschiedliche Zahlungsvorgänge, die Krankenbehandlung, Spiel und Unterhaltung und nicht zuletzt das Grundbedürfnis Kommunikation. Alle Instrumente, die diese Alltagstätigkeiten erleichtern oder erst ermöglichen, können grundsätzlich auch der Überwachung dienen – von der Kundenkarte des Handels, über die ec-Karte, Kreditkarte, verschiedene Formen des e-cash (Netzgeld wie auch Kartengeld) und der SV-Chipcard bis zum Mobiltelefon und der Internetnutzung.

Je mehr Lebensbereiche betroffen sind, umso dichter werden die Datenspuren. Daraus ergeben sich folgende Fragen:

→ Werden sie auch aussagekräftiger?

→ Welche Aussagen lassen sich machen?

→ Was wissen die NutzerInnen darüber?

→ Ist ihnen die Tragweite so mancher Anwendung überhaupt bewußt?
Bsp.: Mobiltelefon, Kundenkarte ...

Zukünftige Probleme

Grundsätzliche Entscheidung zwischen Bequemlichkeit und möglichem Verlust an Privatheit

Ein Blick in die Zukunft zeigt: Bussysteme, smart-homes und „intelligente" Helferleins, ubiquitous/calm computing, persönliche Assistenten im Netz lassen eine neue Qualität der Überwachung entstehen. Sie kann umfassender, permanent und vor allem unbemerkt vor sich gehen. Dies hängt unmittelbar mit der grundsätzlichen Entscheidung zwischen Bequemlichkeit und möglichem Verlust an Privatheit zusammen. Je besser uns die Technik individuell unterstützen soll, umso mehr personenbezogene Daten werden benötigt.

Ein grundsätzliches Problem zeigt sich auch darin, dass die Systeme immer komplexer, die Vernetzung immer dichter und die Systeme entsprechend verwundbarer werden, was aus Systemsicht steigende (technische) Kontrolle erfordert.

Problem der fehlenden Wahlfreiheit ...

Zunehmend stellt sich auch das Problem der Wahlfreiheit: kann man/frau sich diesen Entwicklungen überhaupt entziehen? „Wissende" können sich schützen, was macht der Rest? Hier wird auf gesellschaftlicher Ebene die Frage des „Digital Divide" angesprochen. Informationsarme werden nicht nur von vielen Lebensbereichen bzw. Einkommensmöglichkeiten ausgeschlossen sondern möglicherweise zusätzlich stärkerer Kontrolle ausgesetzt sein.

---

[6] Wie im Abschnitt über Telekommunikation und Internet ausgeführt wird, kann in der Diversifikation der Kontakte über verschiedene Medienunternehmen auch ein gewisser Vermeidungsaspekt erblickt werden.

und

... De-Kontextualisierung

Ein weiteres Problem ist in der De-Kontextualisierung der Daten zu erblicken. Durch das Auseinanderfallen von Entstehungs- und Verwertungszusammenhang, durch die Scheinobjektivität erhobener Daten entstehen „falsche Bilder". Dies macht die Einschränkung der Übermittlung der Daten zu einem wesentlichen Angelpunkt von Datenschutzbestimmungen. Gerade durch die weltweite Vernetzung und die Übermittlung „auf Knopfdruck" ist es notwendig nicht nur die einzelnen Datensammlungen im Auge zu behalten, sondern eine notwendige Systemsicht walten zu lassen. Probleme machen vor allem die Vernetzung unterschiedlicher Datenbestände, die jede für sich unproblematisch scheinen.

Die wirtschaftliche Vernetzung schafft ähnliche Probleme wie die technische

Die technische Vernetzung ist jedoch nur eine Seite des Problems. Zumindest ebenso problematisch sind wirtschaftliche Verflechtungen und zunehmende Integration über Branchengrenzen hinweg. Als Beispiel dafür seien die Bestrebungen von BILLA und Bank Austria zu nennen, die auf der BILLA-Card auch Zahlungsverkehrs- und Sparfunktionen anbieten. Noch komplexer werden Modelle, die das Handy als Zahlungsmittel in den Mittelpunkt ihrer Visionen[7] rücken. Bei derartigen Systemen, in die dann beim Bezahlungsvorgang nicht mehr nur KonsumentIn, Bank und Händler, sondern zusätzlich auch noch die Mobilfunkbetreiber involviert sein werden, ist auf sichere, den Datenschutz berücksichtigende Systemgestaltung besonderes Augenmerk zu legen.

[7] Von Visionen ist hier deshalb dir Rede, da die derzeit angebotenen Systeme (z. B. http://www.paybox.de) noch Pilotversuchscharakter haben und von einer flächendeckenden Verfügbarkeit noch weit entfernt sind.

3 Empirie: Wieviel wird wo gespeichert?

Eine der wesentlichen Aufgaben in dieser Arbeitsphase war es, abzuschätzen wie groß das Datenschutzproblem tatsächlich ist, in wie vielen Datenbanken sich ein durchschnittlicher Österreicher wiederfindet und wie sich das im Zeitablauf verändert. Dies kann jedoch aus mehreren Gründen nicht genau festgestellt werden. Einerseits ist es unmöglich, eine(n) „DurchschnittsösterreicherIn" zu kreieren, andererseits wäre bei der Vielzahl von DV-Anwendungen der Erhebungsaufwand auch zu groß. Aus diesem Grund muss versucht werden, realistische Annahmen zu treffen und aufgrund publizierter Zahlen zu einer Abschätzung zu kommen.

320.000 registrierte Datenverarbeitungen

Erste Anlaufstellen dazu sind das Datenverarbeitungsregister und die publizierten Datenschutzberichte. Der aktuelle Datenschutzbericht 1997 bezieht sich auf den Zeitraum 1. Juli 1995 bis 30. Juni 1997 und ist unter http://www.austria.gv.at/regierung/VD/DS97.PDF im Internet abrufbar. Etwas aktuellere Zahlen gibt es im „Tätigkeitsbericht des DVR 1998" publiziert im „Tätigkeitsbericht des Statistischen Zentralamtes über das Jahr 1998". Per 31. Dezember 1998 waren demnach 320.109 Datenverarbeitungen beim DVR registriert. Davon entfielen 81.161 auf den öffentlichen und 238.948 auf den privaten Bereich. Diese rund dreihundertzwanzigtausend Verarbeitungen wurden von 88.216 Rechtsträgern (7.057 öffentliche und 81.159 private) durchgeführt. Die Verteilung der registrierten Datenverarbeitungen je Rechtsträger zeigt folgendes Bild: 29 % aller Rechtsträger legten dem DVR nur eine Datenverarbeitung zur Registrierung vor, 27 % aller Rechtsträger zwei Datenverarbeitungen, 34 % aller Rechtsträger drei bis fünf Datenverarbeitungen, 8 % aller Rechtsträger sechs bis zehn Datenverarbeitungen und 2 % aller Rechtsträger elf und mehr Datenverarbeitungen. Elf Auftraggeber scheinen bereits mit mehr als 100 einsichtsfähigen Datenverarbeitungen im DVR auf.

Jede(r) KonsumentIn ist in mehreren Hundert Datensammlungen ...

... das Bewusstsein darüber ist jedoch sehr gering

Wenn man nun einer Berechnung der ARGE Daten (Zeger et al. 1998, S 42) folgt und als Untergrenze 10.000 Betroffene je Datenverarbeitung annimmt, so kommt man auf etwa 3,2 Mrd personenbezogene Datensätze in Österreich. Bezogen auf die Gesamtbevölkerung von etwa 8 Mio ergibt dies ca. 400 Datenverarbeitungen für jede(n) ÖsterreicherIn. Eine Untersuchung des Niederländischen Verbraucherverbandes kam im Februar 1998 auf durchschnittlich 900 Dossiers je niederländischem Konsumenten. Interessant erscheint in diesem Zusammenhang auch, dass 66 % der befragten KonsumentInnen glaubten, in weniger als 25 Datenbeständen vertreten zu sein und nur 4 % glaubten, dass es mehr als 100 seien (vgl. Borking 1998, S 286). Gerald Reischl kommt in seinem Buch „Im Visier der Datenjäger" für sich selbst auf 87 Datensammlungen, sodass wohl von einer Untergrenze von etwa 100 Datensammlungen für jede KonsumentIn ausgegangen werden kann.

Individuelles Verhalten wichtig

Diese statistischen Werte haben für den/die Einzelne(n) jedoch nur bedingt Erklärungscharakter, da die Zahl der Datensammlungen, in denen Einträge von einem selbst gespeichert sind, sehr stark auch vom individuellen Verhalten mit beeinflusst werden und die Zahl somit nach oben wohl beliebig erweiterbar sein dürfte. Je nachdem ob man gerne bei Gewinnspielen mitmacht, viele Kundenkarten verschiedenster Handelshäuser hat bzw. eine Vielzahl von Versicherungen und Bankdienstleistungen in Anspruch nimmt, wird sich die Zahl der Datensammlungen vergrößern bzw. bei entsprechend entgegengesetztem Verhalten gering halten. Daraus ergibt sich direkt eine individuelle Verantwortung jeder einzelnen KonsumentIn für ihren/seinen Umgang mit personenbezogenen Daten. In gesättigten Märkten mit starker Konkurrenz werden zusätzliche Informationen über potentielle KundInnen zu einem nicht zu un-

terschätzenden Wettbewerbsfaktor. Die Unternehmen werden also neue Wege suchen, an derartige Zusatzinformationen zu kommen. Dies bedeutet für die KonsumentInnen oft eine Entscheidung zwischen einem Mehr an Bequemlichkeit oder anderen mehr oder weniger großen Vorteilen gegenüber einem Weniger an Privatheit.

Eine weitere Einschränkung zu dieser Abschätzung ergibt sich aus dem Umstand, dass nur 81.000 private Rechtsträger beim DVR registriert sind. Aufgrund der Miniaturisierung in der EDV, dem gleichzeitigen Preisverfall muss man davon ausgehen, dass fast jedes Unternehmen in Österreich mittlerweile EDV einsetzt. Auch wenn es die eine oder andere Anwendung geben sollte, die keine personenbezogenen Daten verarbeitet, so ist zwischen den registrierten 81.000 privaten Rechtsträgern im DVR und den 374.718 Kammermitgliedern (lt. WKÖ: http://wko.at/statistik/jahrbuch/km1.htm) im Jahre 1999 doch eine gehörige Differenz festzustellen, was die Vermutung nährt, dass die Zahl der Datenverarbeitungen in Österreich wesentlich größer sein dürfte, als in den offiziellen Zahlen dargestellt. Dieses Mißverhältnis von veröffentlichten Zahlen und der Realität wird sich in der Statistik für das Jahr 2000 weiter verschärfen, da ab 07/2000 nach der sogenannten Standard- und Musterverordnung (StMV, BGBl. II Nr. 201/2000, ftp://ftp.adis.at/privacy/dsg2000/stmv.pdf) viele Standardverarbeitungen nicht mehr registrierpflichtig sind.

