

PRIVATSPHÄRE 2.0

**BEEINTRÄCHTIGUNG DER
PRIVATSPHÄRE IN ÖSTERREICH
NEUE HERAUSFORDERUNGEN
FÜR DEN DATENSCHUTZ**

ENDBERICHT

**ITA-PROJEKTBERICHT NR.: A53
ISSN: 1819-1320
ISSN-ONLINE: 1818-6556**



OAW

Österreichische Akademie
der Wissenschaften



INSTITUT FÜR
TECHNIKFOLGEN-
ABSCHÄTZUNG



PRIVATSPHÄRE 2.0

BEEINTRÄCHTIGUNG DER PRIVATSPHÄRE IN ÖSTERREICH NEUE HERAUSFORDERUNGEN FÜR DEN DATENSCHUTZ

ENDBERICHT

INSTITUT FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
DER ÖSTERREICHISCHEN AKADEMIE DER WISSENSCHAFTEN

Projektleitung: Mag. Dr. Walter Peissl

Autoren: Jaro Sterbik-Lamina, MSc
Mag. Dr. Walter Peissl
Ing. Mag. Johann Čas

STUDIE IM AUFTRAG DER BUNDESARBEITSKAMMER

WIEN, FEBRUAR 2009

IMPRESSUM

Medieninhaber:

Österreichische Akademie der Wissenschaften
Juristische Person öffentlichen Rechts (BGBl 569/1921 idF BGBl I 130/2003)
Dr. Ignaz Seipel-Platz 2, A-1010 Wien

Herausgeber:

Institut für Technikfolgen-Abschätzung (ITA)
Strohgasse 45/5, A-1030 Wien
<http://www.oeaw.ac.at/ita>

Die ITA-Projektberichte erscheinen unregelmäßig und dienen der Veröffentlichung der Forschungsergebnisse des Instituts für Technikfolgen-Abschätzung.

Die Berichte erscheinen in geringer Auflage im Druck und werden über das Internetportal „epub.oeaw“ der Öffentlichkeit zur Verfügung gestellt:
<http://epub.oeaw.ac.at/ita/ita-projektberichte>

ITA-Projektbericht Nr.: A53

ISSN: 1819-1320

ISSN-online: 1818-6556

<http://epub.oeaw.ac.at/ita/ita-projektberichte/d2-2a53.pdf>

© 2009 ITA – Alle Rechte vorbehalten

Inhalt

Zusammenfassung	I
1 Einleitung	1
2 Technische Entwicklung	3
2.1 Radio Frequency Identification (RFID)	3
2.2 Web 2.0	5
2.3 Das Moore'sche Gesetz	5
2.4 P3P	6
2.5 Ubiquitous Computing	7
2.6 Verteilte Systeme	8
2.7 Kryptographie	9
2.8 Sensortechnik	9
3 Gesellschaftliche Trends	11
3.1 Web 2.0	11
3.1.1 Aufmerksamkeitsökonomie und Bürgerjournalismus	13
3.1.2 Google Earth und Street View	14
3.2 Vertrauen der ÖsterreicherInnen in den Datenschutz	15
3.3 Datenfilterung	16
3.4 Sicherheitsbedürfnis und Videoüberwachung	17
3.5 Cyber-Crimes	18
4 Staatlich-politische Initiativen	21
4.1 Österreich	22
4.1.1 Telekommunikationsgesetz 2003 (TKG 2003)	22
4.1.2 Sicherheitspolizeigesetz (SPG)	22
4.1.3 Bildungsdokumentationsgesetz	23
4.1.4 Elektronischer Gesundheitsakt (ELGA)	23
4.1.5 e-Government	24
4.1.6 e-Voting	25
4.2 Europa	25
4.2.1 Stellungnahmen der Article 29 Working Party	25
4.2.2 Vorratsdatenspeicherung	27
4.2.3 Passagierdatenweitergabe	28
5 Privatwirtschaftliche Anwendungen	29
6 Datenschutz & Datenschatz	31
7 Schlussfolgerungen	37
8 Literatur	41
8.1 Bücher/Berichte	41
8.2 Gesetze/Standards/Normen	41
8.3 Im Internet verfügbare Informationen	42
Anhang	51
Abkürzungsverzeichnis	51
Glossar	52

Tabellenverzeichnis

Tabelle 1: Speicherorte und Datenarten	33
--	----

Zusammenfassung

Fast 10 Jahre nach der Studie zur „Beeinträchtigung der Privatsphäre Österreichs“ ist es angesichts der kurzlebigen Zeit gut, einen erneuten Blick auf die Situation in Österreich zu werfen. Der relativ lange Zeitraum lässt auch einen distanzierten Rückblick und einen nüchternen Ausblick auf die weitere Entwicklung zu. Nüchtern fällt diese Beurteilung aber nicht nur wegen der zeitlichen Distanz aus, sondern auch weil der Zug scheinbar unbeirrt – aus Sicht des Datenschutzes – in die falsche Richtung weiterfährt. Dabei zeichnen sich durchaus auch positive Alternativen am Horizont ab, diese werden aber von den EntscheidungsträgerInnen zumeist, bewusst oder unbewusst, nicht wahrgenommen.

Die geringsten Veränderungen im Vergleich zur letzten Studie sind im Bereich der technischen Entwicklung zu beobachten. Hier setzt sich der Trend fort, dass neue Technologien die Möglichkeiten der Datengenerierung und deren Verarbeitung beständig und teilweise massiv erhöhen, die parallel stattfindenden Innovationen im Bereich datenschutzfördernde Technologien aber kaum in der Realität genutzt werden.

Auch auf individueller und gesellschaftlicher Ebene scheint sich die Lücke zwischen der geäußerten Anerkennung der Bedeutung von Privatsphäre und dem tatsächlichen Verhalten nicht zu schließen. Im Gegenteil, im Bereich sozialer Netzwerke im Internet werden teilweise intimste Details freiwillig veröffentlicht. Hier wird offensichtlich vergessen, dass das Netz nicht vergisst, ebenso dass die Anonymität vor dem Bildschirm und die Geschlossenheit von Freundeskreisen nur scheinbar sind, über die persönlichen Daten aber, sofern sie erst einmal preisgegeben wurden, nicht mehr selbst bestimmt werden kann. Eine ähnliche Diskrepanz lässt sich im Bereich Sicherheit und Schutz der Privatsphäre beobachten, während Studien eine beträchtliche Skepsis innerhalb der Bevölkerung bezüglich der Wirksamkeit und Angemessenheit von Überwachungsmaßnahmen aufzeigen, spiegelt sich diese Skepsis kaum in öffentlichen oder politischen Debatten wider.

Im Bereich innere Sicherheit waren in infolge der Terroranschläge von New York, London und Madrid wohl die größten Veränderungen zu beobachten. Sie haben auf nationaler und internationaler Ebene zu Maßnahmen geführt, die ohne diese Ereignisse wohl kaum durchsetzbar gewesen wären. Als Konsequenz sind – nach einer Phase, in der private Unternehmungen als Hauptbedrohung für die Privatsphäre angesehen wurden – wieder staatliche Institutionen in den Mittelpunkt dieser Befürchtungen gerückt; insbesondere wenn man bedenkt, dass auch der Zugriff auf im privaten Bereich generierte Daten, zum Beispiel die Nutzung von Telekommunikations- und Internetdiensten, betroffen ist.

Der Bereich Sicherheit ist aber auch jenes Gebiet, in dem sich Gegenentwicklungen am stärksten abzeichnen. Beispiele von Diebstählen oder Verlusten von großen Datenmengen stärken das öffentliche Bewusstsein, dass der Schutz von persönlichen Daten ein wesentliches Element von Sicherheit vor wirtschaftlichen Nachteilen darstellt, maßlose Wünsche und Missbrauchsfälle im staatlichen Bereich, dass der Schutz der Privatsphäre einen unverzichtbaren Bestandteil individueller Sicherheit darstellt.

Im Bericht wird auch eine Reihe von neuen Entwicklungen und Instrumenten skizziert, die auf gesetzlicher, organisatorischer, technischer und wirtschaftlicher Ebene den Schutz der Privatsphäre fördern und stärken können. Hier bleibt unverändert die Forderung aufrecht, diese Möglichkeiten in einer krea-

tiven und intelligenten Weise zu nutzen: diese reichen von einer verstärkten Aufklärung der Bevölkerung, Anpassung der regulativen Vorgaben an neue technische und gesellschaftliche Entwicklungen, die Umsetzung von entsprechenden organisatorischen und technischen Konzepten bis zur Förderung von Instrumenten der Selbstregulierung, um einige der wesentlichen Elemente zu nennen. Zentral wird es sein, diese Instrumente koordiniert einzusetzen und die entsprechenden Ressourcen zur Durchsetzung von gesetzlichen Vorgaben zur Verfügung zu stellen. Eine aktive Unterstützung dieser Bemühungen durch Interessenvertretungen zum Wohle der KonsumentInnen und BürgerInnen erscheint in Österreich unverzichtbar.

I Einleitung

In den vergangenen Jahren gab es eine Reihe von Entwicklungen, die zu einer veränderten Situation für den Schutz der Privatsphäre beigetragen haben; einerseits den technischen Fortschritt und andererseits die damit in Wechselwirkung stehende gesellschaftspolitische Entwicklung.

Diese Kurzstudie versucht, anknüpfend an die Studie „Beeinträchtigung der Privatsphäre in Österreich“, die im Jahr 2000 im Auftrag der Bundesarbeitskammer erstellt wurde, die wesentlichen Entwicklungen der letzten Jahre aufzuzeigen, die veränderte Situation im Hinblick auf die Privatsphäre der BürgerInnen zu beschreiben und daraus mögliche Vorgehensweisen zum Schutz derselben abzuleiten.

Die technologische Seite lässt sich in drei Bereiche unterteilen, die unterschiedlich großen Einfluss auf die Entwicklung genommen haben. Es gab Weiterentwicklungen von bestehenden Technologien, Innovationssprünge und es gibt Visionen für die Zukunft, die in den nächsten Jahren Marktreife erlangen können und damit neue Möglichkeiten für Schutz oder Bedrohung der Privatsphäre eröffnen.

Die Weiterentwicklung bestehender Technologien erfolgt in der Regel relativ kontinuierlich und in kleineren Schritten. Oft entstehen durch technische Verbesserungen neue Einsatzgebiete und Märkte, weil Produkte zum Beispiel billiger produziert werden können oder kleiner, robuster oder autonomer werden, wie man etwa am Beispiel der Videokameras sehen kann.

Innovationssprünge sind dort zu beobachten, wo neue technische Möglichkeiten eingesetzt werden, die vorher nicht existierten. Ein klassischer Innovationssprung der letzten Jahre ist die Entwicklung im Internet zum sogenannten Web 2.0. Da wird schon durch die Bezeichnung, ähnlich wie bei der Versionierung von Softwareprodukten eine neue Versionsnummer nur bei einer wesentlichen Neuerung vergeben wird, der Innovationssprung angedeutet. In diesem Fall war es eine Vielzahl an technologischen Entwicklungen und Verbesserungen, die erst gemeinsam dazu geführt haben, dass die Interaktivität verbessert und die Bildung von vielen ausdifferenzierten Gemeinschaften über Web-Portale und damit eine soziale Innovation möglich wurden.

An der Schwelle von der Vision zur Innovation steht heute zum Beispiel die Quantenkryptographie. Sie wird in den nächsten Jahren vermutlich Marktreife erlangen und damit eine Revolution in der Sicherheit der digitalen Kommunikation einleiten.¹ Ein anderes Beispiel für eine vor uns liegende Entwicklung ist die zunehmende Durchdringung des Alltags mit sogenannten „smart objects“, die uns – bis hin zum „smart dust“ – in einer vom „ubiquitous computing“ geprägten Welt umgeben werden, für uns oder andere „verlängerte“ Sinnesorgane darstellen und unsere Sicht auf die Wirklichkeit beeinflussen werden.²

**Die Entwicklungen
der letzten Jahre im
technologischen
Bereich ...**

¹ Die Presse (2008): Geheime Post zwischen Wien und St. Pölten, <http://diepresse.com/home/techscience/wissenschaft/421055/index.do> (6. Jänner 2009).

² Mattern, Friedemann (2008): Herausforderungen der technischen Entwicklung an den Datenschutz, <http://www.lfd.m-v.de/dschutz/veranst/aktechnik50/mattern50.pdf> (28. Jänner 2009).

**... und im
gesellschaftlichen
Bereich**

Auch in Wechselwirkung mit dem technischen Fortschritt steht die zeitgleich stattfindende gesellschaftliche Entwicklung, die von verschiedenen Faktoren beeinflusst wird. Ein immer wieder genanntes Ereignis, das viel zur aktuellen Situation im Bereich Datenschutz und Privatsphäre beigetragen hat, waren die Terroranschläge vom 11. September 2001 in New York. Seit diesem Tag, verstärkt noch nach den späteren Anschlägen in Madrid und London, wird versucht, auch durch gesetzliche Regelungen den Terror besser bekämpfen zu können, was sich unter anderem darin äußert, dass die Hürden für die Überwachung der BürgerInnen stark gesenkt wurden. Die Stimmung, die das erleichterte, wird aber auch dazu genutzt, Begehrlichkeiten nach Daten durchzusetzen, die sonst vermutlich keine Chance auf Realisierung gehabt hätten. Dadurch entstand ein Ungleichgewicht in der Balance zwischen (vermeintlicher) Sicherheit und Freiheit des Einzelnen, das jedoch bis heute noch nicht zu dem breiten gesellschaftlichen Diskurs geführt hat, den man sich bei so substantiellen Änderungen erwarten würde.

2 Technische Entwicklung

Im Folgenden sollen die wichtigsten Entwicklungen exemplarisch aufgezählt werden, die die Entwicklung der Privatsphäre in den letzten Jahren beeinflusst haben, oder in den nächsten Jahren beeinflussen können.

2.1 Radio Frequency Identification (RFID)

Diese Technologie, die es mit einem Lesegerät über Funk bzw. elektromagnetische Wellen ermöglicht, Personen und Gegenstände, die zuvor mit einem Transponder versehen wurden, zu identifizieren, wird in zunehmendem Maße den Alltag der KonsumentInnen durchdringen. Seit den Sechziger Jahren des 20. Jahrhunderts wird diese Technologie im zivilen Bereich eingesetzt. In den letzten Jahren wurde die Logistik als ein wesentlicher Anwendungsbereich erkannt. In weiterer Folge wird sie in den kommenden Jahren die bisher oft verwendeten Barcodes und zum Teil auch Magnetstreifenkarten und ähnliches ersetzen.

Die Technik kommt in verschiedenen Varianten zum Einsatz. Die Transponder können entweder permanent mit Energie versorgt sein, oder diese durch Induktion vom Lesegerät erhalten. Damit ist es ihnen dann möglich, nach einer entsprechenden Anfrage eines Lesegeräts den gespeicherten Inhalt eines Chips, der Teil des Transponders ist, zu senden. Der Speicherinhalt enthält die Daten, die zur Identifikation notwendig sind.

Dadurch ist es heute möglich von einzelnen Verpackungen, über Paletten bis hin zu Containern im Transportwesen auch aus größerer Entfernung als bei Barcodes und deutlich schneller die einzelnen Stücke zu erfassen.

So wurde zum Beispiel die Firma Northland in Österreich mit dem „ebiz e-government award“ dafür ausgezeichnet, dass sie im Rahmen eines Projekts an allen Bekleidungsstücken im Geschäft in Graz RFID-Etiketten angebracht hatte, um ohne manuelle Zählung jederzeit erfassen zu können, welche und wieviele Produkte sich im Geschäft befinden. Zusätzlich werden die RFID-Tags auch in der Diebstahlsicherung eingesetzt.³ Natürlich kann mit der selben Technologie nicht nur der Aufenthaltsort eines bestimmten Objekts festgestellt werden – solange zu erwarten ist, dass einer der Chips bei einer bestimmten Person bleibt, könnten auch damit (kleinräumige, etwa in Firmen über Ausweiskarten) Bewegungsprofile erstellt werden.

Die Transponder lassen sich sehr klein und sehr kostengünstig herstellen, wodurch sie mittlerweile in Nummernschildern, Ausweisen, Fahrkarten, Preisschildern, Transportaufklebern, Büchern in Bibliotheken, Nutztieren, Wegfahrsperrern und ähnlichem zu finden sind.

Immer mehr Einsatzgebiete für die kleinen, kostengünstigen Speicher

³ ebiz e-government award (2008): Sieger 2008, <http://www.report.at/award/archive/Sieger2008.htm> (6. Jänner 2009); Presstext Austria (2008): Outdoor-Experte Northland für neuartige RFID-Diebstahlsicherung ausgezeichnet, <http://www.pressetext.at/pte.mc?pte=080925039> (6. Jänner 2009); Digitales Österreich (2008): Ministerin Silhavy vergibt bundesweiten ebiz-e-government Preis und Sonderpreise, http://www.digitales.oesterreich.gv.at/site/cob__32165/5236/default.aspx (6. Jänner 2009).

Jeder kann den Inhalt auslesen

Der größte Nachteil dieser Technologie ist leicht zu erkennen: dort wo Informationen über eine gewisse Entfernung ausgelesen werden können, können Unbefugte den Vorgang des Auslesen belauschen, um an die Informationen zu gelangen, oder selbst ein Lesegerät bereit halten, um die Chips auszulesen.

In Österreich werden spätestens Ende Juni 2009 nicht nur die Passbilder sondern auch die Abdrücke der beiden Zeigefinger auf dem RFID-Tag im Reisepass gespeichert.⁴ Bei zunehmender Bedeutung der biometrischen Identifizierung von Personen werden auch diese Daten wichtiger und begehrter werden. Um das Auslesen durch Unbefugte zu verhindern, werden verschiedene Verschlüsselungsverfahren eingesetzt, die inzwischen aber kaum noch ein Hindernis darstellen. Dem weltweit bei Ticketing-Anwendungen am meisten verbreiteten Mifare-Chip der Firma Philips wurden schon mehrmals Sicherheitslücken nachgewiesen.⁵ Probleme können aber natürlich schon davor, bei der Verarbeitung der Daten, entstehen, wenn hier nicht mit der nötigen Sorgfalt vorgegangen wird.⁶

Es ist also zu befürchten, dass nicht nur Identitätsdiebstahl damit in den kommenden Jahren eine neue Dimension bekommen wird, sondern dass auch die informationelle Selbstbestimmung unter dem vermehrten Einsatz der Technik leiden wird, da es bei immer mehr getagten Waren, Kundenkarten und nicht merkbaren Auslesevorgängen für den Verbraucher nicht mehr nachzuvollziehen ist, wer über sein Konsumverhalten, die mitgeführten Gegenstände, seine Interessen usw. Bescheid weiß. Genau das ist aber der Punkt, wo die Wünsche der KonsumentInnen in eine andere Richtung gehen als die aktuelle Entwicklung. Wie aus der Arbeit zum Projekt RFID-Consultation seit 2006 ersichtlich ist, wünschen sich VerbraucherInnen vor allem mehr Transparenz, mehr Wissen über die Technologie und die Anwendungen und das Recht selbst zu entscheiden.⁷

⁴ Bundesministerium für Inneres (2008): BM.I Internet – Reisepass, <http://www.bmi.gv.at/reisepass/> (6. Jänner 2009).

⁵ Naone, Erica (2008): Gehackte U-Bahn, <http://www.heise.de/tr/Gehackte-U-Bahn--/artikel/114374> (6. Jänner 2009); Die Firma NXP-Semiconductors, die den Chip produziert und das Projekt gemeinsam mit Northland und RF-iT durchgeführt hat (siehe Fußnote 3), hatte übrigens im Juli 2008 eine niederländische Universität verklagt, um zu verhindern, dass Details über Sicherheitslücken des Mifare-Chips an die Öffentlichkeit gelangen.

⁶ Heise security (2009a): Bericht: Unsichere Verarbeitung der Fingerabdrücke in Meldebehörden, <http://www.heise.de/security/Bericht-Unsichere-Verarbeitung-der-Fingerabdruecke-in-Meldebehoerden--/news/meldung/126707> (4. Februar 2009).

⁷ Your voice on RFID (2006): Background document for public consultation on Radio Frequency Identification (RFID) – Summary of five workshops, http://www.rfidconsultation.eu/docs/ficheiros/Your_voice_on_RFID.pdf (4. Februar 2009).

2.2 Web 2.0

Aus technischer Sicht ist das sogenannte Web 2.0 nicht eine einzelne Weiterentwicklung oder Neuerung, sondern ein Bündel von verschiedenen Neuerungen, die erst gemeinsam das möglich machen, was heute als Web 2.0 bezeichnet wird. Es gibt jedoch auch Kritiker, die es für unpassend halten, dass der Begriff benutzt wird, weil sie der Ansicht sind, dass das Internet davor auch schon interaktiv war (zum Beispiel Usenet-Groups, sowie Webbrowser, die auch als HTML-Editoren zu verwenden waren), und die Neuerungen keine revolutionäre Innovation seien, sondern das Ergebnis eines kontinuierlich verlaufenden Entwicklungsprozesses.⁸

**Viele Neuerungen
führten zum Web 2.0**

Aus rein technischer Sicht mag das stimmen. Die Rezeption der zur gleichen Zeit neu verfügbaren Techniken beim User und dem, was Webentwickler daraus gemacht haben, hat aber zu einer breiteren und anderen Art der Benutzung geführt, weshalb aus Sicht der Autoren die Verwendung eines neuen Begriffs gerechtfertigt erscheint.