Ein weiterer Weg, um zu empirischen Daten über die Größe des Problems zu kommen, war eine Internetrecherche zum Thema[8]. Diese wurde einerseits in allgemeinen Suchmaschinen, andererseits aber auch in den elektronischen Archiven österreichischer Tageszeitungen durchgeführt. Zusammen mit Experteninterviews in den Bereichen Datenschutz, Konsumentenschutz und Technik ergab sich eine „Landschaft der Problemfelder". Besonders interessant erwiesen sich folgende Bereiche:

Landschaft der Problemfelder

- *Öffentliche Institutionen* (Kommunale Verwaltung, Meldewesen, Grundbuch, Polizei/Gericht, Bundesheer/Zivildienst, Finanzbehörden, Bildungssystem, Statistik Österreich)
- *Arbeitgeber*
- *Telekommunikation* (Festnetz, alternative Festnetzbetreiber, Mobiltelefonie, Internetprovider, Gesamtanbieter, ...)
- *Finanzdienstleister* (Gehaltskonto, Pensionskonto, Studentenkonto, Bankomat/Maestro, Kredite, Bausparkassen, div. Fondsverwaltungen, Kreditkartenanbieter, Abrechnungszentralen (APSS – Austria Payment System Service), Kreditvermittler, Finanzberater, ...)
- *Gesundheitswesen* (SV, Ärzte, private Krankenversicherungen, Spitalserhalter/Länder und Gemeinden sowie private, Apotheken ...)
- *Versicherungen* (KfZ, Gebäude- und Haushalt, Lebensversicherungen, Makler, ...)
- *Händler und Dienstleister verschiedener Branchen* (Kundenkarten, Konsumprofile, ...)
- *Kirchen* und *Vereine*.

Die im Text und in der Tabelle wiedergegebenen Informationen entsprechen dem publizierten Wissensstand. In der zur Verfügung stehenden Zeit war es aus praktischen Gründen nicht immer möglich und auch nicht geplant, alle Daten zu verifizieren. So sind geplante Interviewtermine mit Telekombetreibern (noch) nicht zu Stande gekommen bzw. in einem Fall wurde eine Absage erteilt.

---

[8] Die Ergebnisse sind im Anhang dargestellt.

Kategorisierung der Daten

Die Tabelle gibt einen Überblick darüber, welche Daten bei welchen Einrichtungen gespeichert werden oder werden können. In der Tabelle werden die einzelnen Daten zu den Kategorien „Standard Grunddaten“, „Erweiterte Grunddaten“, „Private Lebenslaufdaten“, „Privatleben“, „Versicherung“, „Körper“, „Finanzielle Daten“, „Vermögen“, „Kriminalität“, „Kontakte“ und „Gewohnheiten“ zusammengefasst. Diese Daten werden jeweils mit den Einrichtungen gekreuzt. Dabei steht an jedem Kreuzungspunkt ein „**X**“ für Daten, die mit sehr hoher Wahrscheinlichkeit registriert oder gespeichert werden, ein „**O**“ für Daten, die möglicherweise gespeichert werden und ein leeres Feld für Daten, die eher nicht gespeichert werden.

Dennoch muss darauf hingewiesen werden, dass beispielsweise ein leeres Feld nicht automatisch bedeutet, dass diese Daten unter keinen Umständen aufgenommen oder von der jeweiligen Einrichtung recherchiert werden. Die Angaben stehen nur für solche Daten, die offiziell gesammelt und gespeichert werden. Was die Einrichtungen teilweise noch zusätzlich über einzelne Personen wissen, ist in der Regel nicht offiziell bekannt oder für die Einzelne/den Einzelnen nicht erkennbar. Schwierig ist es z. B. bei der Kategorien „Polizei/Gericht“. Wird eine Person rechtlich verfolgt, so werden mehr Daten über sie aufgenommen bzw. recherchiert als wenn die Person nur ordnungsgemäß gemeldet ist. Ziel der Tabelle ist es nicht, 100 %ig korrekte Angaben zu haben, sondern die Schwerpunkte bei der Aufnahme von Daten zu zeigen.

In der Tabelle sind die Einrichtungen in öffentliche und private unterteilt. „Statistik Österreich“ ist zwar mittlerweile ausgegliedert, ist aber dennoch als öffentliche Institution anzusehen. Auffallend in dieser Tabelle ist, dass bei den öffentlichen Unternehmen mehr Daten gespeichert sind als bei den privaten. Ausnahmen sind hier in erster Linie der Arbeitgeber, der allein schon durch die Bewerbung an viele persönliche Daten gelangt und auch die Telekommunikationsunternehmen, die sehr private Dinge wie finanzielle Daten, Kontakte und Gewohnheiten wie z. B. benutzte Internetseiten registrieren können.

Aus der Tabelle ist außerdem ersichtlich, dass die sogenannten „Standard Grunddaten“ von allen Einrichtungen gespeichert werden und dass die gespeicherten Daten mit zunehmender Privatsphäre (im unteren Teil der Tabellen) immer seltener gespeichert werden. Mit zunehmender Digitalisierung bzw. immer stärkerem Einsatz von Informations- und Kommunikationsmedien wird es aber für alle Einrichtungen bzw. bei sämtlichen Tätigkeiten einfacher sein, auch private und sehr persönliche Daten über Personen zu speichern.

	Institution/Organisation	Öffentlich										Privat							
	Daten	Meldewesen	Grundbuch	Kommunale Verwaltung	Polizei/Gericht	Bundesheer/ Zivildienst	Finanzbehörden	Sozialversicherung	Gesundheitssystem	Bildungssystem	Statistik Österreich (Volksz.)	Arbeitgeber	Finanzdienstleister	Telekommunikation	Kirchen	Private Versicherungen	Rundfunk. Medien	Vereine	Div. Branchen Kundenkarten
Standard Grunddaten	Name (Vor- und Nachname)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Geschlecht	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Titel	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Postadresse	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Erweiterte Grunddaten	Telefonnummer (Festnetz-Mobil, frei verfügbar)			0	0	0	0	0	0	X		X	0	X	0	0	0	0	0
	Telefonnummer (Festnetz geheim, Wertkartenhandy)									0				X					
	Faxnummer			0	0	0	0	0	0		0	0	0	X		0	0	0	0
	Email-Adresse				0							0	0	X		0	0	0	0
Private Lebenslaufdaten	Geburtsdatum/Alter	X	X	X	X	X	X	X	X	X	X	X	0	X	X	X	0	0	0
	Geburtsort	X			0	X				X	X	0			X				
	Familienstand			X	0	X	X	X	X	X	X	X	0		0	X	0	0	0
	Staatsangehörigkeit	X	0	X	X	X	X	X	X	X	X	X	0	0	0	X	0	0	0
	Beruf				0	X	X	X	0	X	X	X	0	0	0	X	0	0	0
	Arbeitsstätte				0	0	X	X	X	X	X	X	X	X		X			
	Anzahl Kinder			X		0	X	X	X	X	X	X	0		0	X			0
	Bildungsweg					X	X	X	X	X						0	0		0
	Konfession	X				X						0			X				
Privatleben	Daten über Familienangehörige (Name, Adresse, Beruf etc.)			X		X	X	X	X	X	X	0	X	0	X	X			0
	Wohnungsgröße			0							X		0			X			
	Mitbewohner/innen/zum Haushalt gehörende Personen						0	0			X								
	Nachbarn										X								
Versicherung	Sozialversicherungsnummer				0	X	X	X	X			X				0			
	Versicherungsdaten (Lebens-, Kranken-, Autoversicherung etc.)						X	X	X				0			X			

	Institution/Organisation	Öffentlich										Privat							
	Daten	Meldewesen	Grundbuch	Kommunale Verwaltung	Polizei/Gericht	Bundesheer/ Zivildienst	Finanzbehörden	Sozialversicherung	Gesundheitssystem	Bildungssystem	Statistik Österreich (Volksz.)	Arbeitgeber	Finanzdienstleister	Telekommunikation	Kirchen	Private Versicherungen	Rundfunk. Medien	Vereine	Div. Branchen Kundenkarten
Körper	Gesundheits-/Krankheitsdaten				0	X	0	X	X				0			0			
	DNA-Daten				0				0										
Finanzielle Daten	Bankdaten (Konto-, Kreditkartennummer; Kontostand)					X	X	0				X	X	X	0	X	X	0	0
	Einkommen						X	X				X	X		0	0			0
	Ausgaben												X						0
	Bonität						X					X	X	X	0				
	Gezahlte Steuern						X					X	0						
Vermögen	Immobilien		X	X			X						X						
	Sonst. nicht-monetäres Vermögen						0						0			X			
Kriminalität	Kriminaldaten/polizeilich gespeicherte Daten				X	0						0							
Kontakte	Geschäftliche Kontakte (Zeitpunkt, Häufigkeit, Dauer, Medium, Ort)											X		X					
	Private Kontakte (Zeitpunkt, Häufigkeit, Dauer, Medium, Ort)													X					0
Gewohnheiten	Bewegungsdaten				0							0	X						
	Freizeitverhalten													0				0	0
	Einkaufsverhalten												X	0					X
	Benutze Internetseiten/persönliche Vorlieben													X			0	0	0
	Politisches Einstellungen und Interessen				0	0											0	0	0

X = *Daten werden mit sehr hoher Wahrscheinlichkeit registriert bzw. gespeichert*

0 = *Daten werden möglicherweise/mit geringer Wahrscheinlichkeit registriert oder gespeichert*

= *Daten werden mit hoher Sicherheit nicht gespeichert*

Verbesserte Daten-Analyseprogramme ...

Wie aus der Tabelle zu ersehen, ergibt sich eine stattliche Zahl von Datensammlungen für jede einzelne BürgerIn. Wichtig ist aber darauf hinzuweisen, dass es nicht die Zahl der Datensammlungen an sich ist, die den Datenschutz auszuhöhlen droht. Vielmehr liegt eine zunehmende Gefahr in den wesentlich verbesserten Daten-Analyseprogrammen, die es ermöglichen, Aussagen über zukünftige Entwicklungen zu machen. So lassen sich durch Programme wie sie

und

im Rahmen des Customer Relationship Management (CRM) eingesetzt werden, die unterschiedlichen Kundenprofile einer Wetterkarte gleich darstellen und auch mit relativ hoher Sicherheit Vorhersagen treffen, ob ein Kunde dem Unternehmen treu bleiben wird, oder für bestimmte andere Waren offen ist (vgl. Lechner 2000, B1) D. h. mit anderen Worten: Aus Eigenschaften und bisherigem Verhalten kann mit relativ hoher Genauigkeit auf zukünftiges Verhalten geschlossen werden.

... unbewusste Datenweitergabe

Ein großes Problem ist auch die fehlende Transparenz. Es ist für die KonsumentInnen ja nicht nachvollziehbar, wem sie ihre Daten tatsächlich überlassen. Wer in einer Zeitung ein Horoskop bestellt, muss natürlich sein Geburtsdatum mitliefern, wer bei bestimmten Telefondienstleistern (z. B. Sex-Hotline) oder auch in verschiedenen Call-Centern anruft gibt, so er nicht aktiv dagegen etwas unternommen hat, in der Regel seine Telefonnummer preis[9] und liefert „frei Haus“ auch noch einige Zusatzmerkmale (Kunde bei, wohnhaft in, Interesse für etc.) Wer bei mehreren Unternehmen Einziehungsaufträge laufen hat, übermittelt diesen Unternehmen seine Kontonummer und damit auch die Bank bei er/sie das Konto führt. Ob alle diese Unternehmen die Daten selbst verarbeiten oder sich dazu verschiedener Dienstleister bedienen, kann die KonsumentIn nicht abschätzen. Zudem ist auch in der Branche der Adressverlage und Datenverarbeiter ein Konzentrationsprozess zu beobachten. Auch wenn alle diese Daten aus unterschiedlichen Datensammlungen getrennt geführt werden, können so durchaus Datenpools entstehen, die ein dichtes Netz über Einzelpersonen oder Zielgruppen legen lassen.

Wenn eines der großen Unternehmen im Bereich der Adressverlage in Österreich damit wirbt, über 5 Mio Adressen mit einer Datentiefe von etwa 50 Merkmalen zu führen, so ist zu fragen: woher kommen die Zusatzinformationen, wer verbindet sie und wozu werden sie verwendet?

Viele dieser Anwendungen bewegen sich durchaus legal „am Rande des DSG“. Sobald nicht mehr personenbezogene Daten verwendet werden, greift das DSG nicht mehr. Und für einige Anwendungsgebiete können auch Unternehmen mit einer gewissen Ungenauigkeit leben. Im Bereich der statistischen Datenanalyse ist aber eine wesentliche Verbesserung der Analysemethoden festzustellen, sodass die Eingrenzungen immer genauer werden und in einigen Fällen sicher Rückschlüsse auf Einzelpersonen möglich sind.

[9] Siehe den Absatz zur Rufnummerunterdrückung auf Seite 21.

4 EXKURS: Telekommunikation und Internet

4.1 Telekommunikation

Neue Situation durch Digitalisierung, Mobiltelefonie und Internet

Als besonders bemerkenswerte Entwicklung ist jene im Bereich Telekommunikation/Mobilkommunikation anzusehen. Hier haben im letzten Jahrzehnt gravierende Veränderungen stattgefunden, die natürlich auch zu entsprechenden Konsequenzen für die Privatsphäre führen. Die vier Kernentwicklungen sind die De-Regulierung des Marktes, die Digitalisierung der Telekommunikationsnetze, der rasante Aufstieg der Mobiltelephonie und die ebenso beeindruckende Verbreitung des Internets, wobei von den drei letztgenannten Entwicklungen unmittelbare Beeinträchtigungen auf die Privatsphäre ausgehen.

Rasches Wachstum bei Mobilnetzen und dem Internet

Die Digitalisierung des österreichischen Telekommunikationsnetzes, die zu Beginn der 90er Jahre noch weniger als 10 % betrug, wurde im Jahr 1999 abgeschlossen; die Mobiltelephondichte ist von weniger als einem Prozent (Autotelefon C-Netz und das gerade in Betrieb genommene D-Netz) im Jahr 1990 auf etwa 57 % im Herbst 2000 gestiegen; und das Internet ist von einem auf akademische Anwendungen beschränkten Instrument zu einem von mehr als einem Drittel der ÖsterreicherInnen genutztem Dienst geworden, wobei wir uns in diesem Bereich noch mitten in einer Phase starken Wachstums befinden (die Zahl der Personen in Österreich die grundsätzlich Zugang haben, ist vom 2. Quartal 1999 bis zum 2. Quartal 2000 von 31 % auf 44 % gestiegen).

Stamm-, Vermittlungs- und Inhaltsdaten

Welche konkrete Konsequenzen lassen sich nun aus diesen kurz skizzierten technischen Innovationen und Markttrends identifizieren. Dabei ist es hilfreich, zunächst zwischen den einzelnen Kategorien von Daten zu differenzieren. Ein Ausgangspunkt ist die Unterscheidung von „Stammdaten“[10], „Vermittlungsdaten“[11] und „Inhaltsdaten“[12] gemäß der Definition des österreichischen Telekommunikationsgesetzes („TKG“).

Relativ wenig Veränderungen sind im Bereich der Stammdaten zu verzeichnen. Die Ausnahme bildet dabei die Bonitätsprüfung. Durch den Online-Zugang zu vom „Kreditschutzverband von 1870“ (KSV) geführten Datenbanken wie der Warenkreditevidenz (WKE) ist diese wesentlich schneller durchzuführen und durch die heutzutage übliche direkte Anmeldung von Mobiltelefonen im Fachhandel ist auch der Kreis jener Personen, die Abfragen initiieren können, erheblich gestiegen. Auch umgekehrt dürfte ein Einfluss gegeben sein: die vielfach nicht sehr transparente Tarifgestaltung im Zusammenspiel mit dem enormen Wachstum im Mobiltelefonmarkt hat, wie des öfteren in den

---

[10] TKG § 87. (3) 4. „Stammdaten“ alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter von Telekommunikationsdiensten oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind; dies sind: a) Familienname und Vorname, b) akademischer Grad, c) Adresse, d) Teilnehmernummer, e) Bonität;

[11] TKG § 87. (3) 5. „Vermittlungsdaten“ alle personenbezogenen Daten, die sich auf Teilnehmer und Benutzer beziehen und für den Aufbau einer Verbindung oder für die Verrechnung von Entgelten erforderlich sind; dies sind: a) aktive und passive Teilnehmernummern, b) Anschrift des Teilnehmers, c) Art des Endgerätes, d) Gebührencode, e) Gesamtzahl der für den Abrechnungszeitraum zu berechnenden Einheiten, f) Art, Datum, Zeitpunkt und Dauer der Verbindung, g) übermittelte Datenmenge, h) andere Zahlungsinformationen wie Vorauszahlung, Ratenzahlung, Sperren des Anschlusses oder Mahnungen;

[12] TKG § 87. (3) 6. „Inhaltsdaten“ die Inhalte übertragener Nachrichten.

Medien berichtet wurde, dazu geführt, dass Kunden aufgrund der hohen Telekomrechnungen in Zahlungsverzug geraten sind, und damit auch in Gläubigerschutzdatenbanken Aufnahme gefunden haben.

Vermittlungsdaten: ein Nebenprodukt der Digitalisierung

Ein gänzlich anderes Bild zeichnet sich bei den Vermittlungsdaten ab. Zu Zeiten analoger, elektromechanischer Vermittlungstechnologien war deren Generierung ein zeit- und arbeitsaufwendiger Vorgang. Man braucht sich nur an eine beliebte Szene in älteren Kriminalfilmen erinnern, in denen meist erfolglos versucht wurde, den Anrufer so lange in der Leitung zu behalten, bis die Techniker im Hintergrund ein Zeichen gaben, dass der Übeltäter lokalisiert sei. Als Element zur Spannungssteigerung finden sich solche Szenen auch in neueren Filmen wieder, sie entsprechen aber nicht mehr den realen Gegebenheiten. In modernen, digitalen Telekommunikationsnetzen werden diese Daten automatisch generiert und gespeichert, dies gilt auch für versuchte Anrufe, bei denen eine Verbindung gar nicht zustande kommt. Lt. TKG § 93 dürfen Vermittlungsdaten grundsätzlich nicht gespeichert werden, allerdings gibt es eine Reihe von Ausnahmen. Außer in gesetzlich besonders geregelten Fällen, die eine Datenauswertung erlauben, bleiben die Vermittlungsdaten jedenfalls bis zum Ablauf der Einspruchsfrist gegen ausgestellte Rechnungen gespeichert, mit Zustimmung des Teilnehmers/der Teilnehmerin, die meist in den AGB enthalten ist,[13] dürfen Daten auch für die Vermarktung eigener Dienste ausgewertet werden. Die Telekom Austria als Beispiel für den größten Telekomanbieter gibt in ihren AGB an, Stammdaten spätestens sieben Jahre nach Beendigung des Geschäftsverhältnisses, Vermittlungsdaten binnen eines halben Jahres nach Begleichung der Rechnung zu löschen.

Auch konzerninterne Verwertung von Vermittlungsdaten problematisch

Die freie konzerninterne Verwertung für Marketing- und Werbezwecke ist in zweifacher Hinsicht problematisch. Einerseits fallen in einem Konzern, der neben Festnetz- und Mobilkommunikationsdiensten u. a. auch als Internet-Provider fungiert, sehr viele Daten über einzelne TeilnehmerInnen an, die zu sehr umfassenden Kommunikationsprofilen zusammengefasst werden können. Der zweite Einwand ist von genereller Natur und betrifft die Art der Zustimmung der TeilnehmerIn: Durch die in den letzten Jahren stark gestiegenen Möglichkeiten, mittels Datamining umfassende Datensätze nach unterschiedlichsten Kriterien auszuwerten, wird der Mehrzahl der Kunden gar nicht bewusst sein, welche Konsequenzen eine möglicherweise vor vielen Jahren im „Kleingedruckten“ gegebene Zustimmung haben kann. Als ehemaliger Monopolbetreiber ist die Telekom Austria nicht nur aufgrund ihres Marktanteils in einer besonders kritischen und verantwortungsvollen Position, sondern auch wegen des Umstandes, dass auch der überwiegende Teil des Telekommunikationsverkehrs der alternativen Betreiber zumindest zu einem Teil auf der Infrastruktur der Telekom Austria abgewickelt wird, d. h. auch deren Vermittlungsdaten prinzipiell auswertbar sind.

Inhaltsdaten dürfen nur in Ausnahmefällen gespeichert werden

Inhaltsdaten dürfen nicht gespeichert werden, sofern deren Speicherung nicht einen wesentlichen Bestandteil des Telekommunikationsdienstes darstellt, wie z. B. bei Sprachmailboxdiensten. Im Normalfall werden diese Daten gelöscht, sobald der Dienst erbracht wurde, z. B. eingegangene Nachrichten für eine vereinbarte Zeitspanne gespeichert wurden; eine Reihe von Ausnahmen bestehen für Internet-basierte Dienste. Aus rein kommerziellen Interessen scheint aber eine Speicherung und Auswertung von Inhaltsdaten bei Sprachdiensten kaum lohnend zu sein. Aber natürlich müssen sich KonsumentInnen und BürgerInnen bewusst sein, dass im Zuge polizeilicher oder nachrichtendienstlicher Aktivitäten auch auf Inhalte von Telekommunikationsbeziehungen zugegriffen werden kann und wird. Vergleiche dazu auch die Diskussion um das

[13] Dieser Hinweis findet sich auch in den AGB der Telekom Austria. Auffallend ist, dass nur eine Zustimmung, und keine ausdrückliche Zustimmung gefordert ist.

weltweite Abhörsystem ECHELON (z. B. ITA-News 04/2000 oder unter http://www.heise.de/tp/deutsch/html/such.html?T=echelon oder mit stärkerem Österreichbezug http://www.quintessenz.at/).

Zusammenfassend kann für den Festnetzbereich der/die durchschnittliche ÖsterreicherIn davon ausgehen, dass etwas über ein halbes Jahr zurückliegende Vermittlungsdaten (6 Monate plus Zeitspanne zwischen Nutzung und Bezahlung der Rechnung) gespeichert bleiben. Natürlich ist nicht immer eine eindeutige Zuordnung zwischen Telefonanschluß und einzelnen Personen möglich, ebenso ist zu beachten, dass für die Nutzung von Telekommunikationseinrichtungen, welche durch den Arbeitgeber bereitgestellt werden, abweichende Regelungen möglich sind.

Problemfeld Mobilkommunikation:

Eine wesentlich problematischere Situation ist im Bereich der Mobilkommunikation gegeben. Zusätzlich zu all den oben genannten Vermittlungsdaten fallen hier auch Informationen über den jeweiligen Aufenthalt des Teilnehmers/der Teilnehmerin an. Der Standort wird, sobald das Gerät eingeschaltet ist, ständig erfasst, unabhängig ob tatsächlich Gespräche geführt werden oder nicht. Diese Erfassung ist eine technische Notwendigkeit, um Anrufe an den mobilen Teilnehmer vermitteln zu können, und nicht primär eine Überwachungsmaßnahme. Dennoch stellt allein die Möglichkeit, dass Bewegungsdaten aufgezeichnet, gespeichert und ausgewertet werden können, eine sehr schwerwiegende Veränderung im Überwachungspotential einzelner Menschen dar. In der Vergangenheit wurde diese Möglichkeit von den Mobilnetzbetreibern dementsprechend wenig diskutiert bzw. heruntergespielt.[14] Mit dem Beginn des Angebots und der Vermarktung von „location based services“ mittels WAP (Wireless Application Protocol) hat sich das Bild vollkommen gewandelt. Die Nennung der nächsten offenen Apotheke oder eine Liste mit nahegelegenen 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.