Die Techniken, die hier aufzuzählen wären, um einen kurzen Umriss der technischen Neuerungen zu geben, sind unter anderen: Wikis, Geotagging, Blogs, Abonnementdienste/Feeds (zum Beispiel über RSS/Atom), Podcasts, XML, Ajax, SOAP und Funktionen aus dem Semantic Web.⁹

Die Technik ermöglicht hier jedoch nur das, was mit dem Schlagwort beschrieben wird, und ist nicht selbst die so bezeichnete Innovation. Weitere Erörterungen sind deshalb im nächsten Kapitel zu finden (siehe Punkt 3.1).

2.3 Das Moore'sche Gesetz

Abweichend von der ursprünglichen Interpretation der Aussage von Gordon Moore aus dem Jahr 1965¹⁰ (eine Verdoppelung der Komplexität (Anzahl der Transistoren) integrierter Schaltkreise mit minimalen Komponentenkosten alle ein bis zwei Jahre), versteht man darunter heute die Verdoppelung der Anzahl an Transistoren auf einem handelsüblichen Prozessor alle 18 Monate. Die Entwicklung in diesem Bereich entsprach bis heute im Großen und Ganzen der Beobachtung/Vorhersage Moores.

**Moores Beobachtungen
treffen immer noch zu**

Viele verstehen fälschlicherweise eine Verdoppelung der Leistungsfähigkeit alle 18 Monate darunter. Im Zuge dieser falschen Interpretation wird heute von vielen Bereichen der elektronischen Datenverarbeitung angenommen, dass sich auch die Leistungsfähigkeit anderer Komponenten, wie zum Beispiel die Speicherdichte und damit verbunden die Speicherkapazität von Festplatten, alle 18 Monate verdoppeln würde. Übereinstimmungen sind hier jedoch nur teilweise zu finden.

⁸ Roth, Wolf-Dieter (2006): „Web 2.0 ist nutzloses Blabla, das niemand erklären kann“, <http://www.heise.de/tp/r4/artikel/23/23472/1.html> (6. Jänner 2009).

⁹ Diese Begriffe, so wie andere, werden im Glossar im Anhang dieser Arbeit erläutert.

¹⁰ Wikipedia-Artikel zum Moore'schen Gesetz (2008): http://de.wikipedia.org/wiki/Mooresches_Gesetz (6. Jänner 2009).

**Sehr große
Datenmengen zu
verarbeiten ist kein
Problem mehr**

Was sich in den letzten Jahren aber beobachten ließ, ist eine starke Verbilligung rechenstarker Computersysteme und großer Datenspeicher.¹¹ Zusammen mit Technologien, die den Zusammenschluss vieler kleiner, billiger Systeme zu einem großen Rechnernetz ermöglichen, hat das dazu geführt, dass weder Rechenleistung noch Speicherbedarf ein limitierender Faktor in der Verarbeitung großer Datenmengen sind. In vielen Fällen, in denen es zum Beispiel um die Überwachung einer großen Menge an Personen geht, bei der sehr viele Daten anfallen, konnte man früher noch annehmen, dass nicht alles gemacht wurde, was technisch möglich war, weil es weltweit nur sehr wenig Institutionen gab, die sich das hätten leisten können. Dieses Argument verliert heute durch die Preisentwicklung der letzten Jahre immer mehr an Bedeutung.

Dadurch wird es überhaupt erst möglich, Überwachungen im großen Stil durchzuführen, Profile aller KundInnen eines Konzerns anzulegen und bei jedem KundInnenkontakt zu aktualisieren oder Daten im großen Stil auf Vorrat zu speichern.

2.4 P3P

P3P ist die Abkürzung für Platform for Privacy Preferences, eine virtuelle Plattform zum Austausch von Datenschutzinformationen von Webseiten, die 2002 vom World Wide Web Consortium (W3C) als Standard empfohlen wurde.¹²

P3P hat bis jetzt noch so gut wie keinen Einfluss auf den Schutz der Privatsphäre, wäre aber ein guter Ansatz, um die informationelle Selbstbestimmung zu fördern. Eine Implementierung dieses Konzepts findet sich beispielsweise in Webbrowsern, wo der Benutzer verschiedene Einstellungen für den Besuch von Webseiten mit unterschiedlichem Datenschutzstandard festlegen kann. Der Betreiber der Webseite stellt die Information über die Privacy-Policy in „maschinenlesbarer Form“, in XML, für den Browser zur Verfügung. Dieser kann dann basierend auf den vorher getroffenen Einstellungen des Users mehr oder weniger Informationen an den Dienstbetreiber weitergeben, Cookies zulassen oder nicht, usw. Eine weitere Anwendung, die P3P-Angaben interpretiert, ist „Privacy Bird“, die von den AT&T-Forschungslabors entwickelt wurde und jetzt von einem Team an der Carnegie Mellon University weitergepflegt wird.¹³ Dieses Programm macht die Datenschutzbestimmungen des Websitebetreibers für den User sichtbar und kann vor unerwünschten Policy-Inhalten warnen.

**Ein Vogel, der für
Privatsphäre sorgt**

Der Nachteil ist, wie bei fast jeder Form der Selbstverpflichtung, dass die EndbenutzerInnen wenige Möglichkeiten haben, die nur freiwilligen Angaben des Betreibers und deren Einhaltung zu überprüfen.

¹¹ Weiner, Laurenz (2000): Gigabytes im Überfluß, <http://www.heise.de/ct/00/16/078/> (8. Jänner 2009), und Kissling, Roland (2007): Festplatten-Speicherdichte vor Verdoppelung, <http://www.computerwelt.at/detailArticle.asp?a=108653&n=3> (8. Jänner 2009). Die beiden Artikel zeigen exemplarisch, dass der Trend zu fallenden Preisen pro Megabyte bei exponentiell wachsender Speicherdichte bereits 2000 zu erkennen war und sich seitdem ungebremst fortsetzt.

¹² W3C (2002): The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, W3C Recommendation 16 April 2002, <http://www.w3.org/TR/2002/REC-P3P-20020416/> (6. Jänner 2009).

¹³ Privacy Bird: <http://www.privacybird.org/> (21. Jänner 2009).

2.5 Ubiquitous Computing

Der Begriff „Ubiquitous Computing“ beschreibt parallel zur zunehmenden Durchdringung des Alltags mit technischen Geräten vor allem die steigende Fähigkeit dieser Geräte, Daten zu erfassen, zu verarbeiten, zu speichern und weiterzugeben.¹⁴ Dadurch entsteht bei allen Vorteilen, die damit verbunden sind, eine große Bedrohung für die Privatsphäre, weil der Benutzer, so er dieser Geräte gewahr ist, nur selten die Möglichkeit hat, in deren Arbeit einzugreifen. Es geht ein Stück informationelle Selbstbestimmung verloren, und wenn die Kommunikationsfähigkeit und nicht die Sicherheit bei der Entwicklung der Geräte im Vordergrund stand, auch ein großes Stück Privatsphäre, weil die erfassten Daten dann meist leicht von Unbefugten ausgespäht werden können. Weitere gebräuchliche Begriffe für diese Entwicklung sind auch „Pervasive Computing“, oder neutraler „Ambient Intelligence“.

Ein anschauliches Beispiel für eines der oben beschriebenen smarten Geräte stellt der Prototyp des „Personal Awareness Assistant“ der Firma accenture dar, der in den accenture labs entwickelt wird.¹⁵ Dieses Gerät macht genau das, was DatenschützerInnen befürchten, wenn es um die Themen Privatsphäre und informationelle Selbstbestimmung geht: Es ist mit Kamera, Mikrofon, Kopfhörer und drahtlosen Schnittstellen zur Verbindung mit anderen Geräten ausgerüstet, ist immer aktiv, nimmt Gespräche auf, protokolliert Eingaben der BesitzerInnen, verfügt über Gesichts-, Stimm- und Spracherkennungsfähigkeiten, erfasst und speichert all das, und ist in der Lage, die Daten an andere Geräte weiterzugeben. Wird also nach kurzer Zeit vielleicht sogar besser über die Daten der BesitzerInnen und ihrer Kontakte Bescheid wissen, als diese selbst. In manchen Bereichen mag das für die BenutzerInnen angenehm sein. Aber die Vorstellung, dass ein Gerät, das wir nicht vollständig unter unserer Kontrolle haben (alleine durch die Möglichkeit von Diebstahl, Fehlkonfigurationen und technischem Versagen), unseren gesamten Alltag dauerhaft „mitschreibt“ und diese Daten verwaltet, zeigt, welche Herausforderungen im Bereich des Datenschutzes im Zusammenhang mit Ubiquitous Computing noch zu bewältigen sein werden.

Darüber hinaus geht es in so einem Szenario ja auch um die informationelle Selbstbestimmung des jeweiligen Gegenübers. Viel weitergehend als es heute mit den omnipräsenten Fotohandys möglich ist, würden wir mit diesen Geräten ja auch in die Privatsphäre anderer eindringen. Wer heute schon das Gefühl hat, das Recht am eigenen Bild¹⁶ nicht mehr wahrnehmen zu können, kann nachvollziehen, dass Strategien im Umgang mit der Technik erforderlich sind, deren Entwicklung bislang vernachlässigt wurde.

Ein weiterer Anwendungsfall (dieser hat sich bereits am Markt etabliert) sind Geräte aus dem Bereich Unified Mobile Communication/Messaging. Darunter werden mobile Geräte verstanden, die alle Kommunikationskanäle und den Online-/Offline-Status (letzteren nur bei Unified Communications) des Benut-

**Das ganze Leben wird
protokolliert**

**Immer erreichbar
und nie privat**

¹⁴ Vgl. dazu: Mattern, Friedemann/Marc Langheinrich (2001): Allgegenwärtigkeit des Computers – Datenschutz in einer Welt der intelligenten Alltagsdinge, in: Müller Günter, Martin Reichenbach (Hrsg.) (2001): Sicherheitskonzepte für das Internet, 5. Berliner Kolloquium der Gottlieb Daimler- und Karl Benz-Stiftung, S. 7-26, zit. nach: <http://www.vs.inf.ethz.ch/publ/papers/allgegenwaertig.pdf> (6. Jänner 2009).

¹⁵ accenture: Personal Awareness Assistant, http://www.accenture.com/Global/Services/Accenture_Technology_Labs/R_and_I/PersonalAssistant.htm (6. Jänner 2009).

¹⁶ Das Recht am eigenen Bild ist im § 78 des Urheberrechtsgesetzes festgeschrieben und schützt damit auch die informationelle Selbstbestimmung einzelner Personen.

zers bzw. der Benutzerin zusammenführen und verwalten. Dadurch, dass zum Beispiel auf einem aktuellen Smartphone über Telefon, E-Mail, Fax, SMS, Chat, Twitter u.v.m. kommuniziert werden kann, wird eine bessere Erreichbarkeit erwartet, die zum Beispiel in Firmen wiederum Geschäftsprozesse beschleunigen könnte. Im Gegenzug ist aber auch hier festzustellen, dass nicht nur die Kommunikationskanäle oft nicht so sicher sind, wie die AnwenderInnen denken, sondern dass die Daten, die die Endgeräte schlecht geschützt sammeln, schon viel über die BesitzerInnen aussagen können; ganz besonders trifft dies auch im Hinblick auf die Vorratsdatenspeicherung zu, weil alle Kommunikationsvorgänge, die durch so ein Gerät ja dann bei einem Provider anfallen, in Hinkunft auch dort gespeichert werden müssen.

2.6 Verteilte Systeme

Obwohl die Voraussetzungen andere sind, ergeben sich hier ähnliche Probleme wie im Bereich des ubiquitous computing. Dadurch, dass die Verarbeitung und Speicherung von Daten nicht mehr ausschließlich auf dem eigenen Rechner/Server stattfindet, können die BesitzerInnen der Daten nicht mehr nachvollziehen, wer gerade die Kontrolle über die Daten hat.

Bei verteilten Systemen werden die Datenverarbeitung und die Speicherung von Application Service Providern durchgeführt, die typischerweise im Rahmen von Outsourcing- oder Offshoring-Projekten ausgewählt und mit der Erbringung eines bestimmten Dienstes betraut werden. Für Privatanwender kann das der ISP sein, der nicht nur eine E-Mail-Adresse zur Verfügung stellt, sondern darüber hinaus Groupware-Funktionalität anbietet, indem er einen entsprechenden Server bei sich im Rechenzentrum betreibt und die Benutzung desselben als Dienst an seine KundInnen verkauft.

Wer hat gerade Zugriff auf die Daten?

Auch wenn es mit ausgelagerten Datacentern immer wieder Probleme gibt, zum Beispiel weil sie sich in einem anderen Land, unter anderer Rechtsprechung befinden, wird es etwas kritischer, wenn Application Service Provider die Daten von unterschiedlichen KundInnen verarbeiten, weil nicht nur die gesicherte Übermittlung, Verarbeitung und Speicherung zu beachten ist, sondern auch der unbefugte Zugriff anderer KundInnen vermieden werden muss. In Zukunft wird das Problem vielleicht noch an Komplexität gewinnen, wenn die Pläne bezüglich „Cloud Computing“ umgesetzt werden, an denen viele Firmen zur Zeit arbeiten. Bei dieser Art der verteilten Systeme gibt es nicht mehr nur ein Rechenzentrum für viele KundInnen, sondern viele Rechenzentren für viele KundInnen. So könnten PrivatnutzerInnen beispielsweise die Erbringung und Nutzung eines Dienstes nach Zeit bezahlen, aber keine Kontrolle mehr darüber haben, wo oder von wem die Dienstleistung erbracht wird. Das würde in der namensgebenden „Wolke“ passieren. Damit wäre es vollends unmöglich festzustellen, wer wann Zugriff auf die Daten hat. Dadurch wäre es zwar leicht, im Vergleich zur herkömmlichen Methode der Datenverarbeitung, bei der jeder Verarbeiter die dafür notwendigen Server selbst betreibt, ein großes Einsparungspotenzial zu lukrieren, allerdings ist auch zu befürchten, dass die Kontrolle der privaten oder firmeninternen Daten durch marktbeherrschende Unternehmen zunähme.

2.7 Kryptographie

Kryptographische Verfahren haben aus heutiger Sicht die Möglichkeit, die Privatsphäre zu schützen, werden dazu aber zu selten eingesetzt. Falls Quantencomputer in den nächsten Jahren wirklich Marktreife erlangen, wird zwar die Verschlüsselung von Daten, wie sie heute betrieben wird, obsolet sein, jedoch ergeben sich aus neuen technischen Möglichkeiten auch neue Verfahren für den Datenschutz.

Die Verschlüsselung und Signierung von Datensätzen kann viel dazu beitragen, die Authentizität und den Schutz der Daten zu verbessern. Ein Einsatz zur Authentifizierung von Personen und deren Kommunikation (über die digitale Signatur) wird zwar vom Staat begrüßt und ist im Konzept Bürgerkarte vorgesehen¹⁷, eine aktive Förderung von verschlüsselter Kommunikation könnte die Verbreitung stark beschleunigen, ist jedoch noch nicht zu erkennen.¹⁸ Als eine Begründung dafür wird immer wieder erwähnt, dass dann auch VerbrecherInnen in der Lage wären zu kommunizieren, ohne dass die Exekutive die Möglichkeit hätte, das zu überwachen. Dabei wird allerdings außer Acht gelassen, dass diese Möglichkeit schon besteht, und sie somit schon genutzt werden kann. Übrig bleiben nur die unbedarften AnwenderInnen, denen es zu aufwendig ist, sich mit der Technik, die noch nicht user-freundlich genug ist, auseinanderzusetzen.¹⁹ Dieser Beitrag zum Schutz der Privatsphäre wäre bei ausreichendem politischen Willen leicht zu erbringen.

**Die Verschlüsselung
verhindert Ausspähen
der Daten**

2.8 Sensortechnik

Die Weiterentwicklung der Sensortechnik und der angeschlossenen Signal- und Datenverarbeitung hat dazu geführt, dass in den letzten Jahren einige Geräte marktreif wurden, die in den Neunzigern nur als Idee oder Konzept existierten, und jetzt die Privatsphäre bedrohen.

**Augen und Ohren
überall**

Dazu zählen zum Beispiel die Terahertz-Scanner, die es ermöglichen, durch Wände zu sehen oder „Naked Machines“ zu betreiben²⁰, wie sie auf verschiedenen Flughäfen (zahlreiche große Flughäfen in den USA, Amsterdam Schip-

¹⁷ Siehe auch: A-SIT Zentrum für sichere Informationstechnologie Austria: Bürgerkarte – Vorteile für Bürgerinnen und Bürger, <http://www.buergerkarte.at/de/index.html> (6. Jänner 2009).

¹⁸ Als Ausnahme dazu muss hier festgehalten werden, dass für die bevorstehenden ÖH-Wahlen, die ein e-Voting-Testlauf werden sollen, dafür notwendige Kartenleser und die Aktivierung der eCard gratis an 10.000 StudentInnen abzugeben gewesen wären. Im geplanten Zeitraum von September 2008 bis Jänner 2009 konnten nicht einmal die Hälfte der Angebote an den Mann und die Frau gebracht werden. Quintessenz (2009): Bürgerkarte: Nicht einmal geschenkt ein Renner, <http://www.quintessenz.org/d/000100005462> (3. Februar 2009).

¹⁹ Das war es auch, was Phil Zimmermann in einer Zeit ausdrückte, als die US-Regierung über starke kryptographische Verfahren und Anwendungen Exportverbote verhängte: „If privacy is outlawed, only outlaws will have privacy.“, zit. nach: Zimmermann, Philip (1991): Why I Wrote PGP, <http://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html> (6. Jänner 2009).

²⁰ ORF-Futurezone/APA (2005): Body-Scanner entblättert Fluggäste, <http://futurezone.orf.at/stories/77077/> (8. Jänner 2009), und DerStandard.at/APA (2008a): EU-Kommission will Nackt-Scanner an Flughäfen einführen, <http://derstandard.at/?url=?id=1224256246628> (8. Jänner 2009).

hol, Nizza und im Probebetrieb London Heathrow, geplant Paris Charles de Gaulle) bereits im Einsatz sind. Im Film „Total Recall“ aus dem Jahr 1990 war das noch reine Fiktion; heute, wo der Scan oft noch freiwillig erfolgt, werden Passagiere darauf hingewiesen, dass die Alternative dazu, dass ein/e Flughafenangestellte/r jedes kleinste Detail des nackten Körpers, bis hin zu Schweißtropfen am Rücken, auf einem Monitor betrachtet, die Durchsuchung mit Hand und Metalldetektor ist, die „*never a happy story*“ sei.²¹

Das umfasst aber auch die Steuerungstechnik für unbemannte Flugdrohnen, die nicht nur zur Überwachung am Schlachtfeld sondern auch in Städten eingesetzt werden (eines von vielen Beispielen für ein Verwischen der Grenzen zwischen militärischen und polizeilichen Anwendungen).²² Weiters können Kennzeichen-Scanner Autos identifizieren (zum Beispiel Anwendung bei der sogenannten Section Control oder verschiedenen Mautsystemen), Video-Analyse-Software soll Menschen erkennen²³ und solche bemerken, die sich verdächtig verhalten (und damit auch entscheiden, was überhaupt „verdächtiges Verhalten ist“)²⁴, um Straftaten zu verhindern, und die Gesichter von Reisenden mit Datenbanken der Polizei abgleichen.²⁵

²¹ USA Today (2008): 10 airports install body scanners,
http://www.usatoday.com/travel/flights/2008-06-05-bodyscan_N.htm
(28. Jänner 2009).

Reuters (2007): Amsterdam airport deploys body-scanning machines,
<http://www.reuters.com/article/technologyNews/idUSL1569798620070515>
(28. Jänner 2009).

²² Schmid, Bernard (2007): ELSA sieht alles,
<http://www.heise.de/tp/r4/artikel/26/26560/1.html> (8. Jänner 2009).

²³ ORF-Futurezone/digital.leben (2009): Personenidentifikation fürs Fotoalbum,
<http://futurezone.orf.at/tipps/stories/1501867/>, und Lückenlose Videoüberwachung,
<http://futurezone.orf.at/tipps/stories/1502073/> (1. Februar 2009).

²⁴ Laaff, Meike (2008): Die Kamera weiß, was verdächtig ist,
<http://www.taz.de/1/politik/schwerpunkt-ueberwachung/artikel/1/was-verdaechtig-ist-sagt-die-kamera/> (1. Februar 2009).

²⁵ Fraunhofer Institut für Informations- und Datenverarbeitung (2008):
Aufklärung mit mobilen und ortsfesten Sensoren im Verbund,
<http://www.iitb.fraunhofer.de/servlet/is/18599/> (1. Februar 2009).