Bewegungsprofile ...

und

... lückenlose Informationen über Aufenthaltsorte generierbar

Mit einem ständig mit sich geführten und eingeschalteten „Handy“ hinterlässt man lückenlose Informationen darüber, wann man sich wo aufgehalten hat. Dabei lässt sich der ungefähre Aufenthaltsort anhand der Funkzelle, in der man eingeloggt war, bestimmen. Die Größe dieser Funkzellen hängen u. a. von der verwendeten Technologie bzw. Frequenz und von der Teilnehmerdichte ab; so sind die Zellen bei GSM 1800 und in städtischen Kernzonen kleiner als im D-Netz oder in ländlichen Gebieten. Im Durchschnitt ist von einer Genauigkeit von einigen hundert Metern auszugehen. Bei Bedarf kann aber die Genauigkeit der Lokalisierung wesentlich erhöht werden, indem die Zeitdifferenzen, die zwischen dem Eintreffen von Funksignalen bei den umliegenden Basisstationen auftreten, ausgewertet werden. Für viele der geplanten Dienste, wie z. B. verirrten Touristen in der fremden Großstadt den Weg zu weisen, wird dies auch unumgänglich sein.

Zusätzliche Gefahren durch multifunktionelle Nutzung ...

Die Möglichkeit, zusätzlich zu Kommunikations- auch Bewegungsprofile zu registrieren, stellt für sich alleine schon eine völlig neue Qualität von Datensammlungen und Überwachungspotentialen dar, die in ihren Konsequenzen

[14] Siehe z. B. die Anmerkungen (Abschnitt 4.3) zum Thema „LOKALE ORTUNG“ im Bericht von Kollmann 1999

noch gar nicht umfassend erforscht worden ist. Die Mobilkommunikation birgt aber noch darüber hinaus besondere Risiken in sich. Zum einen wächst die Zahl der möglichen Anwendungen von mobilen Terminals ständig. Neben der normalen Sprachkommunikation und der Nutzung von SMS stehen vielfältige neue Dienste zur Verfügung bzw. kurz vor ihrer Einführung. Mit dem Handy können Waren und Dienstleistungen bestellt und bezahlt, Internetdienste genutzt oder Unterhaltungsangebote konsumiert werden. Die Vielzahl von Nutzungen, die an eine digitale, im SIM gespeicherte Identität geknüpft werden können, erlaubt auf einfache Weise ein sehr umfassendes Bild vom Benutzer/von der Benutzerin zu erhalten, während ohne ein solches Universalinstrument ein so breites Profil, wenn überhaupt, nur bei der Verknüpfung von vielen, einzelnen Datenbanken generiert werden konnte. Dieses Argument mag zwar mit den Fortschritten bei den Methoden des Datamining etwas an Relevanz verlieren, da auch aus sehr heterogenen Datenquellen umfassende Informationen geschaffen werden können. Dennoch unterscheidet sich die Mobilkommunikation sehr gravierend in einem zweiten Punkt.

...und direkte Zuordnung

In der Regel ist sie viel stärker an eine bestimmte Person geknüpft als andere Kommunikationsgeräte. Private Festnetztelefone können von allen Personen im betroffenen Haushalt genutzt werden, auch lässt sich die Internetnutzung über einen PC meist nicht unmittelbar an eine bestimmte Person knüpfen, während die bei Mobilkommunikation anfallenden Daten sich mit großer Wahrscheinlichkeit dem jeweiligen Besitzer zugeordnet werden können. Ausgenommen davon sind Wertkartenhandys bzw. Prepaid-Handys; sofern diese nicht auf Kreditkartenabbuchung umgestellt werden. Mit Wertkartenhandys ist im Normalfall eine anonyme Nutzung gewährleistet, allerdings fallen dabei wesentlich höhere Gesprächsgebühren als bei angemeldeten Mobiltelefonteilnehmern an, da auch die Einrichtungs- und Grundgebühren über die Gesprächstarife eingenommen werden müssen.

SMS: Speicherung und Filterung von Inhaltsdaten

Dieselben Beziehungen der persönlichen Zuordenbarkeit gelten auch für SMS-Nachrichten (Short Message Services), sofern sie mit einem identifizierten Handy versendet werden. SMS-Dienste weisen aber noch zusätzliche Merkmale auf. Ersten müssen diese Textnachrichten zumindest so lange gespeichert werden, bis sie dem Empfänger zugestellt werden können. Zweitens, und hier liegt ein gravierender Unterschied, laufen diese Nachrichten vielfach über Inhaltsfilter, welche z. B. Nachrichten, die obszöne Wörter beinhalten, kennzeichnen und nicht zustellen. Es würde den Rahmen dieses Beitrags sprengen, die zweifelsohne vorhandenen gegensätzlichen Interessen, einerseits vor Belästigungen geschützt zu werden und andererseits private Kommunikation unzensuriert durchführen zu können, abzuwägen und mögliche Lösungen zu diskutieren, die weder das eine noch das andere Recht zu sehr schmälern. So bleibt an dieser Stelle festzuhalten, dass durch die Möglichkeit, eine vor allem bei jüngeren Bevölkerungsschichten weit verbreitete Kommunikationsform automatisch nach inhaltlichen Kriterien zu beurteilen, auch ein neuer und zusätzlicher Gestaltungs- und Regelungsbedarf entsteht.

CLIP und CLIR: neue Dienste der Telekom mit wenig bekannten Folgen

Der Konflikt zwischen dem Schutz vor Belästigungen einerseits und der Möglichkeit, seine Anonymität zu wahren, tritt auch bei der Rufnummeranzeige auf. Mit dem Abschluss der Digitalisierung des Festnetzes hat die Telekom Austria die bei den digitalen Mobilnetzen implementierte Übertragung der Rufnummer des Anrufers an den Angerufenen auch auf das Festnetz ausgedehnt. Die Abkürzungen CLIP (Calling Line Identification Presentation) und CLIR (Calling Line Identification Restriction) bezeichnen die standardmäßig aktivierte Übertragung der Rufnummer bzw. die Möglichkeit, diese wieder zu deaktivieren oder im Einzelfall zu unterdrücken.[15] Da die Mehrzahl der in den

[15] In Österreich muss zu diesem Zweck die Tastenkombination *31* vorgewählt werden.

Privathaushalten verwendeten Telefonapparate die Möglichkeit der Rufnummeranzeige noch nicht bieten, wird vielen Personen wohl gar nicht bewusst sein, dass bei Anrufen ihre eigene Telefonnummer mitübertragen wird. Und noch viel weniger Personen dürften wissen, dass sich mit minimalem Zusatzaufwand damit auch der dazugehörige Eintrag ins Telefonbuch generieren lässt.[16] Eine Konsequenz davon ist, dass z. B. bei jeder Anfrage an ein Unternehmen die theoretische Möglichkeit besteht, dass dabei auch ein entsprechender, an die Person geknüpfter Datenbankeintrag erfolgt und damit die Möglichkeit, ein Bild einer bestimmten Person zu gewinnen, um eine weitere Facette erweitert wird.

Nur wenige Möglichkeiten die Privatsphäre zu schützen ...

Die Unterdrückung der Rufnummernanzeige ist eine der wenigen Möglichkeiten, im Festnetz durch bewusstes Verhalten zur Wahrung der eigenen Privatsphäre beizutragen. Diese Möglichkeit sollte natürlich auch bei Mobiltelefonaten genutzt werden, wenn man anonyme Anfragen stellen möchte.[17] In Mobilnetzen würde eine Minimierung der Datengenerierung zusätzlich bedeuten, das Gerät immer auszuschalten, wenn die Möglichkeit dazu besteht. Der Spielraum hängt dabei stark von den persönlichen Umständen und Neigungen ab, etwa ob das Mobiltelefon privat oder beruflich genutzt wird, oder ob das Handy das einzige Telefon ist und man ständig erreichbar sein will. Eine weitere Option ist die Nutzung eines anonymen Wertkartentelefons. Allerdings muss man dabei eine eingeschränkte Funktionalität – wie bei Geheimnummern ist man nur für denjenigen Personenkreis erreichbar, dem man seine Nummer aktiv mitteilt – und wesentlich höhere Tarife für aktive Gespräche in Kauf nehmen.

... ohne Nachteile in Kauf nehmen zu müssen

4.2 Internet

Mehr Möglichkeiten der Datengewinnung bei der Internetnutzung ...

Zwischen traditionellen Telekommunikationsdiensten und dem Internet bestehen natürlich vielfältige Beziehungen; so erfolgt der Zugang zum Internet derzeit noch vorwiegend über das Telefonnetz und umgekehrt kann man über das Internet telefonieren oder SMS versenden. Dennoch ergeben sich allein aus der Vielzahl von Anwendungen, die das Internet bietet, ebenso vielfältige Möglichkeiten, Daten zu sammeln und zu detaillierten Persönlichkeitsprofilen zusammenzufassen, dass eine gesonderte Diskussion angebracht ist. Ebenso ist der Gestaltungsspielraum, persönliche Daten preiszugeben oder nicht und beispielsweise auf anonyme Identitäten zurückzugreifen, im Internet wesentlich größer als bei herkömmlichen Telekommunikationsdiensten.

... aber auch mehr Möglichkeiten zu Gegenmaßnahmen

Absolute Anonymität nur schwer erreichbar

Wenngleich beim Internet etliche Möglichkeiten bestehen, durch einen bewussten Umgang mit diesem Medium die Preisgabe der Privatsphäre zu beeinflussen und zu minimieren, – die Details eines bewussten Umgangs werden jeweils in Anschluss an ein Problemfeld diskutiert und in den Schlussfolgerungen zusammengefasst –, so muss dennoch betont werden, dass eine absolute Anonymität nur in sehr eingeschränktem Maße erreichbar ist. Grundsätzlich ist jede Internetnutzung an eine IP-Adresse geknüpft. Selbst wenn diese, wie bei PrivatkundInnen von Internet-Service-Providern (ISP) derzeit noch üblich, dynamisch bei jeder Einwahl neu vergeben wird, ist über die Verknüpfung der Log-Files des ISP mit den Vermittlungsdaten des Telekommunikationsnetzbetreibers nachvollziehbar, von welchem Telefonanschluß der Zugang er-

[16] Sofern nicht eine Geheimnummer ohne Eintragung verwendet wird.

[17] Im Einzelfall kann eine Unterdrückung der Anzeige aufgehoben werden: z. B. bei Notrufnummern von Einsatzdiensten, oder um die Verursacher von Telefonterror auszuforschen.

folgt ist. In Analogie zu den Telekommunikationsnetzen bildet daher der Umgang mit Vermittlungs- und Inhaltsdaten des eigenen ISP einen ersten Ansatzpunkt zur Einschätzung der Gefährdung der Privatsphäre.