3 Gesellschaftliche Trends

Im Folgenden sind einige gesellschaftliche Entwicklungen der letzten Jahre aufgeführt, die auch die Privatsphäre in Österreich lebender Menschen beeinflussen. Wobei sich diese Trends entweder parallel zur entsprechenden technologischen Entwicklung herauskristallisiert haben, in einem kontinuierlichen Wechselspiel dazu stehen, oder vollkommen unabhängig von der Technik angesehen werden können.

3.1 Web 2.0

In Anknüpfung an den gleichnamigen Punkt im vorigen Kapitel (siehe Punkt 2.2) sollen hier die nicht-technischen Aspekte des Web 2.0 beleuchtet werden. Der Begriff beschreibt eine Idee hinter Internetangeboten, die durch die kumulative Wirkung kleinerer technischer Weiterentwicklungen möglich wurde. Es geht dabei um das sogenannte „Mitmachweb“, in dem man sich auf Portalseiten einer Community anschließen kann, über verschiedenste Kommunikationswege mit deren Mitgliedern in Kontakt bleiben kann; es geht um das Teilen und Verteilen von Informationen, um das erstellen von Content, um „Bürgerjournalismus“, um Mash-Ups²⁶, um das Semantic Web, um Begriffswolken und Informationsverknüpfungen. Es geht vor allem um Soziale Netze beziehungsweise Social Media, um Weblogs und Podcasts, RSS- und Atom-Newsfeeds und Twitter. Sowie um Benutzerfreundlichkeit, Mobilität und Online-Speicherplatz, sowie die Fähigkeit klassische Offline-Aufgaben überall online erledigen zu können. Es geht aber auch um Crowd-Sourcing und Cross-Media-Marketing, Social Tagging und Viral-Marketing. Das Web 2.0 lässt sich nicht scharf abgrenzen, die Ideen hinter den Angeboten, die dem Web 2.0 zuzurechnen wären, versuchen jedoch immer, zumindest vordergründig, die Interaktion mit den BenutzerInnen zu forcieren und dabei im Sinne einer Mass-Customization auf jede/n persönlich einzugehen, um das Gefühl von Akzeptanz und Gemeinschaft zu erhöhen, sowie das gesammelte Wissen der Communities zu nutzen. Die Verwendung des Begriffs und dessen Aufstieg zu einem „buzzword“ der Jahre 2005 und 2006 wurde vor allem durch Tim O’Reilly in seinem Artikel „What Is Web 2.0? Design Patterns and Business Models for the Next Generation of Software“ forciert.²⁷

Was macht das Web 2.0 aus?

Dieser Boost an Interaktivität, oder zumindest der einfachere Zugang dazu, hat zu interessanten Entwicklungen geführt. Einerseits wird erlerntes soziales Verhalten auch über die neuen Medien abgebildet, ohne dabei deren Eigenheiten zu berücksichtigen, andererseits entstehen darüber hinaus in nachfol-

²⁶ Diese Begriffe, so wie andere, werden im Glossar im Anhang dieser Arbeit erläutert.

²⁷ O’Reilly, Tim (2005): What Is Web 2.0? – Design Patterns and Business Models for the Next Generation of Software, <http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html> (6. Jänner 2009).

**Wie wird das
Web 2.0 verwendet?**

genden Generationen ganz neue Kommunikationsformen²⁸. Teilweise werden auch Regeln des zwanglosen Zusammentreffens von Communities in die reale Welt übernommen²⁹.

Durch das Übertragen bestehender Verhaltensmuster in die Welt des Internet ergeben sich für die Privatsphäre der User oft Gefahren, deren sie sich nicht bewusst sind.³⁰ Viele Soziale Netze, mit ihren Möglichkeiten Freunde „zu sammeln“, andere User als Freunde zu markieren, Nachrichten nur an diese zu verschicken usw., verleiten zu der irrigen Annahme, dass man sich da zwar halb-öffentlich aber doch irgendwie im Freundeskreis austausche. Der Unterschied besteht allerdings darin, dass einem „User“ an einem realen Stammtisch mit seinen Freunden nicht die ganze Welt sondern nur die Sitznachbarn als Mithörer lästig werden können, niemand mitschreibt, und ein Großteil der ausgetauschten Informationen dadurch bald wieder in Vergessenheit gerät, und dass der Wirt weder einer fremden Jurisdiktion unterliegt, mithört, noch die User-Daten zu Marketingzwecken an Dritte weitergibt; die Allgemeinen Geschäftsbedingungen eines Wirtshauses bewegen sich im zu erwartenden Rahmen, und man kann es benutzen ohne sich registrieren zu müssen. Das Nicht-Bewusst-Machen dieser Unterschiede auf Seiten der UserInnen führt dazu, dass ausschließlich auf finanziellen Erfolg schauende Betreiber von Web 2.0 Plattformen die Möglichkeit haben, die Privatsphäre Ihrer KundInnen hintanzustellen, wenn es um den Gewinn des Unternehmens geht.³¹ Die Daten, die die UserInnen von sich preisgeben, und zum Teil auch die Daten, die die Provider aus anderen Quellen in Erfahrung bringen können, werden gesammelt und gespeichert, um gezielt kommerziell verwertet zu werden (zum Beispiel in der Form, dass auf die jeweiligen NutzerInnen-Profile zugeschnittene Werbung eingeblendet oder zugeschickt wird)³². Abhängig von den Ge-

²⁸ Ito, Joichi (2007) bei seinem Vortrag im Rahmen der Grundrechtstagung zum Auftakt der ars electronica über den Bedeutungswandel von Kommunikation per SMS für Jugendliche, der von „share information“ zu „share their presence“ geht, und den Teilnehmern an der Kommunikation somit eher das Zusammengehörigkeitsgefühl einer Gruppe vermittelt als das Wissen um bestimmte Informationen. Der Webcast kann unter folgender Adresse angesehen werden:
<http://www.aec.at/en/festival2007/webcasts/index.asp> (6. Jänner 2009).

²⁹ Und äußern sich dort zum Beispiel als Barcamps oder Treffen von Chat-Communities an einem realen Stammtisch.

³⁰ ORF-Futurezone/dpa (2008a): Soziale Netzwerke werden unterschätzt,
<http://futurezone.orf.at/stories/1500433/> (8. Jänner 2009).

³¹ Eine ausführliche Studie über den Schutz der Privatsphäre in Sozialen Netzen findet sich hier: Fraunhofer-Institut für Sichere Informationstechnologie SIT (2008): Privatsphärenschutz in Soziale-Netzwerke-Plattformen,
http://www.sit.fraunhofer.de/fhg/Images/SocNetStudie_Deu_Final_tcm105-132111.pdf (8. Jänner 2009).

³² Als Beleg genügt es in der Regel die Allgemeinen Geschäftsbedingungen oder Datenschutzbestimmungen von verschiedenen Web 2.0-Plattformen anzusehen; zum Beispiel hier die Datenschutzrichtlinie vom 26. November 2008 von facebook.com in der deutschen Übersetzung: <http://de-de.facebook.com/policy.php?ref=pf> (6. Jänner 2009). Besonders Formulierungen wie „*Wenn du Facebook verwendest, kannst du dein persönliches Profil erstellen, Beziehungen eingehen, Nachrichten senden, nach Inhalten suchen, Gruppen gründen, Veranstaltungen erstellen, Anwendungen hinzufügen und Informationen durch verschiedene Kanäle übermitteln. Wir sammeln diese Informationen, damit wir dir diese Dienste und personalisierte Funktionen anbieten können.*“, „*Facebook kann ferner Informationen über dich aus anderen Quellen, wie Zeitungen, Blogs, Instant Messaging-Diensten und der Verwendung der Facebook-Dienste durch andere Nutzer (z. B. Foto-Markierungen), sammeln, um dir nützlichere Informationen und ein personalisierteres Erlebnis bieten zu können.*“ und „*Wir können Informationen über dich, welche wir aus anderen Quellen sammeln, zusätzlich zu denen in deinem Profil verwenden. Diese*

schäftsbedingungen und Datenschutzerklärungen der jeweiligen Betreiberfirmen haben die BenutzerInnen in manchen Fällen die Möglichkeit, zum Beispiel die Zusendung von Werbung zu untersagen. Das ändert jedoch nichts an der Speicherung der Daten an sich. Diese Datensammlungen bergen jedoch auch die Gefahr, dass sie missbräuchlich verwendet, verkauft oder veröffentlicht werden, oder aus Unachtsamkeit an die Öffentlichkeit gelangen und in weiterer Folge dazu beitragen, dass mehr Information über jeden/jede Einzelne(n) digital verfügbar sind³³.

3.1.1 Aufmerksamkeitsökonomie und Bürgerjournalismus

Wie Michael H. Goldhaber in seinem Artikel „Die Aufmerksamkeitsökonomie und das Netz“³⁴ ausführt, gerät Aufmerksamkeit, wie es ja schon von Andy Warhol in seinem Ausspruch über die 15 Minuten Berühmtheit angedeutet wurde³⁵, zu einem wichtigen, und zunehmend auch wirtschaftlich relevanten Gut. Im Licht dieser Entwicklung ist die Entstehung des Web 2.0 eine logische Konsequenz, da es damit für jeden Einzelnen einfacher wird, nach Aufmerksamkeit zu streben und zu hoffen, dass sie im Internet, bei einer bestimmten Community, gefunden werden kann. Der Betreiber der jeweiligen Plattform kann diese Sehnsucht in bare Münze verwandeln.

**Aufmerksamkeit ist
Geld wert**

Eine andere Konsequenz der stark vereinfachten Content-Produktion im Web 2.0 ist die Zunahme an Menschen, die die Aufgabe des Berichtens und Kommentierens in einer Art von Laienjournalismus übernehmen.³⁶ Einerseits findet sich auch hier der Wunsch, mit seinen eigenen Ansichten eine gewisse Berühmtheit zu erlangen, andererseits kann eine breite Meinungsvielfalt gut für eine gesellschaftliche Diskussion sein. Allerdings ist vor allem bei Professionistinnen der Zunft nach wie vor umstritten, ob dieser Bürgerjournalismus die Informiertheit der Bevölkerung verbessert, oder ob das Mehr an Information einerseits ohnedies nicht mehr aufgenommen werden kann, und andererseits die Qualität der gesamten Berichterstattung zu einem Thema durch schlecht recherchierte Artikel sinkt. Man kann sich nur wünschen, dass sich auf beiden Seiten die verantwortungsbewussten JournalistInnen durchsetzen.

*beinhalten unter anderem Zeitungen und Internetquellen wie Blogs, Instant Messaging-Dienste, Facebook-Plattformentwickler und andere Facebook-Nutzer. Wo auch immer diese Informationen verwendet werden, gestatten wir dir **normalerweise** mithilfe deiner Privatsphäre-Einstellungen anzugeben, ob du dieser Verwendung zustimmst oder ob du die Verbindung dieser Informationen mit deinem Profil einschränken möchtest (z. B. durch das Entfernen von Links für Foto-Markierungen).“ erhöhen nicht gerade das Vertrauen in einen verantwortungsbewussten Umgang mit den Kundendaten.*

³³ Heise security (2009b): Job-Börse erneut Opfer eines Datendiebstahls, <http://www.heise.de/security/Job-Boerse-erneut-Opfer-eines-Datendiebstahls--/news/meldung/122315> (1. Februar 2009).

³⁴ Goldhaber, Michael H. (1997): Die Aufmerksamkeitsökonomie und das Netz – Teil I (deutsche Übersetzung durch Florian Rötzer), <http://www.heise.de/tp/r4/artikel/6/6195/1.html> (6. Jänner 2009).

³⁵ Wikipedia-Artikel: 15 minutes of fame, http://en.wikipedia.org/wiki/Fifteen_minutes_of_fame (6. Jänner 2009).

³⁶ Niggemeier, Stefan (2006): Bürgerjournalismus – Hobby: Reporter, in: Frankfurter Allgemeine Sonntagszeitung, vom 8. Oktober 2006, Nummer 40, S. 35, zit. nach: <http://www.faz.net/s/Rub475F682E3FC24868A8A5276D4FB916D7/Doc-EAD3B9321BBBD42659CB366758B6698CF-ATpl-Ecommon-Scontent.html> (6. Jänner 2009).

**Die „Inszenierung
des Privaten in der
Öffentlichkeit“**

In vielen Fällen verquicken die AutorInnen, BloggerInnen und PosterInnen Privates mit „Weltgeschehen“ und erreichen durch die „schonungslose“ Berichterstattung über Dinge aus der eigenen Privatsphäre ein Durchlöchern derselben³⁷, weil auch hier oft das Bewusstsein für die Konsequenzen fehlt. Die Tatsache, dass das, was geschrieben wird, kaum jemals wieder zu löschen sein wird, weil es ab dem ersten Augenblick auch in den verschiedensten Archiven gespeichert wird, ist den wenigsten klar. Darüber hinaus sind die meisten BürgerjournalistInnen eventuell weniger mit Persönlichkeits- und Medienrecht vertraut und überschreiten in ihrer Berichterstattung dadurch auch leichter die Grenze zur Privatsphäre anderer.

3.1.2 Google Earth und Street View

**Satellitenaufnahmen,
ergänzt um Fotos für die
3D-Darstellung**

Google Earth und Street View³⁸ sind in den letzten Jahren immer populärer geworden; sogar am Mobiltelefon, wo das vor einiger Zeit aus technischen Gründen (wie zum Beispiel Bandbreitenbeschränkungen, aber auch fehlende Prozessorleistung und Displayauflösungen bei den mobilen Endgeräten) noch undenkbar gewesen wäre. Die einen sehen darin eine sinnvolle Hilfe bei der Urlaubsplanung oder der Orientierung unterwegs, die anderen ein Werkzeug für Einbrecher und Kriminelle, wieder andere versuchen alle „schwarzen Flecken“ auf der Landkarte zu finden, die Regierungen ausblenden lassen, um ihre geheimen Areale besser schützen zu können³⁹. Aber auch unabhängig davon, ob man sich darum sorgt, dass der Out-of-Office-Assistent vielleicht verrät, dass man auf Urlaub ist, woraufhin die EinbrecherInnen schon mal die Gegend auf Google Earth auskundschaften, stellt das Service Street View einen Eingriff in die Privatsphäre dar. Um nämlich die Bilder der Straßenzüge im Web anzeigen zu können, fahren von Google beauftragte Firmen durch die jeweilige Stadt, in jede Straße, und filmen dabei rundum vom Auto aus, in Wohnungen und Häuser hinein, und jede Person, die ins Bild kommt, ob diese das nun möchte oder nicht.⁴⁰ Die Gesichter der Personen versucht ein von Google entwickelter Bilderkennungsalgorithmus zu erfassen und unkenntlich zu machen, der sogar laut Google „nicht perfekt“ arbeitet. Der Rest, wie zum Beispiel Autokennzeichen, wird nur auf Wunsch unkenntlich gemacht.⁴¹

**Die Position jedes/jeder
Einzelnen wird erfasst**

Um festzustellen, wo das Mobiltelefon sich zum Zeitpunkt einer Abfrage befindet, können einerseits die Providerdaten über die Funkzelle, in der sich das Telefon gerade befindet, verwendet werden, was aber vor allem in ländlichen Gebieten, wo die Abstände zwischen den Sendemasten größer sind, zu ungenau wäre. Andererseits lassen sich dafür sowohl die in immer mehr Endgeräten vorhandenen GPS-Empfänger und auch die WLAN-Module verwenden. Eine Positionsbestimmung mittels GPS ist meistens problemlos möglich, jedoch verfügen nicht alle Telefone über ein GPS-Modul. Für diejenigen, die

³⁷ Im Sinne einer „Inszenierung des Privaten in der Öffentlichkeit“; vgl. dazu: Rössler, Beate (2001), S. 307ff.

³⁸ Google Earth: <http://earth.google.de/> und Google Streetview: <http://www.google.de/press/streetview/index.html> (6. Jänner 2009).

³⁹ Rötzer, Florian (2007): Bildbereinigung durch Google Earth, <http://www.heise.de/tp/r4/artikel/24/24483/1.html> (6. Jänner 2009).

⁴⁰ Heise online (2008b): Bundesdatenschützer sieht Google Street View sehr kritisch, <http://www.heise.de/newsticker/Bundesdatenschuetzer-sieht-Google-Street-View-sehr-kritisch--/meldung/112886> (6. Jänner 2009).

⁴¹ Shankland, Stephen/Stefan Beiersmann (2008): Google anonymisiert Gesichter in Street View, <http://www.zdnet.de/news/tkomm/0,39023151,39190820,00.htm> (9. Jänner 2009).

zumindest eine Wireless-LAN-Verbindung aufbauen können, gibt es in städtischen Regionen, die über eine hohe WLAN-Dichte verfügen, die Möglichkeit an Hand der im Umkreis vorhandenen Drahtlosnetzwerke zu bestimmen, wo man sich befindet. Um sich in Google Earth, oder einem beliebigen location-based-service, den eigenen Standpunkt anzeigen lassen zu können, muss der Dienstanbieter natürlich das Ergebnis der Positionsbestimmung erhalten. Dadurch lassen sich, wenn auch lückenhafter als beim Mobilfunkbetreiber, auch bei anderen Firmen Bewegungsprofile erstellen und speichern.⁴²

3.2 Vertrauen der ÖsterreicherInnen in den Datenschutz

Eine Erhebung der Firma Oekonsult zum Thema „Das Vertrauen der ÖsterreicherInnen in den Datenschutz“ zeigt, dass ein überwiegender Teil der Befragten hierzulande mit einem gewissen Unbehagen an Dinge wie den Schutz der persönlichen Daten und der Privatsphäre denkt, weil sie das unbestimmte Gefühl haben, dass das etwas sei, das außerhalb ihrer Kontrolle läge und das keinen angemessenen Schutz erfahre. Das führt aber kaum dazu, dass die Datenschutzdiskussion im Alltag stattfindet, oder sich viele BürgerInnen damit auseinandersetzen. Wobei man festhalten muss, dass sich viele schlecht informiert fühlen, nicht wissen, wo sie die relevanten Informationen bekommen, und sich wünschen, dass dieses Informationsdefizit durch geeignete Maßnahmen ausgeglichen wird.⁴³

**Kein Vertrauen in den
Datenschutz**

Eine kürzliche veröffentlichte Studie, die das Verhalten von StudentInnen, die Web 2.0-Plattformen nutzen, und deren Wissen über Datenschutz beziehungsweise Möglichkeiten der informationellen Selbstbestimmung untersucht hat, kommt unter anderem zu dem Ergebnis, dass viele vermuten, dass ihre Daten dort zu lange gespeichert werden, für Werbezwecke ausgewertet werden etc., das am Verhalten aber nur wenig ändert. Mögliche Ursachen dafür sind vor allem ein Gewöhnungseffekt, der eintritt, wenn trotz dieser Datenschutzverletzungen keine unmittelbaren negativen Konsequenzen für die eigene Person festzustellen sind, und die Tatsache, dass das Thema in der Öffentlichkeit nicht breit genug diskutiert wird, um das Problem als wirkliche Bedrohung zu empfinden.⁴⁴

⁴² Die populären Geräte iPhone und iPod der Firma Apple verwenden zum Beispiel das Wi-Fi Positioning System der Firma Skyhook Wireless Inc. Dadurch werden bei jeder Positionsbestimmung die Daten über umliegende WLANs an die Firma Skyhook geschickt. Gleichzeitig ist das aber keine sichere Methode, da schon im April des vergangenen Jahres von Forschern der ETH Zürich gezeigt werden konnte, dass sich dieses System leicht überlisten lässt, sodass dem Gerät eine falsche Position vorgespiegelt werden kann.

Tippenhauer, Nils Ole/Rasmussen, Kasper Bonne/Pöpper, Christina/Čapkun, Srdjan (2008): iPhone and iPod Location Spoofing: Attacks on Public WLAN-based Positioning Systems, <ftp://ftp.inf.ethz.ch/pub/publications/tech-reports/5xx/599.pdf> (2. Februar 2009).

⁴³ Allwinger Kristin/Joshi M.A. Schillhab (2008): Vertrauen der ÖsterreicherInnen in den Datenschutz, Juli 2008, <http://www.oekonsult.eu/datensicherheit2008.pdf> (6. Jänner 2009).

⁴⁴ Fuchs, Christian (2009): Social Networking Sites and the Surveillance Society. A Critical Case Study of the Usage of studiVZ, Facebook and MySpace by Students in Salzburg in the Context of Electronic Surveillance, http://fuchs.icts.sbg.ac.at/SNS_Surveillance_Fuchs.pdf (2. Februar 2009).

Diese Tendenzen werden auch ganz deutlich von der Eurobarometer Umfrage Nummer 225, aus dem Februar 2008, zum Thema „Datenschutz in der Europäischen Union aus Sicht der BürgerInnen“ bestätigt. So würden beispielsweise 69 % der ÖsterreicherInnen der Aussage zustimmen, dass das Datenschutzbewusstsein der BürgerInnen in Österreich niedrig sei.⁴⁵

3.3 Datenfilterung

**Wer entscheidet,
was ich sehe?**

In der Regel greifen Internetbenutzer nur auf die Marktführer im Suchmaschinen-Bereich zu, wenn Informationen gefunden werden sollen. Dadurch wird immer nur ein bestimmter Ausschnitt der online verfügbaren Informationen betrachtet. Wenn das ein Unternehmen, wie zum Beispiel Google ist, das über den Google News Service auch viele Webseiten automatisiert mit Nachrichten versorgt (was an sich schon ein Problem sein kann)⁴⁶, dann kann das einerseits der Firma nutzen, weil der User über IP-Adresse, Cookie oder Login wiedererkannt werden kann, und seine Suchabfragen sein Profil abrunden werden, und andererseits dem Kunden zum Nachteil gereichen, weil er sich nie sicher sein kann, ob Google nicht manche Treffer aus den Ergebnislisten herausgefiltert hat, wie das in einigen Ländern der Fall ist.⁴⁷

Eine Berücksichtigung kleinerer und spezialisierter Anbieter erscheint im Sinne einer Diversifikation des Informationsangebotes sinnvoll, um damit einerseits Meinungsvielfalt und Pluralismus in der Gesellschaft zu fördern, und andererseits die eigene Privatsphäre zu schützen, indem nicht alle Suchanfragen bei nur einem Anbieter mitverfolgt werden können.

⁴⁵ The Gallup Organization (2008): Flash Eurobarometer Series #225: Data Protection in the European Union – Citizens' Perceptions, http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf (4. Februar 2009).

⁴⁶ Schuler, Thomas (2008): Automatischer Absturz, <http://www.sueddeutsche.de/computer/480/310409/text/> (8. Jänner 2009).

⁴⁷ Schröder, Burkhard (2002): Google filtert, <http://www.heise.de/tp/r4/artikel/12/12948/1.html> (6. Jänner 2009).

3.4 Sicherheitsbedürfnis und Videoüberwachung

Seit den Terroranschlägen 2001 in New York und danach 2004 in Madrid und 2005 in London wird nicht nur der internationale Kampf gegen den Terrorismus beschworen, sondern parallel dazu auch ein Bedürfnis der Bevölkerung nach Sicherheit geweckt und verstärkt, das die Politik zu befriedigen versucht. Es ist allerdings fraglich, ob sich wirklich alle so unsicher fühlen, und ob die ergriffenen Maßnahmen tatsächlich zu mehr Sicherheit führen.

Ein offensichtliches Beispiel für diese Art von Maßnahmen ist Videoüberwachung, die seit 2001 drastisch zugenommen hat; in Österreich meist ohne die notwendige Genehmigung durch die Datenschutzkommission (DSK)⁴⁸. Vor allem im privatwirtschaftlichen Bereich, sei es zum Beispiel durch LokalbesitzerInnen, durch Hausverwaltungen, oder in anderen Situationen, scheint kein Gefühl für die Verhältnismäßigkeit beim Einsatz solcher Überwachungsmaßnahmen zu bestehen. Sehr schnell wird Videoüberwachung als Allheilmittel eingesetzt, weil nach wie vor an die abschreckende Wirkung einer Videokamera und die Möglichkeit einer lückenlosen Verbrechensaufklärung geglaubt wird, und der Wert auch der eigenen Privatsphäre als zu gering erachtet wird.

Wie Dietmar Kammerer in seinem kürzlich erschienenen Buch zeigt, lässt sich nicht nur belegen, dass die vor allem in Großbritannien übermäßig eingesetzte Videoüberwachung nicht den gewünschten Effekt erzielt hat⁴⁹ (wie auch schon Vertreter der englischen Polizei zugegeben haben⁵⁰), sondern dass damit, im Versuch schon vor der Begehung einer Straftat alle Verdächtigen auszufiltern, ein Wandel von einer Disziplinar- zu einer Kontrollgesellschaft vollzogen wird.⁵¹ Erstere war darauf fokussiert nach einer Gesetzesübertretung eine passende Strafe auszusprechen und durchzusetzen, wodurch zwar „nur“ bestraft wurde, das aber in der Hoffnung, damit auch abschreckende Wirkung zu erzielen, den Schaden wiedergutzumachen und/oder weitere Vergehen zu verhindern. Die Kontrollgesellschaft, in die sich viele westliche Demokratien zu verwandeln scheinen, versucht von vornherein ein so hohes Maß an Kontrolle über die BürgerInnen aufzubauen, dass möglichst viele Vergehen vor deren Ausübung vereitelt werden können. Dadurch kommt es natürlich zu einem drastischen Überwachungsdruck auf die Gesellschaft, einer kaum noch auf den intimsten Kernbereich des privaten Lebens beschränkten Privatsphäre, der Aufgabe der Unschuldsvermutung (weil es sonst ja gar keinen Grund zur Überwachung gäbe) und in weiterer Folge möglicherweise zu einer Bestrafung für etwas, das noch nicht getan wurde, jedenfalls aber zur Aufdeckung und potentiellen Diskriminierung von unkonventionellem Verhalten.⁵²

**Viele nicht genehmigte
Videoüberwachungen**

**Von der Disziplinar- zur
Kontrollgesellschaft**

⁴⁸ Im Datenschutzbericht 2005-2007 der Österreichischen Datenschutzkommission (<http://www.dsk.gv.at/DocView.axd?CobId=30637> (6. Jänner 2009)) wird eigens hervorgehoben, dass die Anfragen bezüglich Videoüberwachung stark angestiegen seien, bis dato jedoch nur 300 insgesamt gemeldet wurden, von denen wiederum nur ein kleiner Teil registriert wurde.

⁴⁹ Kammerer, Dietmar (2008), S. 74-75. Zusammenfassend lässt sich sagen, dass eine positive Beeinflussung der Kriminalitätsrate nur bei bestimmten sach- und ortsbezogenen Delikten möglich ist, und auch nur dann, wenn durch mediale Aufmerksamkeit immer wieder an deren Einsatz „erinnert“ wird. Impulsiv begangene Straftaten lassen sich grundsätzlich nicht verhindern durch den Einsatz von Kameras.

⁵⁰ ORF-Futurezone/dpa (2008b): Videoüberwachung ein „völliges Fiasko“, <http://futurezone.orf.at/stories/275884/> (6. Jänner 2009).

⁵¹ Vgl. Kammerer, Dietmar (2008), S. 131ff.

⁵² Mühlbauer, Peter (2008): Zypries und Schäuble wollen „Beziehungen“ zu verbotenen Vereinigungen unter Strafe stellen, <http://www.heise.de/tp/r4/artikel/29/29406/1.html> (2. Februar 2009); fild

Gefahr für Demokratie und Rechtsstaat

Diese Entwicklung kann als Risiko für einen demokratisch organisierten Staat gesehen werden, weil damit die Privatsphäre und in weiterer Folge auch die Freiheit des Einzelnen stark beschnitten werden. Diese Freiheit ist aber eine *conditio sine qua non* einer modernen Demokratie. BürgerInnen, die sich durch das Gefühl überwacht zu werden im Rahmen der Gesellschaft nicht frei entfalten können, sind nicht mehr in der Lage als freie, unbeeinflusste StaatsbürgerInnen zu agieren und eine freie (Wahl)Entscheidung zu treffen, was in demokratietheoretischen Überlegungen aber jeweils als unabdingbar für das Funktionieren einer Demokratie eingestuft wird.

Ebenso ist zu berücksichtigen, dass zur Eröffnung eines Ermittlungsverfahrens, das die Überwachung einzelner Personen ermöglichen würde, ein Anfangsverdacht auf Grund der Gültigkeit der Unschuldsvermutung erforderlich ist. Die teilweise Abkehr von der Unschuldsvermutung, im Sinne der Europäischen Menschenrechtskonvention (EMRK)⁵³, und das Zulassen eines jedenfalls zunächst unbegründeten Generalverdachts, der alle einschließt und dadurch die flächendeckende Überwachung sinnvoll erscheinen lässt, muss im Hinblick auf die Wahrung der Rechtsstaatlichkeit ebenfalls als bedenklich betrachtet werden.

3.5 Cyber-Crimes

Datensammlungen werden attackiert

Eine der am stärksten wachsenden Straftaten ist Identitätsdiebstahl.⁵⁴ Ein Verbrechen, das sich unmittelbar auf eine schlechte Situation des Schutzes der Privatsphäre und auf ein mangelndes Wertbewusstsein die eigenen Daten betreffend in der Bevölkerung zurückführen lässt.

Wo große Datensammlungen entstehen, weckt das Begehrlichkeiten, die oft auf kriminellem Weg gestillt werden. Identitätsdiebstahl im Sinne des schon fast als klassisch zu bezeichnenden Zahlens mit einer fremden Kreditkarte kommt in Österreich zwar nicht so häufig vor wie zum Beispiel noch in Nordamerika, wo die Zahlen mittlerweile auch bei Phishing-Angriffen auf einem sehr hohen Niveau leicht rückläufig sind.

Das Versenden von Spam, das auch dafür notwendige Ansammeln und Betreuen („herding“) von gekaperten Rechnern („Zombie-Rechnern“) in Netzwerken aus fernsteuerbaren Rechnern („Bot-Nets“) und eben Phishing-Angriffe, oft mit Hilfe von Keyloggern, sind aber auch hierzulande in steigendem

Überwachungsstaat.at (2008): Die Akte Clemens A., <http://www.ueberwachungsstaat.at/index.php?id=63195> (2. Februar 2009) und <http://www.ueberwachungsstaat.at/index.php?id=63196> (2. Februar 2009); Schattenblick (2007): Bush-Regierung schließt Tausende vom Flugverkehr aus, <http://www.schattenblick.de/infopool/politik/redakt/usa/108.html> (2. Februar 2009); Hasbrouck, Edward (2009): Recent developments in the USA in relation to the protection of travel data, <http://www.papersplease.org/wp/2009/01/15/recent-developments-in-the-usa-in-travel-data/#more-326> (2. Februar 2009).

⁵³ Art. 6 Abs. 2 der EMRK, die in Österreich im Verfassungsrang steht, besagt: „Jede Person, die einer Straftat angeklagt ist, gilt bis zum gesetzlichen Beweis ihrer Schuld als unschuldig.“

⁵⁴ Gartner Inc. (2007): Gartner Says Number of Identity Theft Victims Has Increased More Than 50 Percent Since 2003, <http://www.gartner.com/it/page.jsp?id=501912> (8. Jänner 2009).

Maße an der Tagesordnung.⁵⁵ Aktuelle Bedrohungen im Cyber-Crime-Umfeld sind nach wie vor Erpressung durch angedrohte dDoS-Attacken bei Unternehmen wie Online-Wettbüros, die vom Internetanschluss abhängig sind und in einem kurzen Zeitraum viel Geld verdienen können. Wirtschaftsspionage ist bei technologisch fortschrittlichen Unternehmen die größte Bedrohung der Informationssicherheit⁵⁶ und könnte laut einer Studie von McAfee in den kommenden Jahren auf Grund der Wirtschaftskrise weiter an Bedeutung gewinnen, weil zusätzlich zu den Bedrohungen von außen skrupellose (Ex-)MitarbeiterInnen, die sich in finanziellen Nöten befinden oder sich ungerecht behandelt fühlen, versucht sein könnten, Daten der Firma zu verkaufen. Davon wären einerseits Entwicklungsergebnisse andererseits aber auch personenbezogene Daten betroffen.⁵⁷ Bei EndanwenderInnen ist es schon seit einiger Zeit Phishing, damit verbunden die Anheuerung als Agents⁵⁸, und „normale“ Betrugs-szenarien, wie sie auch offline vorkommen, wie vorgetäuschte Gewinnspiele o. Ä.

⁵⁵ Presstext Austria (2007): USA: ID-Klau auf dem Rückzug, <https://presstext.at/pte.mc?pte=070202015> (6. Jänner 2009).

⁵⁶ ORF-Online (2006): Warnung vor Computer-Spionage, <http://salzburg.orf.at/stories/104375/> (6. Jänner 2009).

⁵⁷ McAfee (2009): Unsecured Economies: Protecting Vital Information, <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport> (2. Februar 2009).

⁵⁸ Angefangen bei Anzeigen, die wie Jobinserate aussehen, bis hin zu eBay-Auktionen wird versucht, gestohlenen Geld (meistens erhalten durch Konto-Ausräumen nach Phishing-Attacken) außer Landes zu schaffen. Überweisungen würden von den betroffenen Banken wieder rückgängig gemacht werden, sodass das Geld meistens auf das Konto eines/r Unbedarften überwiesen wird, der/die es binnen kürzester Zeit abheben und per Western Union Money Transfer o. ä. verschicken muss. Die Geschichte ist oft so erdacht, dass „irrtümlich“ zuviel Geld überwiesen wird, und der/die Betroffene sich einen kleinen Prozentsatz für seine/ihre Mühen behalten darf, wenn er/sie den Rest prompt „zurückschickt“. Dadurch können heimische Banken nur die manchmal immer noch gutgläubig handelnden Personen erreichen, meistens aber nicht die DrahtzieherInnen des Betrugs. Diese heben das Geld oft in einem entfernten Land ab, in dem es in der Regel schneller ankommt, als sich die lokale Polizei mobilisieren ließe.

4 Staatlich-politische Initiativen

Eine wichtige Quelle von Veränderungen sind Maßnahmen, die im Zuge der Terrorbekämpfung nach den bereits erwähnten Anschlägen auch in Österreich gesetzt wurden, die zu mehr Sicherheit vor allem vor diesen seltenen aber gefährlichen Bedrohungen führen sollten.

Allerspätestens zum Zeitpunkt der jedenfalls notwendigen Evaluierung der Maßnahmen muss jedoch kritisch hinterfragt werden, welche davon zu einem tatsächlichen Sicherheitsgewinn geführt haben, und inwieweit der damit in der Regel verbundene Grundrechtseingriff im Hinblick auf die Verhältnismäßigkeit der Mittel gerechtfertigt ist. Einige Methoden, wie Videoüberwachung, scheinen nur in seltenen Fällen, nur kurzfristig und nur auf Grund von medialer Aufmerksamkeit eine abschreckende Wirkung zu entfalten, sodass sehr bald nur mehr die „gefühlte Sicherheit“ als Positivum festzustellen ist. Die Herstellung oder Erhöhung eines subjektiven Sicherheitsempfindens in der Bevölkerung sollte in einem modernen Rechtsstaat allerdings nicht ausreichen, um die objektiven Eingriffe in die Grundrechte der BürgerInnen zu rechtfertigen. In Untersuchungen konnte auch gezeigt werden, dass die Zustimmung zu Videoüberwachung in der Bevölkerung dann hoch ist, wenn sich die BürgerInnen unsicher fühlen, und niedrig, wenn das subjektive Sicherheitsempfinden hoch ist. Sich unsicherühlende Befragte waren aber sogar beunruhigter, wenn die Videoüberwachung bemerkt wurde, als wenn sie ihnen nicht bewusst war, weil das als Indiz dafür gewertet wurde, dass es eine wirklich unsichere Gegend sein müsste, wenn Kameras zur Überwachung installiert werden.⁵⁹

An bestimmten Beispielen lässt sich auch zeigen, dass diese Möglichkeiten, nachdem sie einmal zur Verfügung gestellt wurden, immer wieder für andere Ermittlungen zweckentfremdet, weil nicht der Intention des Gesetzgebers entsprechend, ausgenutzt wurden, oder in Fällen, in denen die Anwendung von Anti-Terror-Maßnahmen als überschießend bezeichnet werden muss, weil das zu bekämpfende Vergehen in keinem Verhältnis zu den eingesetzten Mitteln steht.⁶⁰

**Nur Gefühlte Sicherheit,
oder mehr?**

⁵⁹ Kammerer, Dietmar (2008), S. 77ff.

⁶⁰ Rötzer, Florian (2008a): Ausbreitung der zur Terrorbekämpfung eingeführten Überwachung in den Alltag, <http://www.heise.de/tp/blogs/8/119371> (8. Jänner 2009), Rötzer, Florian (2008b): Vom allgemeinen Nutzen der Antiterrorgesetze, <http://www.heise.de/tp/r4/artikel/29/29057/1.html> (8. Jänner 2009), Whitehead, Tom (2008): Town halls ordered to stop using terror laws to catch dog-foulers, <http://www.telegraph.co.uk/news/newsttopics/politics/lawandorder/3485716/Town-halls-ordered-to-stop-using-terror-laws-to-catch-dog-foulers.html> (8. Jänner 2009) und Überwachungsstaat.at (2008): Die Akte Clemens A., <http://www.ueberwachungsstaat.at/index.php?id=63195> (2. Februar 2009) und <http://www.ueberwachungsstaat.at/index.php?id=63196> (2. Februar 2009).

4.1 Österreich

Einige Änderungen seit 2000 von öffentlicher Seite, die eine Auswirkung auf die Privatsphäre haben:

4.1.1 Telekommunikationsgesetz 2003 (TKG 2003)

Verbotener Spam Neben der Regelung des Betriebs von Telekommunikationsanlagen sorgt das TKG 2003 für einen zumindest theoretischen Schutz der Verbraucher vor SPAM. § 107 untersagt Anrufe, Faxe und E-Mails, wenn es sich dabei um unerwünschte Werbenachrichten handelt.⁶¹

4.1.2 Sicherheitspolizeigesetz (SPG)⁶²

Keine unabhängige Kontrolle für Eingriffe der Polizei in die Privatsphäre

Seit Inkrafttreten der Novelle zum Sicherheitspolizeigesetz Ende 2007 ist es der Polizei nun erlaubt, ohne richterliche Anordnung (mit Hilfe der Provider) die Handystandort-Daten zu ermitteln und Auskunft über Name, Anschrift und Teilnehmernummer zu einer bestimmten IP-Adresse zu verlangen. Weiters wurde die Errichtung einer Sexualstraftäter-Datei beschlossen.⁶³

Dadurch ist es nicht nur möglich, sehr weitgehende Eingriffe in die Privatsphäre durchzuführen, sondern es fehlt auch jede Art von unabhängiger Kontrolle, zum Beispiel durch Richter.

Bereits die Art der Beschlussfassung dieses Gesetzes löste in weiten Teilen der Bevölkerung Unmut aus: Es wurde am Ende einer 15 Stunden dauernden Sitzung des Nationalrates, der letzten im Jahr 2007, am späten Abend beschlossen, ohne, wie es sonst üblich gewesen wäre, vorher den zuständigen Innenausschuss des Parlaments damit zu befassen. Darüber hinaus wurden von den Parlamentsfraktionen der Regierungsparteien kurz vor der Abstimmung noch Änderungsanträge eingebracht, die die Befugnisse der Polizei gegenüber der Gesetzesvorlage stark ausweiteten.⁶⁴

Als erstes Ergebnis der Gesetzesnovelle konnte nach einer diesbezüglichen parlamentarischen Anfrage festgestellt werden, dass die Polizei in den ersten vier Monaten (1. Jänner bis 30. April 2008) 3.863 Auskunftsverlangen gemäß § 53 Abs. 3a gestellt hat. Dieser erlaubt es den Sicherheitsbehörden bei „Gefahr im Verzug“ die entsprechenden Daten von den Providern einzufordern. Das sind annähernd 32 Auskunftsbegehren pro Tag, die keiner unabhängigen (richterlichen) Kontrolle unterliegen.⁶⁵

⁶¹ Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 – TKG 2003)

⁶² Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz – SPG)

⁶³ DerStandard.at/APA (2008b): Sicherheitspolizeigesetz im Eiltempo und ohne Diskussion beschlossen, <http://derstandard.at/?url=/?id=3141872> (8. Jänner 2009).

⁶⁴ Sokolov, Daniel (2007): Neues österreichisches Sicherheitspolizeigesetz in der Kritik, <http://www.heise.de/newsticker/Neues-oesterreichisches-Sicherheitspolizeigesetz-in-der-Kritik-/meldung/100667> (8. Jänner 2009).

⁶⁵ ORF-Futurezone (2008): Polizei: 32 SPG-Abfragen pro Tag, <http://futurezone.orf.at/stories/288198/> (2. Februar 2009).

4.1.3 **Bildungsdokumentationsgesetz⁶⁶**

Das Bundesgesetz über die Dokumentation im Bildungswesen schreibt vor, dass Daten über den Bildungsweg der einzelnen BürgerInnen in der Regel bis zu 60 Jahre nach dem letzten Eintrag einer Bildungseinrichtung ins Register gespeichert werden. Pro Datenart kann hier das Unterrichtsministerium per Verordnung unterschiedliche Speicherzeiträume festlegen. Das wird damit begründet, dass diese Information für die Berechnung der Pension erforderlich sei⁶⁷, andererseits soll der Personenbezug nach 20 Jahren gelöscht werden (§ 8 Abs. 6 Z 2). Verschlüsselt (nicht anonymisierend) werden die Daten nur in der Gesamtevidenz, mit deren Führung die Statistik Österreich betraut ist, nicht jedoch in den Datenbanken der einzelnen Bildungseinrichtungen. Weiters ist erst für Ende 2009 geplant, dass dem Nationalrat ein Bericht über Alternativen zur Verwendung der Sozialversicherungsnummer als „bildungsspezifisches Personenkennzeichen“ vorlegt wird (§ 14 Abs. 5).