Unterschiedliche Handhabung von Datenschutz bei verschiedenen ISP

Grundsätzlich erklären die gegenwärtig 167 (116 davon als Zugangsanbieter) Mitglieder des Vereines der Internet Service Provider Austria (ISPA) in ihren Verhaltensrichtlinien[18] Vermittlungsdaten und Daten abgerufener Internet-Inhalte prinzipiell nur anonym zu speichern und diese Daten im geregelten Geschäftsverkehr nicht zu personifizieren, woraus aber auch hervorgeht, dass im Sonderfall eine Personifizierung möglich ist. Die Verhaltensrichtlinien nehmen zwar in der Unterscheidung von Stamm-, Vermittlungs- und Inhaltsdaten auf das TKG Bezug, allerdings fehlen die entsprechenden Einschränkungen bei der Dauer der Speicherung von Vermittlungsdaten bzw. des generellen Verzichts bei Inhaltsdaten. Man muss daher davon ausgehen, dass einzelne Provider die Speicherung dieser Daten unterschiedlich handhaben können, und die AGB des jeweiligen Providers herangezogen werden müssen, um konkrete Aussagen treffen zu können. Die Telekom Austria zum Beispiel verweist für Inhaltsdaten auf die Bestimmungen des TKG § 95, bei den Stamm- und Vermittlungsdaten wird keine explizite Unterscheidung bezüglich deren Handhabung in den AGB getroffen, sondern festgehalten, dass die Daten spätestens mit Beendigung des Vertragsverhältnisses gelöscht werden, sofern sie nicht noch für Verrechnungszwecke benötigt werden.[19] Andere Provider geben beispielsweise an, personenbezogene Vermittlungsdaten lt. TKG und sonstige Log-Files nach technischen Erfordernissen zu speichern, wieder andere speichern Vermittlungsdaten drei Jahre ab Rechnungsdatum. Ohne allgemeingültige Aussagen treffen zu können, muss der/die InternetnutzerIn davon ausgehen, dass sich seine/ihre Aktivitäten am Internet auch über länger zurückliegende Zeiträume rekonstruieren lassen. Er/sie kann aber für in Österreich ansässige Internetprovider im Normalfall davon ausgehen, dass diese Daten Dritten nur im Rahmen gesetzlicher Bestimmungen zugänglich gemacht werden. Eine Verpflichtung dazu ergibt sich etwa aus § 89 TKG.

Der einschränkende Zusatz „im Normalfall“ soll nicht Missbrauchsabsichten unterstellen, sondern darauf hinweisen, dass ein unberechtigter Zugriff auf diese Daten nicht hundertprozentig ausgeschlossen werden kann, ein Umstand, auf den einzelne Provider in ihren AGBs durch Einschränkungen der Haftung für daraus resultierende Sachschäden hinweisen. Diese Einschränkung ist auch insofern berechtigt, als immer wieder Fälle publik werden, in denen ein externer Zugriff auf Kundendaten möglich war, teilweise auch inklusive Kreditkartendaten oder Passwörtern, wobei des öfteren nicht Hackerattacken, sondern mangelnde Sorgfalt von Seiten der Provider dafür verantwortlich zu machen sind.

Internetnutzung lässt Rückschlüsse auf persönliche Interessen und Einstellungen zu

Die Wahrung der Privatsphäre gewinnt bei der Internetnutzung besondere Brisanz, da bereits Vermittlungsdaten allein genügen können, um ein umfassendes Bild von der Person zeichnen zu können. So können allein aus den besuchten Webseiten, die ja bestimmte Inhalte präsentieren, weitgehende Rückschlüsse auf berufliche und private Interessen, persönliche Vorlieben in unterschiedlichen Lebensbereichen oder politische Einstellungen gezogen werden.

Personifizierung durch IP-Nummer und Log-Files

Umgekehrt ist es aber nicht eine notwendige Bedingung, Zugang zu den vollständigen Vermittlungsdaten bzw. zu den Log-Files des eigenen Providers zu haben, um Persönlichkeitsprofile erstellen zu können. Praktisch jede Aktivität am Internet generiert an unterschiedlichen Orten eine Vielzahl von Daten. Viele davon werden freiwillig weitergegeben, und oft sind es sehr sensible Informationen, die man bewusst oder unbewusst preisgibt. Dennoch bilden die Log-

[18] http://www.ispa.at/Richtlinie/Richtlinie.htm

[19] http://www.telekom.at/docs/service/agb/AGBON.DOC

Files des eigenen Providers einen zentralen Ansatzpunkt von möglichen Verletzungen der Privatsphäre. Anhand der IP-Nummer erlauben sie eine nachträgliche Personifizierung der Internetnutzung, auch wenn diese anonym erfolgt ist. Und mit ihrer Hilfe lässt sich ein sehr umfassendes und vollständiges Bild des Nutzungsverhalten am Internet rekonstruieren, ein Bild, welches sich aufgrund der verteilten Struktur des Internets und des paketorientierten Datenverkehrs auch mit sehr großem Überwachungsaufwand nicht in diesem Umfang gewinnen lässt.

AGB der Internet-Provider vergleichen und ...

... eventuell mehrere ISP nutzen

Damit lassen sich bereits zwei grundsätzliche Hinweise für einen bewussten Umgang mit dem Internet ableiten. Bevor man einen Vertrag mit einem Internet-Provider abschließt, empfiehlt es sich, nicht nur die Tarife zu vergleichen, sondern auch die AGB hinsichtlich der Datenschutzbestimmungen zu überprüfen, insbesondere die Dauer der Speicherung von Vermittlungs- und Inhaltsdaten und die Weitergabe von Daten betreffend. Zweitens bietet sich als präventive Maßnahme an, die Dienste von mehr als einem ISP in Anspruch zu nehmen. Dies kann bei Nutzung der jeweils unterschiedlichen Tarife zu Kern- und Randzeiten und von freien Kontingenten auch aus Kostengründen empfehlenswert sein, sofern die individuelle Internetnutzung nicht am billigsten über einen pauschalierten Zugang realisierbar ist. Für technisch weniger versierte NutzerInnen können mehrere ISP auch einige Probleme mit sich bringen, da sich die mitgelieferte Zugangssoftware oftmals recht ungeniert Systemparameter verändert und sich jeweils selbst an die erste Stelle bei Internetanwahlen stellt.

Nutzung von Internetdiensten

Persönliche Daten als Preis für „kostenlose" Dienste und individualisierte Informationsangebote

Daten über die Nutzung des Internets fallen nicht nur bei den Zugangsprovidern, sondern auch bei den jeweiligen Anbietern von Internetdiensten wie etwa bei Suchmaschinen, E-Mail-Konten oder Informationsangeboten an. In vielen Fällen ist die Preisgabe persönlicher Daten eine Bedingung, um einen „kostenlosen" Dienst nutzen, oder an einem Gewinnspiel teilnehmen zu können. In diesen Fällen ist zumindest eine Entscheidung möglich, inwieweit Daten preisgegeben werden und welche Identität dabei gewählt wird. Die Aufgabe von Privatheit stellt in diesem Sinn den Preis dafür dar, den man für Dienste ohne monetäre Gegenleistung zu bezahlen hat. Viele aufwendige Internetdienste wie z. B. Suchmaschinen finanzieren sich über die Weitergabe von Kundenprofilen an die Werbewirtschaft, die diese für zielgerichtete Werbekampagnen oder Marketingaktivitäten verwendet. Die Preisgabe von Daten wird auch mit dem Argument schmackhaft gemacht, dadurch auch den Bedürfnissen der Nutzer besser angepasste Angebote entwickeln zu können. Diese Argumente sind durchaus nicht von vornherein von der Hand zu weisen, und es bleibt dem/der einzelnen KonsumentIn überlassen, wieweit er bzw. sie diesem Modell folgt. Voraussetzung für ein bewusstes Handeln ist natürlich, dass man über die möglichen Folgen unterrichtet ist.

Informationen einholen, was mit personenbezogenen Daten geschieht

Einen ersten Hinweis darauf geben publizierte Informationen zu Datenschutzregeln; sind keine entsprechenden Richtlinien publiziert, sollte man solche anfordern, ehe man persönliche Daten freigibt. Strenge Selbstbeschränkungen bei der Datenauswertung und -weitergabe sind noch nicht hinreichend, diesen auch zu trauen. Zumindest einen Hinweis, dass Datenschutzaspekte ernst genommen werden, können „Gütesiegel"[20] von Privacy-Organisationen geben. Webanbieter, die solche Zertifikate beantragen, verpflichten sich, gewisse Mindeststandards einzuhalten, und eine Überprüfung derselben zuzulassen. In der Regel

[20] Beispielsweise das TRUSTe-Siegel, nähere Informationen dazu finden sich unter der Adresse http://www.truste.org am Internet.

beschränken sich diese Mindestanforderungen auf die Publikation von ausführlichen Regeln, wie mit den Daten der Benutzer umgegangen wird. Damit wird zumindest eine informierte Entscheidung des/der NutzerIn ermöglicht. Da in einzelnen Staaten unterschiedliche Normen und Gebräuche angewendet werden, bleibt einem eine Durchsicht der jeweiligen Bedingungen nicht erspart. Eine wirkliche Garantie, dass kein Missbrauch mit den Daten getrieben wird, können aber auch die strengsten Richtlinien nicht bieten, sie können beispielsweise weder Hackerattacken noch Missbräuche durch Angestellte ausschließen.

Grundsätzlich ist Zurückhaltung bei der Weitergabe persönlicher Daten angebracht

Im Zweifelsfall, und insbesondere wenn es um sensible Daten geht, ist Zurückhaltung angebracht. Es ist durchaus nicht notwendig, seine wahre Identität preiszugeben, oder vollständige Angaben zu machen, wenn nicht Waren bezahlt oder an eine bestimmte Adresse zugestellt werden sollen. Für die oftmals geforderte Angabe einer Email-Adresse, an die z. B. ein Passwort zur Freischaltung von bestimmten Websites oder Software zurückgesandt wird, reicht eine anonyme Adresse vollkommen aus. Aber auch hier darf der Hinweis nicht fehlen, dass über die IP-Adresse in vielen Fällen eine nachträgliche Personifizierung prinzipiell möglich ist.

Pseudonyme können vor weitreichenden Verknüpfungen schützen ...

Die Angabe der wahren Identität ist aus weiteren Gründen nur eingeschränkt zu empfehlen. Eine überwiegende Anzahl von Websites macht Gebrauch von sogenannten Cookies. Dies sind Files, in denen Websites nutzerspezifische Daten auf der Festplatte des eigenen PCs speichern. Mit Hilfe der darin enthaltenen Informationen können einmal getätigte Eingaben, wie z. B. Passwörter beim Besuch einer Site, automatisch neu generiert werden oder spezifische Angebote erstellt werden. Im Normalfall beziehen sich diese Informationen auf den benutzen PC oder einen darauf eingerichteten Account. Wenn aber bei der Registrierung der wahre Name angegeben worden ist, so sind nicht nur die damals gegebenen Daten daran knüpfbar, sondern auch alle weiteren Informationen, die aus dem Surfverhalten auf dieser Site ableitbar sind. Die Einschätzung der Gefährlichkeit von Cookies variiert entsprechend der Vielfalt ihrer Aufgaben und Merkmale, wie etwa der Lebensdauer. Einerseits können sie den Surfalltag ganz erheblich erleichtern, indem sie Routineeingaben automatisieren oder sich etwa bestellte Artikel in einem Warenkorb merken, andererseits können sie die Generierung von Nutzungsprofilen ganz erheblich vereinfachen. Jedenfalls lassen sich einige Sites bei abgeschalteter Cookie-Option nicht oder nur unvollständig wiedergeben, und auch ein manuelles Akzeptieren oder Ablehnen von Cookies wird bei regelmäßigem Surfen zu einer nervenstrapazierenden Aufgabe. Eher praktikabel sind Tools, die teilweise auch als Freeware am Internet erhältlich sind und einen gezielten Umgang mit Cookies erlauben. Allerdings setzen sie für einen effizienten Einsatz in der Regel, wie auch die weiteren, noch skizzierten Privacy-Tools, fortgeschrittene Computer-Kenntnisse voraus.