**Auch
Bildungseinrichtungen
wissen alles**

4.1.4 **Elektronischer Gesundheitsakt (ELGA)**

Bis 2012 sollen die Basiskomponenten der ELGA-Infrastruktur eingerichtet sein. Ziel ist es, in diesem System möglichst viele Informationen über alle PatientInnen zu speichern, um den Wissensaustausch unter den Gesundheitsdiensteanbietern zu verbessern und mehr Transparenz in der Behandlung zu erreichen. Damit handelt es sich letztendlich um ein Register mit den Links zu sensiblen personenbezogenen Daten fast aller ÖsterreicherInnen (die Daten selbst sollen jeweils dort gespeichert werden, wo sie anfallen).

**Der Zugriff auf die
Gesundheitsdaten über
ein zentrales Register**

Das wirft natürlich die Frage nach der Sicherheit auf. Lange war nicht klar, wer auf die Daten zugreifen können sollte, ob damit nicht das Arztgeheimnis und damit die Vertrauensbasis zwischen Arzt/Ärztin und PatientInnen untergraben werde, und was alles in der Datenbank gespeichert werden sollte. Nach dem aktuellen Plan hat die Arbeitsgruppe ELGA dieses Problem gelöst, indem die PatientInnen die informationelle Selbstbestimmung bis ins kleinste Detail ausüben können: Die PatientInnen sollen entscheiden, welche Daten darin gespeichert werden, und wer darauf Zugriff haben soll. Grundsätzlich ein guter Gedanke – einerseits entscheiden diejenigen, deren Daten gespeichert werden, andererseits ist die ARGE ELGA das Problem los, sich überlegen zu müssen, wo die Grenze zwischen Komfort und Schutz der Privatsphäre verläuft.⁶⁸

Vieles bleibt dabei jedoch noch ungelöst – zum Beispiel die Frage, wieviel ich meiner Versicherung verraten muss, um den Versicherungsschutz nicht zu verlieren. Wird die Strafandrohung ausreichen, um alle Arbeitgeber davon abzuhalten, ihre Angestellten zur Preisgabe der Daten zu drängen? Werden die technischen Sicherheitsvorkehrungen in dem Fall so hoch sein, dass es zu keinem Diebstahl der Daten kommt? Wird es möglich sein, eine/n Zugriffsberechtigte/n zu finden, der/die bereit ist, gegen Geld Daten aus dem System herauszuschleusen? Heißt „Speicherung dort, wo die Daten anfallen“, dass, so

**Viele ungelöste
Probleme, großes
Missbrauchspotenzial**

⁶⁶ Bundesgesetz über die Dokumentation im Bildungswesen, beschlossen 2002, zuletzt novelliert 2008.

⁶⁷ Landesschulrat Niederösterreich (2005): Das Bildungsdokumentationsgesetz (BilDokG) – Häufig gestellte Fragen und Antworten, <http://bsr.lsr-noe.gv.at/gf/verordnungen/2005/0512/bl3c.pdf> (3. Februar 2009).

⁶⁸ Hack, Günter (2008): Der ELGA-Fahrplan, <http://futurezone.orf.at/stories/276191> (8. Jänner 2009).

wie es bei vielen Krankenhausinformationssystemen gängige Praxis ist, die Sicherheitsvorrichtungen dadurch umgangen werden, dass sich am Beginn des Arbeitstages jemand mit möglichst vielen Rechten am System anmeldet, und danach alle MitarbeiterInnen mit diesem Account arbeiten; somit zumindest auf die selbst eingestellten Daten deutlich mehr Zugriff haben, als der Patient das wollte? Wird jede der datenspeichernden Gesundheitseinrichtungen in der Lage sein, die Daten entsprechend zu schützen? Wird man Behandlungen von der Krankenkasse bezahlt bekommen, wenn man sie nicht eintragen lassen will? Ist der Zugriff mittels Bürgerkarte bei deren geringer Verbreitung praktikabel? Braucht das AMS auch diese Daten?

Die zentrale Verfügbarkeit dieser Informationen könnte dazu führen, dass zum Beispiel Kreditinstitute wissen wollen, wie es um die Gesundheit potentieller KreditnehmerInnen bestellt ist. Vielleicht wollen zukünftige Arbeitgeber dann vom Betriebsarzt/-ärztin, dass er/sie „schnell und unbürokratisch“ überprüft, ob „mit dem/der Neuen eh alles in Ordnung sei“, oder nachschaut, warum verschiedene KollegInnen schon wieder im Krankenstand seien. Eventuell sind auch Versicherungen an diesen Daten interessiert, um die Versicherungsleistung und Prämien soweit an die KonsumentInnen anzupassen, dass einerseits das Geschäftsergebnis besser aussieht und andererseits niemand für etwas zahlt, das er/sie nicht braucht – was im Umkehrschluss auch hieße, dass das ein weiteres Gebiet wäre, auf dem ein bisher solidarisiertes Risiko in Zukunft auf den/die Einzelne/n abgewälzt werden könnte.

4.1.5 e-Government

Sehr langsame Durchsetzung von e-Government- Anwendungen

Durch das im Jahr 2004 beschlossene und zuletzt 2008 novellierte E-Government-Gesetz⁶⁹ wurde die rechtliche Grundlage für den elektronischen Datenverkehr mit Behörden geschaffen, was dann noch weitere Änderungen, wie zum Beispiel im Zustellgesetz nach sich zog. Allgemein lässt sich feststellen, dass die Rahmenbedingungen zwar geschaffen wurden, aber abgesehen von wenigen sehr speziellen Angeboten (zum Beispiel „Finanz online“ oder „help.gv.at“) von den BürgerInnen noch nicht akzeptiert wurden. Wobei ein Grund dafür das klassische „Henne-Ei-Problem“ sein könnte: Solange der Zugang so kompliziert und die Anwendungsmöglichkeiten so selten sind, will niemand auf den elektronischen Datenverkehr umsteigen; und solange nicht genügend UserInnen das System nutzen, werden auch weitere Anwendungen nicht, oder nur zögerlich entwickelt.

Eine Pseudonymisierung, die die Verknüpfung verschiedener Daten zu einer Person über unterschiedliche staatliche Anwendungsbereiche hinweg verhindern soll, ist die bereichsspezifische Personenkennzahl (bPK). Für die Erzeugung wird die Stammzahl verwendet, die sich aus der ZMR-Zahl ableiten lässt. Die Aufgabe der Berechnung und Verwaltung der Stammzahlen im Stammzahlregister hat die Datenschutzkommission, was den Nachteil hat, dass sie sich bei Unregelmäßigkeiten in dem Bereich selbst zu kontrollieren hätte.⁷⁰

Fehlende Gewaltenteilung

Wie Peter Parycek bereits 2006 auf der Konferenz TA'06 ausführte, muss die Gewaltenteilung auch im e-Government umgesetzt werden, um weiterhin eine unabhängige Kontrolle zu gewährleisten. Vorschläge dazu wären die Ein-

⁶⁹ Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-GovG).

⁷⁰ ARGE DATEN (2005): EU-Beschwerde – (Teil)Erfolg für die ARGE DATEN, http://www2.argedaten.at/session/anonym545032xpxjao612569.E42_INP.html (3. Februar 2009).

führung einer Kontrollinstanz, analog zum Rechnungshof, die die Datenverarbeitung des Bundes überprüft, sowie die Verschiebung der Registerverwaltung in den Bereich der Jurisdiktion.⁷¹

Im Rahmen der e-Government-Initiative wurde auch das Konzept „Bürgerkarte“ eingeführt, das unter anderem die elektronische Signatur und die Authentifizierung bei elektronischen Behördenwegen ermöglichen soll. Auch hier ist zu bemerken, dass die verschiedenen Umsetzungen unter geringer Standardisierung und mangelnder Benutzerfreundlichkeit leiden, was einer großen Verbreitung bisher im Wege stand. Nähere Details dazu finden sich auch im eID-Länderbericht für Österreich⁷².

4.1.6 e-Voting

In der Hoffnung die Wahlbeteiligung bei den ÖH-Wahlen zu verbessern und einen Testlauf für kommende Nationalratswahlen durchführen zu können, soll es bei der für das Frühjahr 2009 bevorstehenden ÖH-Wahl erstmals möglich sein, die Stimme über das Internet abzugeben. Es werden zwar hitzige Diskussionen zu dem Thema geführt, aber es scheint, als würde vor einem Konsens schon der Wahltermin kommen.⁷³

Grundsätzlich besteht bei allen Formen von e-Voting das Problem, dass Manipulationen viel schwerer als auf dem Papier nachzuweisen sind, die Übertragung und Auswertung der Stimmen intransparenter ist, es teurer ist als das bestehende Papier-System, und vor allem in Zeiten der Vorratsdatenspeicherung bei Wahlen über das Internet eine Zusammenführung von Verkehrsdaten und Wahldaten zuverlässig verhindert werden muss. Interessant ist der Fokus auf e-Voting in Österreich auch deshalb, weil er zu einem Zeitpunkt einsetzt, zu dem andere Staaten, wie die Niederlande und Irland, die e-Voting-Systeme bereits eingeführt hatten, diese wieder abgeschafft haben.⁷⁴

**Trend zu riskantem
Wahlverfahren**

4.2 Europa

In einem zusammenwachsenden Europa, und als Mitglied der Europäischen Union, wirken sich viele auf europäischer Ebene getroffenen Entscheidungen auch auf Österreich aus – ein paar Beispiele dazu im Folgenden.

4.2.1 Stellungnahmen der Article 29 Working Party

Das Gremium, das die Datenschutzrichtlinie der Europäischen Union interpretiert, die Article 29 Working Party, setzt sich aus den VertreterInnen der Datenschutzbehörden der einzelnen Mitgliedsstaaten zusammen und hat in

**Datenschutz auf
europäischem Niveau**

⁷¹ Parycek, Peter (2006): Staatliche Informationsgebarung – Gläserne Bürger im gläsernen Staat?, <http://www.oeaw.ac.at/ita/ta06/Parycek.pdf> (3. Februar 2009).

⁷² Aichholzer, Georg/Strauß, Stefan (2009).

⁷³ Hack, Günter (2009): Ministerium kontert E-Voting-Gegner, <http://futurezone.orf.at/stories/1502109/> (3. Februar 2009).

⁷⁴ Vorträge von Wolter Pieter und von Rop Gonggrijp auf der Conference for Computers, Privacy and Data Protection (CPDP) 2009, <http://www.cpdpconferences.org/presentations.html> (3. Februar 2009).

den letzten Jahren immer wieder Unklarheiten ausgeräumt und im Zuge dessen viele datenschutzrelevante Stellungnahmen abgegeben⁷⁵. Zu ihren Aufgaben gehört auch die Beratung der Europäischen Kommission in Fragen des Datenschutzes und der Rechte und Freiheiten natürlicher Personen im Zusammenhang mit der Verarbeitung personenbezogener Daten. In Ihrem Arbeitsprogramm für den Zeitraum 2008 bis 2009 sollen unter anderen folgende Kernthemen (zusätzlich zu direkten Anfragen) behandelt werden: verbesserte Anwendung der europäischen Datenschutzrichtlinie, Gewährleistung des Datenschutzes im internationalen Datenverkehr und Gewährleistung des Datenschutzes im Bezug auf neue Technologien.⁷⁶

Im Folgenden zwei Beispiele zu speziellen (Suchmaschinen) und grundsätzlichen Fragen (Was sind personenbezogene Daten?):

**Stellungnahme 1/2008 zu
Datenschutzfragen im Zusammenhang mit Suchmaschinen⁷⁷**

**Wichtige
Entscheidungen**

Besonders interessant im Hinblick auf Anbieter wie Google, die ihren Benutzern verschiedenste Dienste anbieten, findet sich dort folgender Absatz:

„Eine übergreifende Korrelation von Daten aus verschiedenen Diensten des Suchmaschinenbetreibers darf nur durchgeführt werden, wenn die Einwilligung des Benutzers für diesen speziellen Dienst vorliegt.“⁷⁸

Stellungnahme Nr. 4/2007 zum Begriff der personenbezogenen Daten⁷⁹

Hier werden einige Beispiele dazu gebracht, welche Daten als personenbezogen einzustufen sind, aber auch unter welchen Umständen. Es kann Daten geben, die nur in einem bestimmten Kontext personenbezogen sind.

Jedenfalls personenbezogen ist die IP-Adresse eines Internetanschlusses, auch wenn es sich um eine dynamisch vergebene Adresse handelt, sofern sich diese nicht zum Beispiel auf den Anschluss in einem Internet-Cafe bezieht, das keine Benutzerregistrierung vorsieht. Das wurde schon 2000 festgelegt⁸⁰, wird in diesem Papier aber noch einmal erwähnt und an Hand von Beispielen erläutert.

⁷⁵ Die hier zu finden sind: Art. 29 Datenschutzgruppe, http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_de.htm (2. Februar 2009).

⁷⁶ Artikel 29 Datenschutzgruppe (2008): Arbeitsprogramm 2008-2009, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp146_de.pdf (4. Februar 2009).

⁷⁷ Art. 29 WP (2008): Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_de.pdf (8. Jänner 2009).

⁷⁸ Ebenda, S. 30.

⁷⁹ Art. 29 WP (2007): Stellungnahme Nr. 4/2007 zum Begriff der personenbezogenen Daten, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_de.pdf (8. Jänner 2009).

⁸⁰ Art. 29 WP (2000): Stellungnahme 7/2000 zum Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp36de.pdf (8. Jänner 2009).

4.2.2 Vorratsdatenspeicherung

Unter dem Begriff der Vorratsdatenspeicherung wird die Umsetzung der Richtlinie 2006/24/EG verstanden, die die verdachtsunabhängige Speicherung sämtlicher Telekommunikationsverkehrsdaten (Mobil- und Festnetztelefonie, Internetnutzung, SMS, E-Mail, VoIP und dergleichen) vorsieht.⁸¹ Ursprünglich wurde für die 2006 beschlossene Richtlinie ein Umsetzungszeitraum von 18 bis 36 Monaten eingeräumt. In einigen europäischen Staaten, wie etwa Deutschland, wurde die Richtlinie schon in nationales Recht übernommen. Österreich hat die Umsetzung vorerst ausgesetzt, um das Urteil über die beim EuGH eingebrachten Klagen gegen die Richtlinie abzuwarten. Einerseits hat Irland eine Klage wegen eines Verfahrensfehlers beim Beschluss der Richtlinie eingebracht, der sich die Slowakei angeschlossen hat.⁸² Andererseits haben über 40 verschiedene Organisationen im Frühjahr 2008 gemeinsam eine Klage gegen die Richtlinie beim EuGH eingelegt, weil die Richtlinie die Privatsphäre verletze und damit gegen Artikel 8 der EMRK verstoße. Zumindest im ersten Verfahren ist in Kürze ein Urteil zu erwarten: die Verkündung wurde für den 10. Februar 2009 anberaumt. Danach werden sich vermutlich die weiteren Schritte in den verschiedenen Nationalstaaten richten.⁸³

Die Speicherung der Verbindungs- und Standortdaten, die explizit keine Inhaltsdaten enthalten soll, ist aus vielen Gründen problematisch. Oft können Verbindungsdaten von Inhaltsdaten nicht eindeutig getrennt werden, weil zum Beispiel aufgerufene Internetadressen leicht Rückschlüsse auf die angesehenen Inhalte zulassen.

Auch wenn es vorläufig geplant ist, die gespeicherten Daten nur zur Verfolgung von Vergehen, die mit mindestens 3 Jahren Haft bedroht sind, einzusetzen, ergibt sich vor allem aus dem großen Missbrauchspotenzial⁸⁴ eine enorme Gefahr für die Gesellschaft und die BürgerInnen, die in keinem Verhältnis zum möglichen Sicherheitsgewinn steht, da anzunehmen ist, dass diejenigen, die tatsächlich kriminelle Machenschaften verbergen wollen, die Vorratsdatenspeicherung unterlaufen werden.⁸⁵

Der Gläserne Mensch entsteht

⁸¹ Richtlinie 2006/24/EG des Europäischen Parlaments und Rates über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, <http://register.consilium.eu.int/pdf/de/05/st03/st03677.de05.pdf> (3. Februar 2009).

⁸² Heise online (2006): Irland und die Slowakei legen Klage gegen Vorratsdatenspeicherung ein, <http://www.heise.de/newsticker/Irland-und-die-Slowakei-legen-Klage-gegen-Vorratsdatenspeicherung-ein--/meldung/73751> (3. Februar 2009).

⁸³ Golem.de (2009): EuGH gibt Urteilstermin für Vorratsdatenspeicherung bekannt, <http://www.golem.de/0901/64684.html> (3. Februar 2009); Heise online (2008c): Verhandlungen zur Vorratsdatenspeicherung in Luxemburg und Dublin, <http://www.heise.de/newsticker/Verhandlungen-zur-Vorratsdatenspeicherung-in-Luxemburg-und-Dublin--/meldung/110307> (3. Februar 2009).

⁸⁴ ORF-Futurezone/APA (2008c): Datenhandel „nicht kontrollierbar“, <http://futurezone.orf.at/stories/317153/> (3. Februar 2009).

⁸⁵ Heise online (2007d): Vorratsdatenspeicherung für eine 0,006 Prozentpunkte höhere Aufklärungsquote, <http://www.heise.de/newsticker/Vorratsdatenspeicherung-fuer-eine-0-006-Prozentpunkte-hoehere-Aufklaerungsquote--/meldung/92746> (3. Februar 2009); Heise online (2007e): Aufregung um Vorratsdatenspeicherung in Österreich, <http://www.heise.de/newsticker/Aufregung-um-Vorratsdatenspeicherung-in-Oesterreich--/meldung/90066> (3. Februar 2009).

**Wichtige Funktionen in
der Gesellschaft sind
bedroht**

Im Gegenzug werden aber das Anwalts- und Ärztegeheimnis gefährdet, InformantInnen, sogenannte Whistle Blower, die eventuell rechtswidriges Vorgehen in der eigenen Organisation aufdecken würden, oder darüber JournalistInnen berichten könnten, laufen Gefahr, ihre Anonymität zu verlieren. Wirtschaftsspionage wird stark vereinfacht, da aus den gesammelten Daten sowohl ein Rückschluss auf die Geschäftstätigkeit möglich wird, als auch Anbahnungen von Firmenzusammenschlüssen und Übernahmen erkannt werden können. Es lassen sich lückenlose Sozialprofile aller BürgerInnen erstellen, weil aus Art, Zeitpunkt, Ort und Häufigkeit der Information über Methoden der Mustererkennung in kürzester Zeit ermittelt werden kann, wer die Familienmitglieder, ArbeitskollegInnen, berufliche Kontakte, FreundInnen und FreizeitpartnerInnen sind.

Die Umsetzung in Österreich wird zeigen, wo die Prioritäten der Politik liegen. In der Zwischenzeit erging ein zweites Mahnschreiben der EU-Kommission an Österreich, weil die Verkehrsdaten aus der Telefonie bereits seit September mit gesetzlicher Grundlage gespeichert werden müssten (die Speicherung der Internet-Verkehrsdaten ist erst ab März 2009 erforderlich).⁸⁶

4.2.3 Passagierdatenweitergabe

Nach den Terroranschlägen vom 11. September 2001 wurden in den USA eine Reihe von Gesetzen und Regelungen erlassen, die unter anderem Fluggesellschaften bei Flügen aus den, in die und durch die Vereinigten Staaten vorschreiben, Daten über Passagiere und Flugpersonal an das amerikanische Heimatschutzministerium weiterzugeben. Im Jahr 2004 einigte sich die Europäische Union mit der Regierung der USA auf ein Übereinkommen, das die Regeln für diese Datenübermittlung fest schrieb. In weiterer Folge wurde diese Vereinbarung vom Europäischen Gerichtshof 2006 jedoch für nichtig erklärt und musste neu verhandelt werden.

**Was man wissen sollte,
wenn man
in die USA reist**

Nach der Neuregelung der Passagierdatenweitergabe an die USA, die unter anderem auch vorsieht, dass die Daten bereits vor dem Abflug übermittelt werden, damit das amerikanische Heimatschutzministerium seiner Ansicht nach riskante Fluggäste noch ausfiltern kann, bevor die Maschine startet, dass die Daten zumindest 15 Jahre gespeichert werden können, und dass sie an andere Behörden (auch in Drittstaaten) weitergegeben werden dürfen⁸⁷, plant der EU-Justizkommissar Frattini nun ein vergleichbares System in Europa. Allerdings kritisierte schon 2007 das Europäische Parlament das Verhandlungsergebnis mit den USA, da das Abkommen kein „angemessenes Niveau“ für den Schutz der Fluggastdaten enthalte.⁸⁸

⁸⁶ ORF-Futurezone/APA (2008b): Zweites EU-Mahnschreiben an Österreich, <http://futurezone.orf.at/stories/308589/> (3. Februar 2009).

⁸⁷ Artikel 29 Datenschutzgruppe (2007): Stellungnahme 2/2007 zur Information von Fluggästen über die Übermittlung von PNR-Daten an amerikanischen Behörden, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp151_de.pdf (4. Februar 2009).

⁸⁸ Die Presse/APA (2007): EU-Parlament kritisiert Flug-Abkommen mit USA, <http://diepresse.com/home/politik/aussenpolitik/316642/index.do> (3. Februar 2009).

5 Privatwirtschaftliche Anwendungen

Zahlreiche Bedrohungen der Privatsphäre kommen auch aus dem privatwirtschaftlichen Bereich. Es ist in den letzten Jahren zu beobachten, dass sowohl die Anzahl der Datensammlungen, als auch deren Größe zunimmt. Für viele Unternehmen ist es selbstverständlich, im Sinne eines Customer Relationship Management, Profile ihrer KundInnen anzulegen und zu pflegen. Damit sollen die Wünsche der KundInnen erahnt beziehungsweise erfüllt werden, bevor diese die Möglichkeit haben, sie woanders zu befriedigen.

Der amerikanische Retail-Konzern Walmart ist schon seit der Mitte der Neunziger Jahre des vergangenen Jahrhunderts in der Lage über Auswertungen des Konsumverhaltens die Lebenssituation seiner StammkundInnen zu beurteilen. Mit einer Wahrscheinlichkeit von 70 % konnte schon damals festgestellt werden, ob der- oder diejenige alleine oder mit anderen gemeinsam lebt, eine Beziehung führt, heiraten wird, wann das erste Kind kommt, in die Schule eintritt usw. Die Werbung, der Einkauf, die Angebote wurden daraufhin personalisiert und optimiert. Wenn man sich als Kunde/Kundin so entwickeln will, wie Walmart das vorsieht, ist das natürlich eine hervorragende Sache. Allerdings bedeutet dies auch, dass das Angebot und damit die Wahlfreiheit einseitig eingeschränkt werden, und die Bedürfnisse viel gezielter gelenkt werden, als das durch herkömmliche Werbung möglich ist.

Die Telekomfirmen hatten auf Grund der Natur der Dienstleistungen, die sie anbieten, schon immer die Möglichkeit festzustellen, wie die sozialen Verknüpfungen zwischen den BürgerInnen aussehen. Durch die Vorratsdatenspeicherung werden sie nun noch dazu verpflichtet diese Daten über einen längeren Zeitraum zu speichern (siehe auch Punkt 4.2.2). Auf Grund des Kommunikationsverhaltens und des Bewegungsprofils ist es ein leichtes mit Mitteln der Mustererkennung festzustellen, ob jemand in einer Beziehung lebt, welche Telefonnummer den Eltern gehört, welche dem Arbeitgeber usw.

Suchmaschinenbetreiber sind in der Lage an Hand der Suchabfragen Rückschlüsse auf die Probleme (zum Beispiel durch die Suche nach bestimmten Krankheitssymptomen oder rechtlicher Beratung), die Interessen und die Konsumgewohnheiten aller NutzerInnen zu ziehen. Bei großen Portalen gibt es nicht nur die Möglichkeit über Cookies oder IP-Adressen jemand wiederzuerkennen, sondern oft werden Dienstleistungen (zum Beispiel Webmail) angeboten, die eine Registrierung und ein Log-In erforderlich machen. Im Fall von Google werden dann auch noch die E-Mails, die über das angebotene Webmail verschickt und empfangen werden, automatisiert nach bestimmten Begriffen gescanned, um passende Werbung dazu einblenden zu können.

Kreditschutzverbände und andere Firmen, die Informationen über die wirtschaftlichen Umstände von Einzelpersonen und Firmen sammeln, haben damit oft einen großen, direkten Einfluss auf das Leben des/der Einzelnen. Viele Online-Shops, Telekom-Provider und Banken benutzen diese Register, um eine Bonitätsprüfung ihrer potentiellen Kunden vor dem Abschluss eines Geschäfts durchzuführen. Ein falscher Eintrag in einer derartigen Datenbank führt leicht dazu, dass ein notwendiger Kredit nicht bewilligt wird, die Person kein Mobiltelefon, oder keinen Mietvertrag erhält.

All diese Informationen müssten eigentlich sicher verarbeitet und aktuell gehalten werden. Es passiert aber immer wieder, dass falsche oder veraltete Informationen gespeichert werden, und zum Teil in die Hände Unbefugter gelangen. Diese benutzen, wie schon ausgeführt, die Daten dann für Identitätsdiebstahl und/oder verkaufen sie an Adresshändler weiter, die daraus wieder

**Immer mehr
Datensammlungen
und allumfassende
Kundenprofile**

**Die Fragen
verraten uns**

**Keine sichere
Datenverarbeitung**

Profile zusammenstellen können, derer sich Unternehmen in weiterer Folge bedienen, um zum Beispiel Direct-Marketing, oder One-2-One-Marketingaktionen gezielter durchführen zu können.

Auch die meisten ArbeitgeberInnen haben es sich in den letzten Jahren zur Gewohnheit gemacht, alle Informationen im Internet zu sammeln, die über bestimmte BewerberInnen für eine Position verfügbar sind. Auch hier kann es sich nachteilig auswirken, wenn gute FreundInnen die Bilder von lang vergangenen Jugendsünden ins Internet gestellt haben. Darüber hinaus wurden in letzter Zeit Fälle von MitarbeiterInnenkontrolle bekannt, die weit über das hinausgehen, was einerseits verdachtsunabhängig und andererseits von Privaten ermittelt werden darf ohne die Privatsphäre der MitarbeiterInnen zu verletzen.⁸⁹

**Urheberrechts-
verletzungen wird mit
Anti-Terror-Maßnahmen
begegnet**

Ein spezieller Fall ist der Kampf einiger RechteinhaberInnen gegen mutmaßliche Urheberrechtsverletzungen. Grundsätzlich ist selbstverständlich nichts dagegen einzuwenden, wenn jemand versucht, seine/ihre ihm/ihr gesetzlich zugesicherten Rechte durchzusetzen und sich gegen einen aus einer Verletzung derselben entstehenden Schaden abzusichern. Allerdings ist über die letzten Jahre zu beobachten, dass oft mit unverhältnismäßig erscheinender Vehemenz vorgegangen wird, die auch nicht davor zurückschreckt, Maßnahmen einzusetzen, die ursprünglich für die Bekämpfung von Terrorismus gedacht waren, und auch einen entsprechenden Eingriff in die Privatsphäre darstellen. Eine Beschränkung des Grundrechts auf Privatsphäre und informationelle Selbstbestimmung ließe sich im sinnvoll geführten Kampf gegen internationalen Terrorismus eventuell hinnehmen, als Maßnahme gegen deutlich geringere Vergehen, kann man aber sicher nicht mehr von Verhältnismäßigkeit sprechen.

⁸⁹ ORF-Futurezone/Reuters (2009): Deutsche Bahn verteidigt Bespitzelungen, <http://futurezone.orf.at/stories/1502159/> (3. Februar 2009); ORF-Futurezone/APA/dpa (2009): Nokia forciert Mitarbeiter-Überwachung, <http://futurezone.orf.at/stories/1502202/> (3. Februar 2009).

6 Datenschutz & Datenschatz

Ähnlich wertvollen Schätzen sollte auch personenbezogene Daten geschützt werden. Informationssicherheit als Beitrag zum Datenschutz, neben den in anderen Passagen des Dokuments erläuterten Problemen, umfasst daher auch den Schutz der Information vor Schaden durch technische Gebrechen an den Speichergeräten, unbefugten Zugriff, Verlust und ähnlich problematische Situationen im Management von Daten. In diesen Bereichen gab es vor allem in den letzten zwei Jahren mit stark zunehmender Häufigkeit Vorfälle, die darauf schließen lassen, dass zu oft die notwendige Sorgfalt vernachlässigt wird. Solche Ereignisse sind immer (natürlich abhängig von der Art der gespeicherten Daten) ein Angriff auf die Privatsphäre der Personen, deren Daten so fahrlässig gefährdet wurden.

Diversen Medienberichten zufolge beginnt das bei einer Festplatte aus dem Bereich des österreichischen Verkehrs- und Infrastrukturministeriums, die auf der Auktionsplattform eBay zur Versteigerung auftaucht⁹⁰, geht über verlorene Datenträger in anderen EU-Ländern wie Großbritannien⁹¹, den Skandal aus den Jahren 2005 und 2006 bei der deutschen Telekom, der im Frühjahr 2008 der breiten Öffentlichkeit bekannt wurde, und das neuerliche Datenleck Ende 2008⁹², über den Verlust eines Laptops der österreichischen Gesundheitsministerin Andrea Kdolsky⁹³, bis hin zu einer zumindest als leichtfertig zu bezeichnenden Kundendatenweitergabe der Telekom Austria an eine vorarlberger Rechtsanwaltskanzlei, die 2008 eine Welle an Abmahnungen an mutmaßliche UrheberrechtsverletzerInnen verschickt hat, und der die Telekom Austria dafür, wie bei gerichtlich angeordneten Überwachungen, eine Gebühr von € 102,84 pro Datensatz verrechnet hat.⁹⁴ Leichtfertig deshalb, weil zum fraglichen Zeitpunkt nicht geklärt war, ob dem ohne richterliche Anordnung verpflichtend nachzukommen wäre, oder ob es nicht sogar unzulässig wäre, weil das Grundrecht auf Datenschutz schwerer wiege. Die Entrüstung bei KundInnen der Telekom Austria, nachdem das Vorgehen in dieser Angele-

**Personenbezogene
Daten sind so wertvoll
wie Schätze ...**

⁹⁰ ORF-Futurezone/APA (2006): Festplatte aus Ministerium landete bei eBay, <http://futurezone.orf.at/stories/115527/> (6. Jänner 2009).

⁹¹ Heise online (2007a): Millionen Briten von Datenpanne betroffen, <http://www.heise.de/newsticker/Millionen-Briten-von-Datenpanne-betroffen--/meldung/99315> (6. Jänner 2009);
Heise online (2007b): Britischen Behörden gehen erneut Millionen Daten verloren, <http://www.heise.de/newsticker/Britischen-Behoerden-gehen-erneut-Millionen-Daten-verloren--/meldung/100742/> (6. Jänner 2009);
Heise online (2007c): Daten von hunderttausenden Patienten sind in Großbritannien verlorengegangen: <http://www.heise.de/newsticker/Daten-von-hunderttausenden-Patienten-sind-in-Grossbritannien-verloren-gegangen--/meldung/101035/> (6. Jänner 2009);
Heise online (2008a): Die nächste Datenpanne beim britischen Militär: <http://www.heise.de/newsticker/Die-naechste-Datenpanne-beim-britischen-Militaer--/meldung/102167/> (6. Jänner 2009).

⁹² Schröder, Burkhard (2008): It's a feature, not a bug, <http://www.heise.de/tp/r4/artikel/28/28007/1.html> (6. Jänner 2009);
ORF-Futurezon/APA/AP (2009): Neue Datenpanne bei der Deutschen Telekom, <http://futurezone.orf.at/stories/1502081/> (2. Februar 2009).

⁹³ Die Presse/APA (2008): Kdolskys Laptop gestohlen, <http://diepresse.com/home/politik/innenpolitik/392978/index.do> (6. Jänner 2009).

⁹⁴ Zsolt, Wilhelm (2008a): Porno-Industrie plant Klagen gegen Österreicher, <http://derstandard.at/Text/?id=1224169785885> (6. Jänner 2009).

genheit publik wurde, führte auch dazu, dass das Unternehmen daraufhin seinen Standpunkt änderte, sich auf eine anderslautende juristische Meinung bezog und jede weitere Datenübermittlung in dem Fall einstellte⁹⁵.

Aber auch Daten aus öffentlichen Registern, wie dem Zentralen Melderegister (ZMR) können leicht zur Ware auf dem internationalen Adressmarkt verkommen⁹⁶, wo auch 1,5 Millionen Datensätze (Name, Adresse, Kontodaten) deutscher Lottospieler im vergangenen Jahr gelandet sind⁹⁷.




**... trotzdem werden
sie nicht wie Schätze
gehütet**

All diese Beispiele zeigen deutlich, dass absolute Sicherheit nicht gewährleistet werden kann. Auch dort, wo versucht wird, das Risiko zu minimieren, treten Situationen auf, beziehungsweise finden Angreifer Schwachstellen, die dazu führen, dass Daten in die falschen Hände geraten – in erster Linie zum Nachteil derjenigen, deren Daten gespeichert wurden, und selten mit ausreichenden Konsequenzen für die Firmen und Institutionen, die die Daten verloren haben.

**Die Sammlungen
auf einen Blick**

Wie sich die Verbreitung von Datensammlungen darstellt, versucht die folgende Tabelle (Tabelle 1: Speicherorte und Datenarten) zu veranschaulichen. Sie zeigt in den Spalten verschiedene Institutionen, die im Alltag der BürgerInnen eine Rolle spielen, und in den Zeilen verschiedene Arten von personenbezogenen Daten, gruppiert nach Lebensbereich und zunehmender Sensibilität. Dabei stehen die mit einem „X“ markierten Felder für Daten, die mit Sicherheit oder sehr hoher Wahrscheinlichkeit gespeichert werden, und die mit einer „0“ gekennzeichneten Felder für Daten, die möglicherweise bzw. mit geringer Wahrscheinlichkeit gespeichert werden. Dort, wo die Felder weiß geblieben sind, und keine Markierung erfolgte, werden die jeweiligen Daten vermutlich nicht gespeichert. Es lässt sich an Hand der Tabelle sehr gut erkennen, wie viele verschiedene Einrichtungen, Institutionen, Firmen etc. Profile über die ÖsterreicherInnen führen, und wie wenige dieser Profile ausreichen würden, um ein vollständiges Bild aller Lebensumstände eines Bürgers/einer Bürgerin zu erhalten.

Betont werden soll, dass es sich lediglich um jene Daten handelt, welche abgefragt und direkt gespeichert werden, nicht jedoch um jene, die sich aus den gespeicherten Daten errechnen beziehungsweise mit statistischen Methoden ermitteln lassen. Darüber hinaus sind legale und illegale Vernetzungen und Datenabgleiche zwischen den Institutionen nicht in der Tabelle berücksichtigt. Bezöge man alle diese mit ein, dann ergäbe sich ein deutlich dichteres Bild.

-  = Daten werden mit Sicherheit oder sehr hoher Wahrscheinlichkeit gespeichert
-  = Daten werden möglicherweise/mit geringer Wahrscheinlichkeit gespeichert
-  = Daten werden vermutlich nicht gespeichert

⁹⁵ Zsolt, Wilhelm (2008b): Datenweitergabe an Porno-Industrie: Telekom Austria stellt Auskünfte ein, <http://derstandard.at/Text/?id=1224169825646> (6. Jänner 2009).

⁹⁶ ORF-Futurezone/APA (2008a): ZMR-Daten auf dem Schwarzmarkt, <http://futurezone.orf.at/stories/303448/> (6. Jänner 2009).

⁹⁷ ORF-Futurezone/AFP/dpa (2008): Deutschland: 1,5 Mio. Kontodaten verkauft, <http://futurezone.orf.at/stories/300639/> (6. Jänner 2009).

Tabelle 1: Speicherorte und Datenarten

Daten	Institution/Organisation	Öffentlich										Privat															
		Meldewesen	Grundbuch	Kommunale Verw.	Polizei/Gericht	Bundesheer/Zivildienst	Finanzbehörden	Sozialversicherung	Gesundheit/GDA	Bildungssystem	Statistik Österreich	Arbeitgeber	Finanzdienstleister	Telekommunikation	Religionsgemeinschaft	Private Versicherungen	Rundfunk, Medien	Vereine	Kundenkarten/-profile	Wirtschaftsauskunftei	ISP	Adressverlage	E-Com./Webshops	Web 2.0 Plattformen	Suchmaschinen	Videoüberwachung	
Standard Grunddaten	Name (Vor- und Nachname)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	0	
	Geschlecht	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	0	X	X	X	X	0	X	
	Titel	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	0	X	X	X	0	0		
	Postadresse	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	0		
Erweiterte Grunddaten	Telefonnummer (Festnetz, Mobil)			0	0	0	0	0	0	X		X	X	X	0	0	0	0	X	0	X	X	X	0	0		
	Telefonn. (Festnetz geheim, Wertkarte)				0					0		0		X			0										
	Faxnummer			0	0	0	0	0	0			0	0	X		0	0	0			X	X	0	0	0		
	Email-Adresse				0		0			X		0	X	X		0	0	0	X		X	0	X	X	X		
	ZMR-Zahl	X	0	X	0	0					X	X	0	0	0					0	0						
Private Lebenslaufdaten	Geburtsdatum/Alter	X	X	X	X	X	X	X	X	X	X	X	X	X	X	0	0	X	0		X	0	X	0	0		
	Geburtsort	X			0	X				X	X	0		X													
	Familienstand				X	0	X	X	X	X	X	X	0		0	X	0	0	0			0		0			
	Staatsangehörigkeit	X	0	X	X	X	X	X	X	X	X	X	0	0	0	X	0	0	0	0		0	0	X			
	Beruf				0	X	X	X	0	X	X	X	0	0		X	0	0	0			0		0		0	
	Arbeitsstätte				0	0	X	X	X	X	X	X	X	X		X	0						0	0		0	
	Anzahl Kinder			X		X	X	X	X	X	X	X	0		0	X		0					0	0			
	Bildungsweg					X	X	X	X	X	X	0				0	0	0				X		0			
	Konfession	X				X	0			0	0	0			X							X		0		0	
Privatleben	Familienmitglieder (Name, Adr., Beruf etc.)			X		0	X	X	X	X	X	0	X	0	X	X		0									
	Wohnungsgröße			0							X		0									0					
	MitbewohnerInnen						0				X														0		
	NachbarInnen										X															0	
Versicherung	Sozialversicherungsnummer				0	X	X	X	X		X	X				0											
	Versicherungsdaten (Lebens-, Kranken-, Autoversicherung etc.)						X	X	X				0			X											
Körper	Gesundheits-/Krankheitsdaten				0	X	0	X	X			0	0			0									0	0	
	Biometrie (DNA, Iris, Foto, Fingerprints ...)				0	X				0	0		0											X		X	
Finanzielle Daten	Bankdaten/Kreditkarte			0		X	X	0				X	X	X	0	X	X	0	0	X	X		X	0			
	Einkommen					0	X	X			0	X	X		0	0					X		0				
	Ausgaben												X				0	0									
	Bonität						X					X	X	X		0		X	X	X	0	X	0				
	Gezahlte Steuern			0			X	0				X	0														
Vermögen	Immobilien		X	X			X					X															
	Sonst. nicht-monetäres Vermögen						0					0				X											
möglichen Kriminalität	Kriminaldaten/polizeilich gespeicherte Daten				X	0					0																
Kontakte	Geschäftliche Kontakte (Zeitpunkt, Häufigkeit, Dauer, Medium, Ort)										X		X								X			X		0	
	Private Kontakte (Zeitpunkt, Häufigkeit, Dauer, Medium, Ort)												X								X			X		0	
Gewohnheiten	Bewegungsdaten				0						0	X	X												0	X	
	Freizeitverhalten											0	0		0		0	0				0	X	X	0	0	
	Einkaufsverhalten											X	0					X		0		X	0	X	0	0	
	Benutzte Internetseiten u. pers. Vorlieben											0		0			0	0	0	X		0	X	X		0	
	Politisches Einstellungen und Interessen				0	0										0	0	0		0		0	X	X	0	0	

Was kann man besser machen?

Wie können Ereignisse wie oben beschrieben in Zukunft verhindert werden? Zunächst muss es das Ziel jedes Datenhalters und -verarbeiters sein, die Datenschutzprinzipien⁹⁸ in der jeweiligen Anwendung bestmöglich umzusetzen. Eine Unterstützung in diesen Bemühungen kann einerseits von der Datenschutzkommission kommen, auch dadurch, dass Vergehen gegen das Datenschutzgesetz konsequent geahndet werden, und andererseits aus dem Markt selbst, wie es das Beispiel des Europäischen Datenschutzgütesiegels EuroPriSe⁹⁹ gezeigt hat. Im letztgenannten Fall erhält das Unternehmen, das Daten speichert und verarbeitet, die Möglichkeit, die Anwendung prüfen zu lassen und bei positivem Ergebnis ein Zertifikat ausgestellt zu bekommen, mit dem es auch leichter ist, die Investitionen in den Schutz der Privatsphäre der Kunden im Vermarktungsprozess sichtbar zu machen.