... aber bewusste Nutzung erfordert Wissen und Zeit

Vorsicht bei Chat- und Newsgroup Beiträgen

Virtuelle Identitäten und Email-Adressen, die keinen Rückschluss auf die Person zulassen, sind auch für die Beteiligung an Chats oder Newsgroup-Diskussionen grundsätzlich empfehlenswert. So lässt sich vermeiden, dass man von anderen Chat- oder Newsgroup-Teilnehmern via Email belästigt wird oder Rückschlüsse auf persönliche Einstellungen oder Vorlieben publik werden. Insbesondere versendete Newsgroup-Beiträge stellen ein großes Privacy-Risiko dar, da diese Beiträge jahrelang archiviert[21] bleiben und abgerufen werden

[21] Unter www.deja.com/home_ps.shtml gelangt man zu einem Formular, in dem Suchabfragen im Archiv gestartet werden können; unter www.deja.com/forms/nuke.shtml zu einem anderen Formular, in dem man die Löschung alter Einträge veranlassen kann. Eine Archivierung von Beiträgen durch Deja kann grundsätzlich verhindert werden, indem in die erste Zeile der Nachricht *x-no-archive: yes* eingetragen wird.

können. Zwar besteht über die IP-Nummer immer noch eine Möglichkeit, die Identität eines Teilnehmers zu rekonstruieren, in der Regel steht dieser Weg aber nur Ermittlungsbehörden und nur mit einem Gerichtsbeschluss offen.

Email ohne Briefumschlag

Eine der häufigsten Nutzungen des Internets ist die Kommunikation über Email. Sowohl in der geschäftlichen als auch in der privaten Korrespondenz spielt sie eine immer wichtigere Rolle. Erstaunlich dabei ist, zumindest auf den ersten Blick, dass der Großteil der Email-Kommunikation unverschlüsselt erfolgt. In Analogie zur herkömmlichen Post würde dies bedeuten, dass die Korrespondenz mittels Postkarten erfolgt bzw. auf Briefumschläge generell verzichtet wird. Das Pendant zu Briefumschlägen ist bei Email die elektronische Verschlüsselung der Nachrichten, die ein unbefugtes Lesen der Nachrichten auf dem Weg über das Internet verhindern können. Hauptansatzpunkte für ein mögliches Lesen von Emails ist aber normalerweise weniger die Übermittlung selbst, sondern die von privaten Email-Providern oder vom Arbeitgeber geführten Email-Accounts. Je nach Konfiguration der Server- und Client-Software bleiben die Nachrichten bis zum Abholen durch den Empfänger oder auch länger am Server gespeichert. Auch hier ist wieder der Hinweis angebracht, dass eine absolute Sicherheit vor unbefugtem Zugang zu vernetzten Rechnern nicht garantiert werden kann. Mit Pretty Good Privacy[22] (PGP) sind zwar seit längerer Zeit schon sehr effiziente Verschlüsselungswerkzeuge verfügbar, die für den privaten Gebrauch als Freeware angeboten werden, dennoch hat sich die Verschlüsselung des Email-Verkehrs noch wenig durchgesetzt. Neben einem wahrscheinlich mitverantwortlichen mangelnden Bewusstsein über mögliche Gefahren ist sicher die Komplexität der Software, welche eine etwas eingehendere Beschäftigung mit kryptographischen Konzepten erfordert, ein weiterer Grund dafür. Allerdings sind schon seit einiger Zeit Versionen verfügbar, die wesentlich einfacher zu installieren und besser in Standard-Email-Programme integriert sind und laufend weiterentwickelt werden. Zudem steigt auch die Zahl von weiteren Anbietern von Email-Verschlüsselungssystemen,[23] welche Verschlüsselungssoftware für weniger versierte Nutzer zugänglich machen, sodass mit steigenden Anwendungszahlen gerechnet werden kann.

Verschlüsselungssoftware vielfach noch zu kompliziert für die breite Anwendung

Einige Dienste versprechen anonymes Surfen und Versenden von Emails

Ein weiterer Aspekt, der bei normaler Post selbstverständlich, bei normalen Emails aber nicht gegeben ist, betrifft die Möglichkeit anonym, d. h. ohne Angabe eines Absenders, Nachrichten zu versenden. Aber auch hier bietet das Internet einige Möglichkeiten. Sogenannte Remailer-, Mixmaster-, Anonymizer- oder Rewebber-Dienste ermöglichen es, anonym zu kommunizieren oder Webseiten[24] zu besuchen. Im Prinzip sind diese Dienste mit Postfächern zu vergleichen, bei denen Nachrichten oder angeforderte Informationen nicht direkt zugestellt bzw. angefordert werden, sondern über besondere Server laufen, die Informationen, welche Rückschlüsse auf den Nutzer erlauben, entfernen, und deren Weiterleitung übernehmen. Bei einfacheren Varianten wird diese Aufgabe von einem Server übernommen. Dementsprechend hängt der erzielbare Grad der Anonymität von der Vertrauenswürdigkeit des Betreibers ab. Ein bekanntes Beispiel für die damit verbundene Problematik ist ein bis 1996 von einem Finnen betriebener Remailer, der seinen Dienst einstellte, nachdem der Betreiber durch Gerichtbeschluss gezwungen wurde, den Absender einer Email bekannt zu geben. Neuere Verfahren bedienen sich ausgeklügelter Verschlüsselungsverfahren und einer Reihe von Servern, über welche Emails weitergeleitet werden. Hier reicht ein einziges vertrauenswürdiges Glied in der

---

[22] Die Software und Dokumentationen dazu sind über http://www.pgpi.org/ erhältlich.

[23] Beispiele dafür finden sich auf http://privacy.net/secureemail/.

[24] Auch dazu sind auf privacy.net Übersichten zu finden: http://privacy.net/remailer/ bzw. http://privacy.net/proxy/.

Kette, um die Anonymität sicherzustellen. Bei diesen sicheren Verfahren besteht aber keine Möglichkeit mehr, Antworten auf ein Mail zu erhalten oder aber die Zustellung einer Nachricht zu überprüfen. Sichere anonyme Email-Zustellung ist sowohl über spezielle Mail-Clients, wie z. B. Private Idaho[25] oder für gelegentliche Nutzung über sogenannte Web-Frontends[26] möglich. Ähnliche Konzepte sind auch für ein anonymes Surfen[27] realisiert worden; auch hier beschränken sich einfache Anonymisierungsserver darauf, eine Zwischenstation zu bilden, bei der Informationen herausgefiltert werden, die Rückschlüsse auf den Nutzer erlauben. Neuere Konzepte setzen auf komplexe Verschlüsselungsmethoden und Netzwerke von Servern, über welche Anfragen geleitet werden. Wie bei den Email-Entsprechungen kann zwischen pseudo-anonymen und wirklich anonymen Konzepten unterschieden werden.

Neuere Systeme bieten höhere Sicherheit ...

Die erste Kategorie ist einfacher und bequemer zu nutzen, die zweite Variante erfordert mehr Kenntnisse und ist mit einem größeren Performanceverlust verbunden, da mehrere Stationen durchlaufen werden müssen, die teilweise vom Nutzer aktiv auszuwählen sind. Dafür ist die Sicherheit nicht davon abhängig, ob man bei einem vertrauenswürdigen Server gelandet ist oder nicht. Neue Systeme, die sich derzeit noch in der Diskussions- oder Entwicklungsphase befinden und teilweise auf anderen Architekturen aufbauen, versuchen, den Kompromiss, den man zwischen Benutzerfreundlichkeit einerseits und Anonymität und Sicherheit andererseits derzeit noch eingehen muss, zu minimieren. Inwieweit diese Systeme weiterentwickelt und in der Praxis verfügbar sein werden, wird nicht zuletzt auch vom Stellenwert abhängen, den Einzelne und die Gesellschaft insgesamt dem Schutz der Privatsphäre beimessen.

... Benutzerfreundlichkeit noch nicht optimal

Umso mehr die Vernetzung um sich greift, und umso länger man mit seinem Rechner online ist, desto größer wird auch die Gefahr, dass von außen auf gespeicherte Daten zugegriffen werden kann. Während bei normalen Zugang zum Internet über Modems dynamisch vergebene IP-Adressen und eine nur temporäre Einbindung ins Internet bereits einen gewissen Schutz vor Angriffen bieten, wird mit der zunehmenden Verbreitung von Always-On-Netzanbindungen über Kabelnetze oder DSL-Technologien auch die Wahrscheinlichkeit von Zugriffen zu privaten Rechnern größer. Ein Zugang von außen zum eigenen Rechner erlaubt je nach den Rechten, die ein Angreifer erreichen kann, wesentliche Einblicke in das Leben der Nutzer. Schlimmstenfalls sind nicht nur Netzaktivitäten wie Email-Kontakte und deren Inhalte sowie besuchte Internetseiten zugänglich, sondern auch Informationen, die nur lokal gespeichert sind, wie z. B. die über den normalen Postweg abgewickelte Korrespondenz.

Schutz des eigenen PC vor Zugriffen von außen gewinnt an Bedeutung

Als Antwort auf diese Gefahren sind eine Reihe von Softwareprodukten[28] verfügbar, welche als private Firewalls den Zugriff auf den Rechner protokollieren und bei verdächtigen Aktivitäten blockieren. Einige dieser Pakete integrieren weitere Funktionen wie etwa die Unterdrückung der Anzeige und Übertragung von Werbebannern, von automatischen Pop-Up-Fenstern oder verhindern die Ausführung von aktiven Inhalten auf dem Rechner. Neben Virenschutzprogrammen, die neben Datenverlusten durch zerstörerische Viren auch einem

Steigendes Problembewusstsein spiegelt sich in neuen Privacy-Tools wider

---

[25] http://www.itech.net.au/pi/

[26] Beispielsweise über http://www.remailer.cjb.net oder etwa http://www.gilc.org/speech/anonymous/remailer.html.

[27] Kostenloses anonymes Surfen ist z. B. über http://www.rewebber.com/ oder http://www.anonymizer.com/services/surf_for_free.html möglich.

[28] Stellvertretend seien die Pakete WebWasher http://www.webwasher.com/ und Freedom http://www.freedom.net/ erwähnt. Sie sind nicht primär als Firewalls konzipiert, sondern bieten eine Reihe von weitergehenden Funktionen zum Schutz der Privatsphäre bei der Internetnutzung an.

Ausspähen der Privatsphäre durch eingeschleuste Trojaner vorbeugen, stellen Firewalls eine weitere Möglichkeit zum Schutz der eigenen Daten dar. Zumindest temporär kann die Installation eines solchen Paktes empfehlenswert sein, lässt sich damit doch eindrücklich nachvollziehen, wie viele Kontakte zu Internet-Sites während der Internetnutzung jeweils im Hintergrund aufgebaut werden, von denen man im Normalfall nichts bemerkt. Damit wird auch deutlich, dass Vorsicht bei der Weitergabe persönlicher Daten und die Möglichkeit anonymer Nutzungsformen die wesentlichen Komponenten für die Wahrung der Privatsphäre darstellen. Der Schutz des eigenen Rechners vor Zugriffen von außen ist zwar sehr wichtig, um einem Verlust eigener Daten vorzubeugen, derzeit stellt er aber noch nicht das primäre Problem bei der Wahrung der Privatsphäre dar. Es ist auch für die Zukunft zu erwarten, dass legale bzw. zumindest nicht ausdrücklich verbotene Formen der Generierung von Nutzerprofilen über „freiwillig“ weitergegebene Daten eine größere Gefahr für den Datenschutz darstellen als der illegale Zugang zu den persönlichen Daten die auf dem eigenen Rechner gespeichert sind.

5 Schlußfolgerungen und Tipps

Datenvermeidung und bewußte Nutzungsentscheidungen

Da die Wege von Daten intransparent sind, ist die beste Strategie sicher jene der *Datenvermeidung*. Dazu ist es aber notwendig die NutzerInnen zu informieren, sie in die Lage zu versetzen die Mechanismen zu erkennen und dann *bewußt* die *Nutzungsentscheidung* zu treffen. Oft wird dies allerdings eine Entscheidung zwischen teilweiser Preisgabe der Privatsphäre und höherer Bequemlichkeit sein.

Wie im Abschnitt über Telekommunikation und Internet erläutert, sind Verschlüsselung, Anonymität, Pseudonyme und bewusste Technologienutzung (Verwendung unterschiedlicher Medien zu unterschiedlichen Zwecken) mögliche Wege zur Aufrechterhaltung/Wiederherstellung von Privatsphäre und Kommunikationsgeheimnis bzw. geschützten Räumen im virtuellen Dschungel.

Aufklärung, Information, Öffentlichkeit

Absolut notwendig ist aber, die *informationelle Selbstbestimmung* im Bewusstsein der NutzerInnen (=aller) zu verankern. Dazu gehören *(Aus-) bildung*, Grundbegriffe der IT-Sicherheit als Basiswissen aller NutzerInnen, *Aufklärung*, *Information*, *Öffentlichkeit* herstellen, breite Diskussion – nicht nur im Kreis der Wissenden.

Tipps zum Umgang mit Datensammlungen und zur Datenvermeidung

- ***Wie erfahre ich, wer was über mich gespeichert hat?***

  Der lange Weg zum Auskunftsrecht

  Diese Frage ist berechtigt, aber nicht ganz leicht zu beantworten. Es gibt keine zentrale Auskunftsstelle, die das beantworten könnte. Das Datenverarbeitungsregister (DVR – § 16 DSG 2000) ist Teil der Datenschutzkommission im Bundeskanzleramt und dazu berufen, alle registerpflichtigen Datenverarbeitungen zu registrieren und Betroffenen Auskunft zu geben. Die Auskunft beinhaltet den Namen und die Adresse der Datenverarbeiter und eine Auflistung der registrierten Verarbeitungen im sogenannten Registerauszug. Die Frage lautet also richtig: wer verbirgt sich hinter der DVR-Nummer XXXXXXX und welche Verarbeitungen werden durchgeführt? Erst im zweiten Schritt kann ich mich als Betroffene an die Unternehmen/ Institutionen direkt wenden und um Auskunft über die mich betreffenden Daten ersuchen. So sehr dieser mehrteilige Weg auch als Hindernis zum gesetzlich fest geschriebenen Auskunftsrecht (§ 26 DSG 2000) gesehen werden kann, so ist dem Argument gegen ein „Superregister“ auch einiges abzugewinnen. Auch wenn man sich als Betroffene schnelle unbürokratische Auskunft über Datenverarbeitungen wünscht, so wäre ein Register, welches auch Inhalte von Datensammlungen registrierte, höchst anfällig für Attaken und damit sicherheitstechnisch ein enormes Risiko. Kritisch anzumerken ist hingegen, dass das DVR in Zukunft kaum mehr ein realistisches Bild über die Datensammlungen in Österreich wird vermitteln können, da durch die sogenannte Standard- und Musterverordnung (StMV, BGBl. II Nr. 201/2000, ftp://ftp.adis.at/privacy/dsg2000/stmv.pdf) eine Reihe von Anwendungen nicht mehr oder nur mehr vereinfacht meldepflichtig sind. Darunter fallen etwa so weitverbreitete Anwendungen wie Kundendateien, Personal- und Mitgliederverwaltung, aber auch Melderegister und Wählerevidenz.

- ***Wie sind die Informationspflichten von Unternehmen und Institutionen geregelt?***

Informationspflicht bei der Ermittlung von Daten

Grundsätzlich muss hier zwischen Informationspflicht bei der Ermittlung von Daten und dem Auskunftsrecht der Betroffenen (einmal jährlich) unterschieden werden.

Die Informationspflicht wird in § 24 DSG 2000 geregelt:

„(1) Der Auftraggeber einer Datenanwendung hat aus Anlaß der Ermittlung von Daten die Betroffenen in geeigneter Weise

1. über den Zweck der Datenanwendung, für die Daten ermittelt werden, und

2. über Namen und Adresse des Auftraggebers,

zu informieren, sofern diese Informationen dem Betroffenen nach den Umständen des Falles nicht bereits vorliegen." Weitergehende Informationspflichten bestehen bei der beabsichtigten Weitergabe von Daten bzw. bei einem bestehenden Widerspruchsrecht der Betroffenen. Problematisch erscheint jedoch die Bestimmung des Absatz 4:

„(4) Keine Informationspflicht besteht bei jenen Datenanwendungen, die gemäß § 17 Abs. 2 und 3 nicht meldepflichtig sind." Damit wird die Informationspflicht ausgehöhlt, da ja wie oben besprochen, durch die StMV eine große Zahl von Anwendungen von der Meldepflicht befreit wurden.

Anders verhält es sich mit dem der Betroffenen.
Dies ist (wie auch die Rechte auf Richtigstellung und Löschung) im § 1 DSG 2000 festgeschrieben und wird im § 26 DSG 2000 näher geregelt:

Auskunftsrecht

„(1) Der Auftraggeber hat dem Betroffenen Auskunft über die zu seiner Person verarbeiteten Daten zu geben, wenn der Betroffene dies schriftlich verlangt und seine Identität in geeigneter Form nachweist. Mit Zustimmung des Auftraggebers kann das Auskunftsbegehren auch mündlich gestellt werden. Die Auskunft hat die verarbeiteten Daten, die verfügbaren Informationen über ihre Herkunft, allfällige Empfänger oder Empfängerkreise von Übermittlungen, den Zweck der Datenverwendung sowie die Rechtsgrundlagen hiefür in allgemein verständlicher Form anzuführen. Auf Verlangen des Betroffenen sind auch Namen und Adresse von Dienstleistern bekannt zu geben, falls sie mit der Verarbeitung seiner Daten beauftragt sind. Mit Zustimmung des Betroffenen kann anstelle der schriftlichen Auskunft auch eine mündliche Auskunft mit der Möglichkeit der Einsichtnahme und der Abschrift oder Ablichtung gegeben werden."

Einschränkungen ergeben sich u. a. aus „überwiegenden berechtigten Interessen der Auftraggeber oder von Dritten" sowie aus „überwiegenden öffentlichen Interessen". Im § 26 wird damit geregelt, dass einmal jährlich kostenlos Auskunft zu erteilen ist. Festzuhalten bleibt, dass dieses Auskunftsrecht sich auf alle Anwendungen bezieht und durch die StMV keine Einschränkung erfährt. Die interessierten Betroffenen können sich demnach direkt an die jeweilige Institution/Unternehmen wenden, auch wenn keine „DVR-Nummer" die als Belästigung empfundenen Anschreiben ziert.

Weitere Rechte der Betroffenen sind die Rechte auf Richtigstellung und Löschung. *Sie werden in § 27 näher geregelt:*

Recht auf Richtigstellung und Löschung

„(1) Jeder Auftraggeber hat unrichtige oder entgegen den Bestimmungen dieses Bundesgesetzes verarbeitete Daten richtigzustellen oder zu löschen, und zwar

1. aus eigenem, sobald ihm die Unrichtigkeit von Daten oder die Unzulässigkeit ihrer Verarbeitung bekannt geworden ist, oder

2. auf begründeten Antrag des Betroffenen."

Das Recht auf Richtigstellung wird allerdings in der Folge eingeschränkt: „Der Pflicht zur Richtigstellung nach Z 1 unterliegen nur solche Daten, deren Richtigkeit für den Zweck der Datenanwendung von Bedeutung ist. Die Unvollständigkeit verwendeter Daten bewirkt nur dann einen Berichtigungsanspruch, wenn sich aus der Unvollständigkeit im Hinblick auf den Zweck der Datenanwendung die Unrichtigkeit der Gesamtinformation ergibt. Sobald Daten für den Zweck der Datenanwendung nicht mehr benötigt werden, gelten sie als unzulässig verarbeitete Daten und sind zu löschen, es sei denn, dass ihre Archivierung rechtlich zulässig ist und dass der Zugang zu diesen Daten besonders geschützt ist."

- ***Was muss ich ausfüllen, was darf ich verweigern, ohne dass mir der Vertrag verweigert wird?***

Nicht alles muss ausgefüllt werden

Sinnvollerweise wird man davon ausgehen müssen, dass KonsumentInnen alle jene Daten zur Verfügung stellen müssen, die zur Abwicklung der angestrebten Geschäftsbeziehung notwendig sind. Darüber hinausgehende Daten können verweigert werden. Grundsätzlich gilt in der österreichischen Rechtsordnung das Prinzip der Vertragsfreiheit. KonsumentInnen können ihnen nicht genehme Passagen aus AGBs streichen, nehmen damit aber in Kauf, dass das jeweilige Unternehmen zu diesen Bedingungen einem Vertag nicht zustimmt. Dies wird in der Regel kaum vorkommen, ist aber möglich. Anders verhält es sich bei Rechtsgeschäften bei denen „Kontrahierungszwang" besteht. Im Bereich Datenschutz relevant ist etwa die Bestimmung des § 91 TKG, der in seinem Absatz 2 festhält, dass „die Übermittlung von im Abs. 1 genannten Daten nur erfolgen (darf), soweit das für die Erbringung jenes Telekommunikationsdienstes, für den diese Daten ermittelt und verarbeitet worden sind, durch den Betreiber erforderlich ist. Sonstige Übermittlungen dürfen nur auf Grund einer vorherigen schriftlichen Zustimmung der Betroffenen erfolgen. Die Zustimmung gilt nur dann als erteilt, wenn sie ausdrücklich als Antwort auf ein Ersuchen des Betreibers gegeben wurde. Die Betreiber dürfen die Bereitstellung ihrer Dienste nicht von einer solchen Zustimmung abhängig machen."

Hier wird also die Notwendigkeit einer ausdrücklichen Zustimmung durch die KonsumentInnen fest geschrieben und gleichzeitig eine Verweigerung der Zustimmung auch real möglich gemacht, da aus der Verweigerung der Zustimmung zur Übermittlung von Daten keine negativen Auswirkungen auf den Dienst selbst (z. B. die Möglichkeit weiter zu telefonieren) entstehen dürfen.

- ***Wann habe ich ein Widerrufsrecht wenn ich einmal zugestimmt habe?***

Widerrufsrecht

Eine einmal gegebene Zustimmungserklärung kann jederzeit widerrufen werden (§ 8 (1) DSG 2000). Darüber hinaus ist auch in § 28 DSG 2000 ein Widerspruchsrecht verankert:

„(1) Sofern die Verwendung von Daten nicht gesetzlich vorgesehen ist, hat jeder Betroffene das Recht, gegen die Verwendung seiner Daten wegen Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen, die sich aus seiner besonderen Situation ergeben, beim Auftraggeber der Datenanwendung Widerspruch zu erheben. Der Auftraggeber hat bei Vorliegen dieser Voraussetzungen die Daten des Betroffenen binnen acht Wochen aus seiner Datenanwendung zu löschen und allfällige Übermittlungen zu unterlassen."

Neben diesen allgemeinen Widerspruchsrechten besteht laut § 268 (6) GewO für Inhaber von Kunden- und Interessentendateien die zusätzliche Verpflichtung „auf die Möglichkeit der Untersagung (der Übermittlung von Daten) ... ausdrücklich und schriftlich hinzuweisen, wenn Daten schriftlich vom Betroffenen zu ermitteln sind."