Andere Entwicklungen, die zu einem höheren Datenschutzniveau führen sollten, lassen sich mit der Bezeichnung „Privacy by Design“ zusammenfassen.¹⁰⁰ Der europäischen Datenschutzbeauftragte, Peter Hustinx, veröffentlichte im April 2008 ein Papier, in dem er die Wichtigkeit des „Privacy by Design“-Ansatzes, speziell in den Forschungsanstrengungen des 7. Rahmenprogramms, unterstrich.¹⁰¹ Einen wichtigen Beitrag dazu leistete auch das Projekt PRISE¹⁰², das unter anderem Kriterien und Methoden erarbeitete, nach denen Forschungsvorhaben im Bereich von Sicherheitstechnologien im Hinblick auf ihren Einfluss auf die Privatsphäre evaluiert werden können (D6.2 Criteria for privacy enhancing security technologies¹⁰³). Interessant sind in dem Zusammenhang auch die Ergebnisse der partizipativen Prozesse in dem Projekt, die sehr deutlich zeigen, dass es für europäische BürgerInnen jedenfalls einen Kernbereich der Privatsphäre gibt, der in jedem Fall unantastbar ist, sowie die Bedeutung der richterlichen Kontrolle bei allen Maßnahmen, die die individuelle Freiheit und die Rechte des/der Einzelnen beschränken (D5.8 Synthesis Report Interview Meetings¹⁰⁴).

⁹⁸ Die sieben Prinzipien des Datenschutzes sind: Legitimität, Transparenz, Datenminimierung, Zweckbindung, Verhältnismäßigkeit, Datenqualität und Datensicherheit.

⁹⁹ EuroPriSe Projekt-Website: <http://www.european-privacy-seal.eu>.

¹⁰⁰ „Privacy by Design“ bezeichnet den Entwicklungsansatz, der den Schutz der Privatsphäre schon bei der Entwicklung einer Technologie, oder der Entwicklung einer bestimmten Anwendung berücksichtigt. ForscherInnen und EntwicklerInnen im Bereich der angewandten Forschung versuchen verschiedene Parameter in ihrer Arbeit zu berücksichtigen. Bevor etwas Marktreife erlangt, muss beispielsweise überprüft werden, ob es sich auf rentablem Weg herstellen lässt. Diese Überlegungen möglichst früh in die Arbeit zu integrieren bringt den Vorteil, dass das viel kostengünstiger durchzuführen ist, als wenn in einem späteren Stadium Modifikationen vorgenommen werden müssen. So ist heute auch unter Software-EntwicklerInnen klar, dass Informationssicherheit von Beginn eines Projekts an „mitgedacht“ werden muss. Die Forderung bei „Privacy by Design“ besteht nun darin, dass eben auch Privacy ein Wert ist, den es von Anbeginn zu berücksichtigen gilt.

¹⁰¹ Hustinx, Peter (2008): The EDPS and EU Research and Technological Development, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf (6. Jänner 2009).

¹⁰² PRISE-Projekt (2006-2008): Projekt-Webseite, <http://prise.oeaw.ac.at> (6. Jänner 2009).

¹⁰³ PRISE-Projekt (2008): D6.2 Criteria for privacy enhancing security technologies, http://prise.oeaw.ac.at/docs/PRISE_D_6.2_Criteria_for_privacy_enhancing_security_technologies.pdf (2. Februar 2009).

¹⁰⁴ PRISE-Projekt (2008): D5.8 Synthesis Report Interview Meetings, http://prise.oeaw.ac.at/docs/PRISE_D_5.8_Synthesis_report.pdf (2. Februar 2009).

Die Privacy Enhancing Technologies (PETs) aus dem Bereich Identity Management, vor allem im Hinblick auf Web 2.0 Communities, versucht das Projekt PrimeLife zu fördern und den Entwicklern in einem interdisziplinären Forschungsansatz näher zu bringen. So heißt es in den „Objectives“ des Projekts:

„PrimeLife will address the core privacy and trust issues pertaining to the aforementioned challenges. Its long-term vision is to counter the trend to life-long personal data trails without compromising on functionality. It will build upon and expand the FP6 project Prime that has shown how privacy technologies can enable citizens to execute their legal rights to control personal information in on-line transactions. The main objective of the project is to bring sustainable privacy and identity management to future networks and services [...]”¹⁰⁵

Für österreichische Bürger besonders interessant ist die noch ausstehende Novelle (DSG-Novelle 2008) zum Datenschutzgesetz (DSG 2000), die unter anderem auch die Einführung von betrieblichen Datenschutzbeauftragten vorsieht.¹⁰⁶ Trotz Bedenken der Wirtschaft, die auf die Unternehmen Mehrkosten zukommen sieht, ohne einen Nutzen erkennen zu können und diese Aufgaben eher beim Betriebsrat angesiedelt gesehen hätte¹⁰⁷, wäre auch das eine zusätzliche Maßnahme, die, durch die Betonung der Wichtigkeit des Datenschutzes durch das Schaffen eines eigenen Aufgabenbereichs, eine weitere Verankerung des Datenschutzes im Bewusstsein der Bevölkerung positiv beeinflussen würde, und die zu einem Rückgang der Datenschutzvergehen führen könnte.

Weiters wird in diesem Entwurf der gesetzlichen Regelung von Videoüberwachungsmaßnahmen besondere Bedeutung geschenkt.¹⁰⁸ Das sollte grundsätzlich zu einer höheren Rechtssicherheit in dem Bereich beitragen. Wie auch der Kommentar des Datenschutzrates aus der Begutachtungsphase zu dem Thema zeigt, gibt es hier aber viele noch zu unpräzise und nicht praktikable Formulierungen¹⁰⁹.

Wer kann nun für eine Umsetzung beziehungsweise Durchsetzung sorgen? In Österreich ist eine überschaubare Gruppe von Institutionen mit dem Thema Datenschutz in unterschiedlicher Intensität befasst. Beispielsweise versuchen die Vereine quintessenz¹¹⁰ und VIBE¹¹¹, die ARGE DATEN¹¹², die Arbeiter-

**Ein neues
Datenschutzgesetz
steht vor der Tür**

¹⁰⁵ PrimeLife-Projekt (2008 bis 2011): Projekt-Webseite, <http://www.primelife.eu/> (6. Jänner 2009).

¹⁰⁶ Entwurf zum Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2008), Z.34 betreffend den zukünftigen §15a.

¹⁰⁷ Wirtschaftskammer Österreich (2008): Wirtschaftskammer Österreich gegen Einrichtung betrieblicher Datenschutzbeauftragter: Zu hohe Kosten ohne Mehrwert!, http://portal.wko.at/wk/format_detail.wk?AnglID=1&StId=401164&DstID=15 (6. Jänner 2009).

¹⁰⁸ Entwurf zum Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2008), Z.82 betreffend den zukünftigen Abschnitt 9a mit den §§50a-e.

¹⁰⁹ Datenschutzrat (2008): Stellungnahme des Datenschutzrates zum Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2008), <http://www.austria.gv.at/DocView.axd?CobId=31083> (6. Jänner 2009).

¹¹⁰ quintessenz – Verein zur Wiederherstellung der Bürgerrechte im Informationszeitalter: <http://www.quintessenz.at> (9. Jänner 2009).

¹¹¹ VIBE!AT: Verein für Internet-Benutzer Österreichs: <http://www.vibe.at> (9. Jänner 2009).

¹¹² ARGE DATEN: <http://www.argedaten.at/> (6. Jänner 2009).

**Wer sorgt für
Datenschutz in
Österreich**

kammer¹¹³, der Verein für Konsumenteninformation (VKI)¹¹⁴ und die Beratungsstelle Internet-Ombudsmann¹¹⁵ in Österreich bis hin zur EU-Initiative Dolceta¹¹⁶ und der europäischen Vereinigung von Bürgerrechts- und Datenschutzorganisationen European Digital Rights (EDRI)¹¹⁷ den VerbraucherInnen helfend zur Seite zu stehen beziehungsweise diese zu informieren. Zum Glück auch immer öfter in Situationen, wo es notwendig ist, das Recht auf Datenschutz der Konsumenten im Umgang mit Webshops und dergleichen durchzusetzen.¹¹⁸

Diese Organisationen leisten damit einen wertvollen Beitrag im Ausgleich der bestehenden Wissensunterschiede zwischen Anbietern und deren Kunden. Diese Unterschiede sind es, die in der Regel zu Abhängigkeitsverhältnissen führen können, aber oft das Geschäftsmodell des Anbieters funktionieren lassen.

¹¹³ Bundesarbeiterkammer: Portal der Arbeiterkammern: Datenschutz – Ihr gutes Recht, <http://www.arbeiterkammer.at/online/datenschutz-2775.html> (6. Jänner 2009).

¹¹⁴ Verein für Konsumenteninformation: <http://www.konsument.at/konsument/detail.asp?category=Computer+%2B+Telekom&id=35567> (9. Jänner 2009).

¹¹⁵ Internet Ombudsmann – Beratung und Streitschlichtung für Online-KonsumentInnen in Österreich: <http://www.ombudsmann.at/> (9. Jänner 2009).

¹¹⁶ Dolceta: VerbraucherInnen-Bildung online, <http://www.dolceta.eu/osterreich/index.php> (6. Jänner 2009).

¹¹⁷ European Digital Rights (EDRI): <http://www.edri.org> (2. Februar 2009).

¹¹⁸ Einige dieser Organisationen, die Mittel, Strategien und Methoden ihrer Arbeit, sowie ihre Pendanten in der übrigen Welt, sind in Colin J. Bennetts Buch „The Privacy Advocates – Resisting the Spread of Surveillance“ beschrieben.

7 Schlussfolgerungen

In den vorangegangenen Beispielen wird deutlich, dass die Privatsphäre und die informationelle Selbstbestimmung in vielen Bereichen stark bedroht beziehungsweise angegriffen sind. Schutz- und Abwehrmechanismen, die zumindest teilweise eine Hilfe darstellen könnten, werden zurzeit nicht in ausreichendem Maße eingesetzt, obwohl sie oft auch persönliche Nachteile (wie zum Beispiel Abhängigkeitsverhältnisse, Steuerung des Konsumverhaltens, Erhöhung des Überwachungsdrucks) verhindern könnten.

Damit einhergehend kommt es auch auf einer übergeordneten Ebene zu Problemen, bedingt durch den Verlust der persönlichen Freiheit des/der Einzelnen. Wie beschrieben kann das zu Defiziten demokratiepolitischer Natur führen, sowie zu einem Verlust an Innovationspotential, durch die Anpassung derer, die andernfalls non-konformistisches Verhalten zeigen und damit Anknüpfungspunkte herstellen und letztendlich Innovationssprünge begünstigen würden.

Ein weiterer Nachteil, der sich in zunehmendem Maße beobachten lässt, ist Risikoselektion. Weil vermeintlich jede einzelne Person in ihrer Gesamtheit immer genauer bestimmbar wird, werden Risiken, die bis jetzt die Gemeinschaft solidarisch getragen hat, auf den Einzelnen abgewälzt. Obendrein oft nicht auf Basis tatsächlicher Risiken, sondern auf Grund von statistischen Korrelationen.

In weiterer Folge führt das auch zu „Social Sorting“: Durch genauere Überwachung und Datenerhebung, die oft auch Daten über die ethnische Zugehörigkeit der BürgerInnen oder deren Bildungsstand einschließt, wird es möglich, diese Daten zum Beispiel mit Gesundheitsdaten zu verknüpfen, sodass sich Risikoselektion auf gesellschaftlicher Ebene durchführen lässt, was die Möglichkeit zu einer „fundierten“ Diskriminierung einzelner Randgruppen eröffnet.¹¹⁹

De-Kontextualisierung der Daten¹²⁰ ist neben fehlerhaften Eingaben, gemeinsam mit statistischen Korrelationen, die für schlüssig gehalten werden, ein Hauptgrund für fehlerhafte Auswertungen aus großen Datenmengen, und entsteht immer dort, wo Daten nicht im Kontext ihrer Erhebung betrachtet werden. Besonders anfällig dafür sind automatisierte Überwachungssysteme, die grundsätzlich den Kontext nicht erfassen können, sodass diese Information unweigerlich verloren geht – ebenso wie bei einer Verwendung der Daten für einen anderen als den ursprünglich geplanten Zweck.

In vielen Bereichen wird ein Umdenken in der Gesellschaft notwendig sein. Ein Beispiel, das er als „Reversal of Defaults“ bezeichnet hat, stammt vom Mathematiker Ronald Rivest, einem der Entwickler des RSA-Verschlüsselungsverfahrens:

„What was once private is now public.
What once was hard to copy is now trivial to duplicate.
What was once easily forgotten is now stored forever.“¹²¹

**Gefahren für die
Grundlagen unserer
Gesellschaft**

**Diskriminierung und
weniger Solidarität mit
den Schwachen**

**Neue Denksätze
sind notwendig**

¹¹⁹ Poudrier, Jennifer (2003), S. 111ff.

¹²⁰ Tichy, Gunther/Peissl, Walter (2001): Beeinträchtigung der Privatsphäre in der Informationsgesellschaft, S. 9, <http://www.oeaw.ac.at/ita/ebene5/GTWPweissenbach.pdf> (3. Februar 2009).

¹²¹ Zit. nach: Mattern, Friedemann (2001): Ubiquitous Computing – Der Trend zur Informatisierung und Vernetzung aller Dinge, S. 8, <http://www.vs.inf.ethz.ch/publ/papers/Internetkongress.pdf> (3. Februar 2009).

**10 Punkte für mehr
Privatsphäre und
informationelle
Selbstbestimmung**

Aber auch wenn man die Gründe für die zunehmende Überwachung heranzieht, um ihren Nutzen an diesen zu prüfen, entstehen Zweifel: Immer größere Datenmengen, die automatisiert verarbeitet werden müssen, in denen nach Verdächtigem und Verdächtigen gesucht wird, vergrößern nur den sprichwörtlichen Heuhaufen, in dem die Nadel zu finden ist. Ein Rückgang der Kriminalität oder des Terrorismus ist nicht zu beobachten.

Die Autoren dieser Studie haben daher versucht, die wichtigsten Punkte zusammenzufassen, die aus heutiger Sicht erforderlich wären, um den Schutz der Privatsphäre im notwendigen Maß zu gewährleisten, und diese in drei Gruppen unterteilt:

● **Bewusstseinsbildung**

- Awareness Raising – Es ist erforderlich, den Wünschen der BürgerInnen (siehe Fußnote 43) entsprechend, die bestehenden Probleme und Lösungsansätze aufzuzeigen. Damit soll sichergestellt werden, dass die Betroffenen fundierte Entscheidungen treffen können. Weiters kann dadurch eine seriöse gesellschaftliche Diskussion zu dem Thema ausgelöst werden.
- Bei DSGVO-Verletzungen und Information Security Incidents sollte eine Informationspflicht vorgeschrieben werden.¹²² Diese ist sowohl gegenüber der Datenschutzkommission als auch gegenüber den Betroffenen zu erfüllen.
- Betreiber von Web 2.0-Plattformen sollten verpflichtet werden, auf die langfristigen Folgen unbedachter Datenpreisgabe hinzuweisen.

● **Regulierung/Governance**

- Die kommerzielle Verwertung von Daten aus Internetdiensten durch Dritte sollte die ausdrückliche Zustimmung der NutzerInnen voraussetzen. Die Verweigerung dieser Zustimmung darf nicht zum Ausschluss vom Dienst führen.
- Bei der Planung, Ausschreibung und Umsetzung von Maßnahmen im öffentlichen Bereich sollte ein Privacy Impact Assessment (PIA) ebenso verpflichtend vorgeschrieben sein wie die Berücksichtigung von Datenschutzzertifizierungen (zum Beispiel dem Europäischen Datenschutzgütesiegel EuroPriSe).
- Grundsätzlich sollte in Unternehmen bei der Entwicklung von neuen Anwendungen, die potentiell in die Privatsphäre eingreifen (wie zum Beispiel RFID, smart objects/ubiquitous computing etc.), darauf geachtet werden, dass vor deren Marktreife/-zulassung geklärt ist, wie die Privatsphäre geschützt und Missbrauch verhindert werden kann. Dies würde als Qualitätsmerkmal einen Wettbewerbsvorteil sichern.
- Die strikte Einhaltung rechtsstaatlicher Grundsätze (wie der Gewaltentrennung und der unabhängigen Kontrolle) muss beachtet werden. Besondere Bedeutung bei der Entscheidung, ob individuelle Rechte beschnitten werden dürfen, kommt daher der richterlichen Kontrolle zu (siehe auch Fußnote 102).
- Die Datenschutzkommission muss mit den notwendigen Rechten und Ressourcen ausgestattet werden, um die Rolle einer aktiven und unabhängigen Kontrollinstanz im Datenschutzbereich erfüllen zu können.

¹²² Wie derzeit in Zusammenhang mit der angekündigten e-Privacy-Directive diskutiert.

- **Forschung**

- Privacy Enhancing Technologies – PETs (zum Beispiel Verschlüsselung, Identity Management, Anonymisierung etc.) – und Ansätze wie „Privacy by Design“ (zum Beispiel Daten mit „Ablaufdatum“¹²³) sollten weiter erforscht und deren Einsatz gefördert werden.
- Weiters ist die Grundlagenforschung im Bezug auf Regulierungsinstrumente und das Wesen von Privatheit und deren Bedeutung für eine Gesellschaft zu fördern.

¹²³ Ein Vorschlag von Viktor Mayr-Schönberg in seinem Beitrag „Nützliches Vergessen“ zum Grundrechtstag im Rahmen der ars electronica 2007, der dazu führen soll, dass wieder ein Zustand hergestellt wird, der dem natürlichen Vergessen ähnelt, das es in der Welt (digital) aufgezeichneter Informationen nicht mehr gibt. Mayr-Schönberg, Viktor (2007), S 15.

8 Literatur

8.1 Bücher/Berichte

- Aichholzer, Georg/Strauß, Stefan (2009): Systemic Change of the Identification of Citizens by Government – Electronic Identity Management as a Complex Technical Innovation and its Organisational, Legal and Cultural Matching in Selected European Countries (Länderbericht für Österreich), Wien.
- Bennett, Colin J. (2008): The Privacy Advocates – Resisting the Spread of Surveillance, Cambridge (MA, USA)/London.
- Kammerer, Dietmar (2008): Bilder der Überwachung, Frankfurt am Main.
- Lyon, David (Hrsg.) (2003): Surveillance As Social Sorting – Privacy, Risk and Digital Discrimination, London/New York.
- Mayr-Schönberg, Viktor: Nützliches Vergessen, in: Reiter, Michael/Wittmann-Tiwald, Maria (Hrsg.) (2008): Goodbye Privacy – Grundrechte in der digitalen Welt, Wien, S. 9-15.
- Poudrier, Jennifer: „Racial“ categories and health risks – Epidemiological surveillance Among Canadian First Nations, in: Lyon, David (Hrsg.) (2003): Surveillance As Social Sorting – Privacy, Risk and Digital Discrimination, London/New York, S. 111-134.
- Reiter, Michael/Wittmann-Tiwald, Maria (Hrsg.) (2008): Goodbye Privacy – Grundrechte in der digitalen Welt, Wien.
- Rössler, Beate (2001): Der Wert des Privaten, Frankfurt am Main.

8.2 Gesetze/Standards/Normen

- Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (Urheberrechtsgesetz).
- Bundesgesetz über die Dokumentation im Bildungswesen (Bildungsdokumentationsgesetz).
- Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-GovG).
- Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird (Telekommunikationsgesetz 2003 – TKG 2003).
- Bundesgesetz über die Organisation der Sicherheitsverwaltung und die Ausübung der Sicherheitspolizei (Sicherheitspolizeigesetz – SPG).
- Entwurf zum Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2008).
- Europäische Menschenrechtskonvention (EMRK).

Richtlinie 2006/24/EG des Europäischen Parlaments und Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, <http://register.consilium.eu.int/pdf/de/05/st03/st03677.de05.pdf> (3. Februar 2009).

8.3 Im Internet verfügbare Informationen

(In Klammern das Datum des letzten Zugriffs.)

A-SIT Zentrum für sichere Informationstechnologie Austria: Bürgerkarte – Vorteile für Bürgerinnen und Bürger, <http://www.buergerkarte.at/de/index.html> (6. Jänner 2009).

accenture: Personal Awareness Assistant, http://www.accenture.com/Global/Services/Accenture_Technology_Labs/R_and_I/PersonalAssistant.htm (6. Jänner 2009).

Allwinger Kristin/Joshi M.A. Schillhab (2008): Vertrauen der ÖsterreicherInnen in den Datenschutz, Juli 2008, <http://www.oekonsult.eu/datensicherheit2008.pdf> (6. Jänner 2009).

ARGE DATEN: <http://www.argedaten.at/> (6. Jänner 2009).

ARGE DATEN (2005): EU-Beschwerde – (Teil)Erfolg für die ARGE DATEN, http://www2.argedaten.at/session/anonym545032xpxjao6l2569.E42_INP.html (3. Februar 2009).

Art. 29 Datenschutzgruppe, http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_de.htm (2. Februar 2009).

Artikel 29 Datenschutzgruppe (2007): Stellungnahme 2/2007 zur Information von Fluggästen über die Übermittlung von PNR-Daten an amerikanischen Behörden, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp151_de.pdf (4. Februar 2009).

Artikel 29 Datenschutzgruppe (2008): Arbeitsprogramm 2008-2009, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp146_de.pdf (4. Februar 2009).

Art. 29 WP (2000): Stellungnahme 7/2000 zum Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp36de.pdf (8. Jänner 2009).

Art. 29 WP (2007): Stellungnahme Nr. 4/2007 zum Begriff der personenbezogenen Daten, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_de.pdf (8. Jänner 2009).