- ***Wie muss eine korrekte DS-Klausel in AGB aussehen?***

  Nach § 8 DSG 2000 sind „schutzwürdige Geheimhaltungsinteressen" der Betroffenen dann nicht verletzt und die Verwendung der Daten somit zulässig, wenn die Betroffene dieser zugestimmt hat. Diese Zustimmung wird mittlerweile von vielen Unternehmen in ihre AGBs eingebaut und von den KonsumentInnen oft ohne bewusste Kenntnisnahme mit unterschrieben. Hier greift nun das KSchG ein, das im § 6 Abs 3 ein „Transparenzgebot" formuliert. Durch ein OGH Urteil aus 1999 wurde geklärt, dass Zustimmungserklärungen gemäß § 6 Abs 3 KSchG klar und verständlich abgefasst sein müssen. Wird z. B. nur auf eine Weitergabe der Daten an Konzernunternehmen verwiesen, so kann sich die Zugehörigkeit einzelner Unternehmen jederzeit ändern und die Klausel wird daher intransparent gemäß § 6 Abs 3 KSchG. (OGH 27.1.1999, 7 Ob 170/98w siehe: Informationen zum Verbraucherrecht, Ausgabe Nr. 5/1999 Stand: 26.4.1999,). Daraus folgt, dass die bislang auf der Basis der unwirksamen Klauseln gesammelten und übermittelten Daten nicht weiter verwendet werden dürfen, es fehlt ja die wirksame Zustimmung der Betroffenen. Zweitens sind viele Unternehmen aufgerufen, Ihre AGB auf ähnlich unklare Klauseln zu durchforsten und diese zu sanieren (vgl. http://www.konsument.at/seiten/p362.htm).

Zustimmung zur Datensammlung und Übermittlung in AGBs oft unklar und damit ungültig

- ***Wie kann ich Datenentstehung vermeiden?***

  Sorgsamer, sparsamer Umgang mit persönlichen Daten. Grundsätzlich nur Daten weitergeben, die für den jeweiligen Geschäftsfall notwendig sind. Beim Möbelkauf werden Angaben über die Lieferadresse notwendig sein, die Frage nach Familienstand oder Geburtsdatum eher nicht. Die intensive Teilnahme an Gewinnspielen lässt die Zahl der individiuellen Verewigung in Datensammlungen sehr rasch in die Höhe schnellen. Bei der Benutzung von Kundenkarten und Vorteilsclubs, sollte der erzielbare Vorteil dem Verlust an Privatheit gegenübergestellt werden. Für den Spezialfall Telekommunikation und Internet folgen nun einige Stichworte, die im entsprechenden Abschnitt auch ausgeführt sind.

Datenvermeidung ist der beste Datenschutz

- ***Vermeidungsstrategien für die Telekommunikation***
  - Unterdrückung der Rufnummernanzeige beim Angerufenen
  - Ausschalten des Handys bei Nichtbenutzung
  - (Wertkartentelefon).

Vermeidungsstrategien für die Telekommunikation

- ***Vermeidungsstrategien für die Internetnutzung***
  - AGBs nach Datenschutzaspekten vergleichen
  - Informationen über Datenschutzrichtlinien besorgen
  - Mehrere Provider nutzen
  - Zurückhaltung bei Preisgabe von Daten
  - Andere Identitäten und anonyme Email-Adressen verwenden; insbesondere bei Chats und Newsgroup-Beiträgen
  - Gegebenenfalls eigene Beiträge aus Newsgroup-Archiv entfernen und Archivierung blockieren
  - Verschlüsselungssoftware nutzen
  - Anonyme Mail- und Webdienste nutzen
  - Spezialisierte Softwarepakete zum Schutz der Privatsphäre und des eigenen Rechners einsetzen.

und das Internet

Anhang

Glossar

AFIS-System..... „Automatisiertes-Fingerabdruck-Indentifizierungs-System“; Datenbank mit Fingerabdrücken, die vom → EKF gespeichert werden.

AUF ..... Kürzel in der → UKV-Liste für Scheckkarten oder Bankomatenmißbrauch

BSI..... Bundesamt für Sicherheit in der Informationstechnik (D)

C..... Kürzel in → UKV-Liste für Kreditkartenüberziehen

Clip ..... Abk. für „Calling Line Identification Presentation“; Telefonnummer des Anrufers wird angezeigt.

CLIR ..... Abk. für “Calling Line Identification Restrication”; Unterdrückung der Anzeige der Rufnummer des Rufenden beim Gerufenen.

DSL..... Abkürzung für „Digital Subscriber Line“-Technologie. DSL bietet eine Technologie, um schnelle Internet-Anbindungen über die Kupferleitungen des Telefonnetzes und parallel zum Telefondienst zu betreiben.

DVR..... Datenverabeitungsregister

EKF..... Büro für Erkennnungs- und Fahndungstechnik (in Wien)

G ..... Kürzel in → UKV-Liste für Girokontenüberziehen

GPS..... „Global Positioning System“; Technologie, die zum Orten von Sendern/Empfängern (z. B. in Handys, Autos, Schiffen o. ä.) mit Hilfe von Satelliten benutzt wird. Erhält ein Empfänger Daten von mindestens vier Satelliten, kann seine Position auf 50 bis 100 genau festgestellt werden. GPS wird u. a. für Navigationssysteme in neuen Automodellen verwendet und soll demnächst evtl. für → Road Pricing benutzt werden. Bei Mobiltelefonen wird GPS in Verbindung mit → GMS verwendet.

GMS..... „Global Mobile Communication System“; Technologie in Handys

HLR ..... „Home Location Register“; Daten vom → MSC werden an das HLR weitergeleitet. Somit kann z. B. der Mobilfunkbetreiber herausfinden, wann sich sein(e) KundIn wo im Ausland befunden hat.

IP-Nummer ..... Nummer über die jeder Rechner im Netz zu erreichen und eindeutig identifizierbar ist. Sie besteht aus vier, durch Punkte getrennten, dezimalen Ziffern zwischen 1 und 254.

ISP ..... Abkürzung für „INTERNET Service Provider“

ISPA..... Verein der Internet Service Provider Austria

ISDN..... Integrated Services Digital Network; digitales Telekommunikationsnetz mit der Möglichkeit mehrere Dienste (Telefon, Fax oder E-mail) gleichzeitig zu nutzen.

KKE ..... „Klein-Kreditnehmer-Evidenz“

KKK..... „Klein-Kreditnehmer-Kartei“

KSV ..... Kreditschutzverband

MSC ..... „Mobile Switching Center“; Daten über den regelmäßigen Funkkontakt von Handys zur Funkstation (auch wenn nicht telefoniert wird) werden weitergeleitet an das MSC, welche wiederum weitergeleitet wird an die Zentrale, das → HLR.

PIN ..... „Personal Identification Number“; Paßwort bzw. Code

Road-Pricing/Satelliten-Road-Pricing
GPS- und GSM-unterstützte Technologie, die feststellen kann, wann sich welches Auto wie lange und wo auf welcher Straße (insb. Autobahn) aufgehalten hat und wieviel Gebühren dadurch anfallen. Wird als Alternative zu pauschalen Maut-Gebühren gehandelt und soll für Lkws 2001 in Österreich eingeführt werden.

SCHUFA ..... Schutzgemeinschaft für allgemeine Kreditsicherung (in Deutschland)

SIM ..... „Subscriber Identification Module“ = Handy-Benutzerkarte; speichert Informationen über das Handy und dessen Einstellungen (z. B. PIN-Code etc.)

SMS ..... „Short Message Service“; Textnachricht mit begrenzter Anzahl von Zeichen (i. d. R. um 160 Zeichen), die via Handy oder Internet an ein Handy geschickt werden kann. Die empfangene Nachricht kann auf dem Display des Handys gelesen werden.

SVK ..... „Sozialversicherungskarte“ ...

TAN ..... Transaktionsnummer; wird bei → Homebanking für Überweisungen benötigt. Da die TANs praktisch die Unterschrift ersetzen, müssen sie vom Kunden aufbewahrt werden ...

UKV ..... „Unerwünschte Kontoverbindung“; „schwarze Liste“ aller Banken, auf der KundenInnen aufgelistet sind, die bei keiner Bank in Österreich einen Kredit erhalten und teilweise auch kein Konto, weil sie irgendwann einmal hoch verschuldet waren. Die Existenz einer solchen Liste wurde lange bestritten, obwohl es sie in Österreich schon seit dem 1. Dezember 1965 gibt. Die aufgelisteten Personen wissen davon in der Regel nichts.

VBG ..... Kürzel in der → UKV-Liste für Versuchter Betrug

WAP ..... Wireless Application Protocol, bietet die Möglichkeit Internetseiten auf Handy-Displays darzustellen.

ZIS ..... (1) „Zentrales Informationssystem“; Datenbank, in der alle Kfz-Haftpflicht und Kaskoschäden gespeichert werden und laufend miteinander abgeglichen werden. ZIS soll Versicherungsbetrug aufdecken.
(2) „Zoll-Informations-System“; Datenbank, in der Finanz-, Zoll-, Import- und Exportdaten innerhalb der EU gespeichert werden.

Kommentierte URL Liste

Siehe: http://www.oeaw.ac.at/ita/ebene2/d2-6.htm

Literatur

BLEICH, H. (2000): Selbstverdunkelung, *c´t Magazin für Computertechnik (16)*, 156-159.

BÄUMLER, Helmut, Hrsg. (1998): *Der neue Datenschutz*, Hermann Luchterhand Verlag GmbH, Neuwied.

BÄUMLER, Helmut, Hrsg. (2000): *E-Privacy*, DuD-Fachbeiträge hrsg. von Andreas Pfitzmann et al 1. Aufl. Friedr. Vieweg & Sohn Verlagsges.mbH, Braunschweig.

BKA (1997): *Datenschutzbericht 1995*, Amtsdruckerei BKA, Wien.

BKA (1999): *Datenschutzbericht 1997*, Amtsdruckerei BKA, Wien.

BORKING, J. (1998): 2008 – Ende der Privatheit?, Bäumler, H. Hrsg., 1998, *Der neue Datenschutz*, 283-293.

DEMUTH, T. (2000): Unerkannt surfen, *c´t Magazin für Computertechnik (6)*, 196-201.

DSG (2000): BGBl. I Nr 165/1999.

DUSCHANEK, Alfred; ROSENMAYER-KLEMENZ, Claudia (2000): *Datenschutzgesetz 2000*, Wissenschaft und Wirtschaftspraxis hrsg. von Wirtschaftskammer Österreich, Wien.

FEDERRATH, H., BERTHOLD, O., KÖHNTOPP, M., KÖPSELL, S. (2000): Tarnkappen fürs Internet, *c´t Magazin für Computertechnik (16)*, 148-155.

JANETZKO, D., ZUGENMAIER, D. (2000): Viele Gesichter, *c´t Magazin für Computertechnik (18)*, 88-92.

KOLLMANN, K. (1999): *Aktuelle Verbraucherprobleme beim Schutz personenbezogener Daten. Datenschutz aus Verbrauchersicht*, im Auftrag von: BMWV, 30. Jänner 1999, Wien: Institut für Technologie und Warenwirtschaftslehre, Wirtschaftsuniversität Wien

LECHNER 2000, Konsumentenwünsche sind vorhersehbar, Der Standard, 12.10.00, B1.

OPASCHOWSKI, HORST W. (1998): *Der gläserne Konsument? Multimedia und Datenschutz*, British-American Tabacco (Germany) GmbH, Hamburg.

PEISSL, Walter (2000): Überwachung total: ECHELON, *ITA-News 04/2000*, Wien.

REISCHL, Gerald (1998): *Im Visier der Datenjäger*, Ueberreuter, Wien.

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

Statistisches Zentralamt (1999): Tätigkeitsbericht des DVR 1998“ publiziert im „*Tätigkeitsbericht des Statistischen Zentralamtes über das Jahr 1998*“, Wien.

StMV, BGBl. II Nr. 201/2000.

VKI (1999): Informationen zum Verbraucherrecht, Ausgabe Nr. 5/1999 Stand: 26.4.1999.

ZEGER et al. (1999): *Erfahrungen zum Datenschutz 1980-1998*, im Auftrag des BMWV, Wien.