Art. 29 WP (2008): Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_de.pdf (8. Jänner 2009).

- Bundesarbeiterkammer: Portal der Arbeiterkammern: Datenschutz – Ihr gutes Recht, <http://www.arbeiterkammer.at/online/datenschutz-2775.html> (6. Jänner 2009).
- Bundesministerium für Inneres (2008): BM.I Internet – Reisepaß, <http://www.bmi.gv.at/reisepass/> (6. Jänner 2009).
- Datenschutzbericht 2005-2007 der Österreichischen Datenschutzkommission, <http://www.dsk.gv.at/DocView.axd?CobId=30637> (6. Jänner 2009).
- Datenschutzrat (2008): Stellungnahme des Datenschutzrates zum Bundesgesetz, mit dem das Datenschutzgesetz 2000 geändert wird (DSG-Novelle 2008), <http://www.austria.gv.at/DocView.axd?CobId=31083> (6. Jänner 2009).
- Datenschutzrichtlinie vom 26. November 2008 von facebook.com in der deutschen Übersetzung: <http://de-de.facebook.com/policy.php?ref=pf> (6. Jänner 2009).
- DerStandard.at/APA (2008a): EU-Kommission will Nackt-Scanner an Flughäfen einführen, <http://derstandard.at/?url=/?id=1224256246628> (8. Jänner 2009).
- DerStandard.at/APA (2008b): Sicherheitspolizeigesetz im Eiltempo und ohne Diskussion beschlossen, <http://derstandard.at/?url=/?id=3141872> (8. Jänner 2009).
- Die Presse (2008): Geheime Post zwischen Wien und St. Pölten, <http://diepresse.com/home/techscience/wissenschaft/421055/index.do> (6. Jänner 2009).
- Die Presse/APA (2007): EU-Parlament kritisiert Flug-Abkommen mit USA, <http://diepresse.com/home/politik/aussenpolitik/316642/index.do> (3. Februar 2009).
- Die Presse/APA (2008): Kdolskys Laptop gestohlen, <http://diepresse.com/home/politik/innenpolitik/392978/index.do> (6. Jänner 2009).
- Digitales Österreich (2008): Ministerin Silhavy vergibt bundesweiten ebiz-egovernment Preis und Sonderpreise, http://www.digitales.oesterreich.gv.at/site/cob__32165/5236/default.aspx (6. Jänner 2009).
- Dolceta: VerbraucherInnen-Bildung online, <http://www.dolceta.eu/osterreich/index.php> (6. Jänner 2009).
- ebiz egovernment award (2008): Sieger 2008, <http://www.report.at/award/archive/Sieger2008.htm> (6. Jänner 2009).
- Fraunhofer Institut für Informations- und Datenverarbeitung (2008): Aufklärung mit mobilen und ortsfesten Sensoren im Verbund, <http://www.iitb.fraunhofer.de/servlet/is/18599/> (1. Februar 2009).
- Fraunhofer-Institut für Sichere Informationstechnologie SIT (2008): Privatsphärenschutz in Soziale-Netzwerke-Plattformen, http://www.sit.fraunhofer.de/fhg/Images/SocNetStudie_Deu_Final_tcm105-132111.pdf (8. Jänner 2009).
- Fuchs, Christian (2009): Social Networking Sites and the Surveillance Society. A Critical Case Study of the Usage of studiVZ, Facebook an MySpca by Students in Salzburg in the Context of Electronic Surveillance, http://fuchs.icts.sbg.ac.at/SNS_Surveillance_Fuchs.pdf (2. Februar 2009).

- Gartner Inc. (2007): Gartner Says Number of Identity Theft Victims Has Increased More Than 50 Percent Since 2003, <http://www.gartner.com/it/page.jsp?id=501912> (8. Jänner 2009).
- Goldhaber, Michael H. (1997): Die Aufmerksamkeitsökonomie und das Netz – Teil I (deutsche Übersetzung durch Florian Rötzer), <http://www.heise.de/tp/r4/artikel/6/6195/1.html> (6. Jänner 2009).
- Golem.de (2009): EuGH gibt Urteilstermin für Vorratsdatenspeicherung bekannt, <http://www.golem.de/0901/64684.html> (3. Februar 2009).
- Google Earth: <http://earth.google.de/> und Google Streetview: <http://www.google.de/press/streetview/index.html> (6. Jänner 2009).
- Hack, Günter (2008): Der ELGA-Fahrplan, <http://futurezone.orf.at/stories/276191> (8. Jänner 2009).
- Hack, Günter (2009): Ministerium kontert E-Voring-Gegner, <http://futurezone.orf.at/stories/1502109/> (3. Februar 2009).
- Hasbrouck, Edward (2009): Recent developments in the USA in relation to the protection of travel data, <http://www.papersplease.org/wp/2009/01/15/recent-developments-in-the-usa-in-travel-data/#more-326> (2. Februar 2009).
- Heise online (2006): Irland und die Slowakei legen Klage gegen Vorratsdatenspeicherung ein, <http://www.heise.de/newsticker/Irland-und-die-Slowakei-legen-Klage-gegen-Vorratsdatenspeicherung-ein--meldung/73751> (3. Februar 2009).
- Heise online (2007a): Millionen Briten von Datenpanne betroffen, <http://www.heise.de/newsticker/Millionen-Briten-von-Datenpanne-betroffen--meldung/99315> (6. Jänner 2009).
- Heise online (2007b): Britischen Behörden gehen erneut Millionen Daten verloren, <http://www.heise.de/newsticker/Britischen-Behoerden-gehen-erneut-Millionen-Daten-verloren--meldung/100742/> (6. Jänner 2009).
- Heise online (2007c): Daten von hunderttausenden Patienten sind in Großbritannien verlorengegangen: <http://www.heise.de/newsticker/Daten-von-hunderttausenden-Patienten-sind-in-Grossbritannien-verloren-gegangen--meldung/101035/> (6. Jänner 2009).
- Heise online (2007d): Vorratsdatenspeicherung für eine 0,006 Prozentpunkte höhere Aufklärungsquote, <http://www.heise.de/newsticker/Vorratsdatenspeicherung-fuer-eine-0-006-Prozentpunkte-hoehere-Aufklaerungsquote--meldung/92746> (3. Februar 2009).
- Heise online (2007e): Aufregung um Vorratsdatenspeicherung in Österreich, <http://www.heise.de/newsticker/Aufregung-um-Vorratsdatenspeicherung-in-Oesterreich--meldung/90066> (3. Februar 2009).
- Heise online (2008a): Die nächste Datenpanne beim britischen Militär: <http://www.heise.de/newsticker/Die-naechste-Datenpanne-beim-britischen-Militaer--meldung/102167/> (6. Jänner 2009).
- Heise online (2008b): Bundesdatenschützer sieht Google Street View sehr kritisch, <http://www.heise.de/newsticker/Bundesdatenschuetzer-sieht-Gogles-Street-View-sehr-kritisch--meldung/112886> (6. Jänner 2009).

- Heise online (2008c): Verhandlungen zur Vorratsdatenspeicherung in Luxemburg und Dublin, <http://www.heise.de/newsticker/Verhandlungen-zur-Vorratsdatenspeicherung-in-Luxemburg-und-Dublin--/meldung/110307> (3. Februar 2009).
- Heise security (2009a): Bericht: Unsichere Verarbeitung der Fingerabdrücke in Meldebehörden, <http://www.heise.de/security/Bericht-Unsichere-Verarbeitung-der-Fingerabdruecke-in-Meldebehoerden--/news/meldung/126707> (4. Februar 2009).
- Heise security (2009b): Job-Börse erneut Opfer eines Datendiebstahls, <http://www.heise.de/security/Job-Boerse-erneut-Opfer-eines-Datendiebstahls--/news/meldung/122315> (1. Februar 2009).
- Hustinx, Peter (2008): The EDPS and EU Research and Technological Development, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/PolicyP/08-04-28_PP_RTD_EN.pdf (6. Jänner 2009).
- Ito, Joichi (2007): Aufzeichnung des Vortrags beim Grundrechtstag 2007, der der Auftakt zur ars electronica war, die 2007 unter dem Thema „Goodbye Privacy“ stand: <http://www.aec.at/en/festival2007/webcasts/index.asp> (6. Jänner 2009).
- Kissling, Roland (2007): Festplatten-Speicherdichte vor Verdoppelung, <http://www.computerwelt.at/detailArticle.asp?a=108653&n=3> (8. Jänner 2009).
- Laaff, Meike (2008): Die Kamera weiß, was verdächtig ist, <http://www.taz.de/1/politik/schwerpunkt-ueberwachung/artikel/1/was-verdaechtig-ist-sagt-die-kamera/> (1. Februar 2009).
- Landesschulrat Niederösterreich (2005): Das Bildungsdokumentationsgesetz (BilDokG) – Häufig gestellte Fragen und Antworten, <http://bsr.lsr-noe.gv.at/gf/verordnungen/2005/0512/bl3c.pdf> (3. Februar 2009).
- Langheinrich, Marc (2001): P3P – Ein neuer Standard für Datenschutz im Internet, in: *digma – Zeitschrift für Datenrecht und Informationssicherheit* (2001), Vol.1, S. 32-34, zit. nach: <http://www.vs.inf.ethz.ch/publ/papers/p3p-digma.pdf> (6. Jänner 2009).
- Mattern, Friedemann (2001): Ubiquitous Computing – Der Trend zur Informatisierung und Vernetzung aller Dinge, S. 8, <http://www.vs.inf.ethz.ch/publ/papers/Internetkongress.pdf> (3. Februar 2009).
- Mattern, Friedemann (2008): Herausforderungen der technischen Entwicklung an den Datenschutz, <http://www.lfd.m-v.de/dschutz/veransta/aktechnik50/mattern50.pdf> (28. Jänner 2009).
- Mattern, Friedemann/Marc Langheinrich (2001): Allgegenwärtigkeit des Computers – Datenschutz in einer Welt der intelligenten Alltagsdinge, in Müller Günter, Martin Reichenbach (Hrsg.) (2001): *Sicherheitskonzepte für das Internet*, 5. Berliner Kolloquium der Gottlieb Daimler- und Karl Benz-Stiftung, S. 7-26, zit. nach: <http://www.vs.inf.ethz.ch/publ/papers/allgegenwaertig.pdf> (6. Jänner 2009).

- McAfee (2009): Unsecured Economies: Protecting Vital Information, <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport> (2. Februar 2009).
- Mühlbauer, Peter (2008): Zyprien und Schäuble wollen „Beziehungen“ zu verbotenen Vereinigungen unter Strafe stellen, <http://www.heise.de/tp/r4/artikel/29/29406/1.html> (2. Februar 2009).
- Niggemeier, Stefan (2006): Bürgerjournalismus – Hobby: Reporter, in: Frankfurter Allgemeine Sonntagszeitung, vom 8. Oktober 2006, Nummer 40, S. 35, zit. nach: <http://www.faz.net/s/Rub475F682E3FC24868A8A5276D4FB916D7/Doc~EAD3B9321BBBD42659CB366758B6698CF~ATpl~Ecommon~Scontent.html> (6. Jänner 2009).
- O'Reilly, Tim (2005): What Is Web 2.0? – Design Patterns and Business Models for the Next Generation of Software, <http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html> (6. Jänner 2009).
- ORF-Futurezone (2008): Polizei: 32 SPG-Abfragen pro Tag, <http://futurezone.orf.at/stories/288198/> (2. Februar 2009).
- ORF-Futurezone/APA (2005): Body-Scanner entblättert Fluggäste, <http://futurezone.orf.at/stories/77077/> (8. Jänner 2009).
- ORF-Futurezone/APA (2006): Festplatte aus Ministerium landete bei eBay, <http://futurezone.orf.at/stories/115527/> (6. Jänner 2009).
- ORF-Futurezone/APA (2008a): ZMR-Daten auf dem Schwarzmarkt, <http://futurezone.orf.at/stories/303448/> (6. Jänner 2009).
- ORF-Futurezone/APA (2008b): Zweites EU-Mahnschreiben an Österreich, <http://futurezone.orf.at/stories/308589/> (3. Februar 2009).
- ORF-Futurezone/APA (2008c): Datenhandel „nicht kontrollierbar“, <http://futurezone.orf.at/stories/317153/> (3. Februar 2009).
- ORF-Futurezone/APA/AP (2009): Neue Datenpanne bei der Deutschen Telekom, <http://futurezone.orf.at/stories/1502081/> (2. Februar 2009).
- ORF-Futurezone/APA/dpa (2009): Nokia forciert Mitarbeiter-Überwachung, <http://futurezone.orf.at/stories/1502202/> (3. Februar 2009).
- ORF-Futurezone/AFP/dpa (2008): Deutschland: 1,5 Mio. Kontodaten verkauft, <http://futurezone.orf.at/stories/300639/> (6. Jänner 2009).
- ORF-Futurezone/digital.leben (2009): Personenidentifikation fürs Fotoalbum, <http://futurezone.orf.at/tipps/stories/1501867/>, und Lückenlose Videoüberwachung, <http://futurezone.orf.at/tipps/stories/1502073/> (1. Februar 2009).
- ORF-Futurezone/dpa (2008a): Soziale Netzwerke werden unterschätzt, <http://futurezone.orf.at/stories/1500433/> (8. Jänner 2009).
- ORF-Futurezone/dpa (2008b): Videoüberwachung ein „völliges Fiasko“, <http://futurezone.orf.at/stories/275884/> (6. Jänner 2009).
- ORF-Futurezone/Reuters (2009): Deutsche Bahn verteidigt Bspitzelungen, <http://futurezone.orf.at/stories/1502159/> (3. Februar 2009).
- ORF-Online (2006): Warnung vor Computer-Spionage, <http://salzburg.orf.at/stories/104375/> (6. Jänner 2009).

- Parycek, Peter (2006): Staatliche Informationsgebarung – Gläserne Bürger im gläsernen Staat?, <http://www.oeaw.ac.at/ita/ta06/Parycek.pdf> (3. Februar 2009).
- Pieter, Wolter und Rop Gonggrijp auf der Conference for Computers, Privacy and Data Protection (CPDP) 2009, <http://www.cpdpconferences.org/presentations.html> (3. Februar 2009).
- Presstext Austria (2007): USA: ID-Klau auf dem Rückzug, <https://presstext.at/pte.mc?pte=070202015> (6. Jänner 2009).
- Presstext Austria (2008): Outdoor-Experte Northland für neuartige RFID-Diebstahlsicherung ausgezeichnet, <http://www.presstext.at/pte.mc?pte=080925039> (6. Jänner 2009).
- PrimeLife-Projekt (2008 bis 2011): Projekt-Webseite, <http://www.primelife.eu/> (6. Jänner 2009).
- PRISE-Projekt (2006-2008): Projekt-Webseite, <http://prise.oeaw.ac.at> (6. Jänner 2009).
- PRISE-Projekt (2008): D6.2 Criteria for privacy enhancing security technologies, http://prise.oeaw.ac.at/docs/PRISE_D_6.2_Criteria_for_privacy_enhancing_security_technologies.pdf (2. Februar 2009).
- PRISE-Projekt (2008): D5.8 Synthesis Report Interview Meetings, http://prise.oeaw.ac.at/docs/PRISE_D_5.8_Synthesis_report.pdf (2. Februar 2009).
- Privacy Bird: <http://www.privacybird.org/> (21. Jänner 2009).
- Quintessenz (2009): Bürgerkarte: Nicht einmal geschenkt ein Renner, <http://www.quintessenz.org/d/000100005462> (3. Februar 2009).
- Reuters (2007): Amsterdam airport deploys body-scanning machines, <http://www.reuters.com/article/technologyNews/idUSL1569798620070515> (28. Jänner 2009).
- Roth, Wolf-Dieter (2006): „Web 2.0 ist nutzloses Blabla, das niemand erklären kann“, <http://www.heise.de/tp/r4/artikel/23/23472/1.html> (6. Jänner 2009).
- Rötzer, Florian (2007): Bildbereinigung durch Google Earth, <http://www.heise.de/tp/r4/artikel/24/24483/1.html> (6. Jänner 2009).
- Rötzer, Florian (2008): Ausbreitung der zur Terrorbekämpfung eingeführten Überwachung in den Alltag, <http://www.heise.de/tp/blogs/8/119371> (8. Jänner 2009).
- Rötzer, Florian (2008b): Vom allgemeinen Nutzen der Antiterrorgesetze, <http://www.heise.de/tp/r4/artikel/29/29057/1.html> (8. Jänner 2009).
- Schattenblick (2007): Bush-Regierung schließt Tausende vom Flugverkehr aus, <http://www.schattenblick.de/infopool/politik/redakt/usa1108.html> (2. Februar 2009).
- Schmid, Bernard (2007): ELSA sieht alles, <http://www.heise.de/tp/r4/artikel/26/26560/1.html> (8. Jänner 2009).
- Schröder, Burkhard (2002): Google filtert, <http://www.heise.de/tp/r4/artikel/12/12948/1.html> (6. Jänner 2009).
- Schröder, Burkhard (2008): It's a feature, not a bug, <http://www.heise.de/tp/r4/artikel/28/28007/1.html> (6. Jänner 2009).

- Schuler, Thomas (2008): Automatischer Absturz,
<http://www.sueddeutsche.de/computer/480/310409/text/>
(8. Jänner 2009).
- Shankland, Stephen/Stefan Beiersmann (2008): Google anonymisiert
Gesichter in Street View, [http://www.zdnet.de/news/tkomm/
0,39023151,39190820,00.htm](http://www.zdnet.de/news/tkomm/0,39023151,39190820,00.htm) (9. Jänner 2009).
- The Gallup Organization (2008): Flash Eurobarometer Series #225:
Data Protection in the European Union – Citizens' Perceptions,
http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf
(4. Februar 2009).
- Tichy, Gunther/Peissl, Walter (2001): Beeinträchtigung der Privatsphäre in
der Informationsgesellschaft, S. 9,
<http://www.oeaw.ac.at/ita/ebene5/GTWPweissenbach.pdf>
(3. Februar 2009).
- Tippenhauer, Nils Ole/Rasmussen, Kasper Bonne/Pöpper, Christina/Čapkun,
Srdjan (2008): iPhone and iPod Location Spoofing: Attacks on Public
WLAN-based Positioning Systems,
<ftp://ftp.inf.ethz.ch/pub/publications/tech-reports/5xx/599.pdf>
(2. Februar 2009).
- USA Today (2008): 10 airports install body scanners,
http://www.usatoday.com/travel/flights/2008-06-05-bodyscan_N.htm
(28. Jänner 2009).
- Überwachungsstaat.at (2008): Die Akte Clemens A.,
<http://www.ueberwachungsstaat.at/index.php?id=63195> (2. Februar
2009) und <http://www.ueberwachungsstaat.at/index.php?id=63196>
(2. Februar 2009).
- W3C (2002): The Platform for Privacy Preferences 1.0 (P3P1.0)
Specification, W3C Recommendation 16 April 2002,
<http://www.w3.org/TR/2002/REC-P3P-20020416/> (6. Jänner 2009).
- Weiner, Laurenz (2000): Gigabytes im Überfluß,
<http://www.heise.de/ct/00/16/078/> (8. Jänner 2009).
- Whitehead, Tom (2008): Town halls ordered to stop using terror laws to
catch dog-foulers, [http://www.telegraph.co.uk/news/newsttopics/
politics/lawandorder/3485716/Town-halls-ordered-to-stop-using-
terror-laws-to-catch-dog-foulers.html](http://www.telegraph.co.uk/news/newsttopics/politics/lawandorder/3485716/Town-halls-ordered-to-stop-using-terror-laws-to-catch-dog-foulers.html) (8. Jänner 2009).
- Wikipedia-Artikel zum Moore'schen Gesetz (2008):
http://de.wikipedia.org/wiki/Mooresches_Gesetz (6. Jänner 2009).
- Wikipedia-Artikel: 15 minutes of fame,
http://en.wikipedia.org/wiki/Fifteen_minutes_of_fame (6. Jänner 2009).
- Wirtschaftskammer Österreich (2008): Wirtschaftskammer Österreich gegen
Einrichtung betrieblicher Datenschutzbeauftragter: Zu hohe Kosten
ohne Mehrwert!, [http://portal.wko.at/wk/format_detail.wk?AnglID=
1&Std=401164&DstID=15](http://portal.wko.at/wk/format_detail.wk?AnglID=1&Std=401164&DstID=15) (6. Jänner 2009).
- Your voice on RFID (2006): Background document for public consultation
on Radio Frequency Identification (RFID) – Summary of five
workshops, [http://www.rfidconsultation.eu/docs/ficheiros/
Your_voice_on_RFID.pdf](http://www.rfidconsultation.eu/docs/ficheiros/Your_voice_on_RFID.pdf) (4. Februar 2009).

- Zimmermann, Philip (1991): Why I Wrote PGP,
<http://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html>
(6. Jänner 2009).
- Zsolt, Wilhelm (2008a): Porno-Industrie plant Klagen gegen Österreicher,
<http://derstandard.at/Text/?id=1224169785885> (6. Jänner 2009).
- Zsolt, Wilhelm (2008b): Datenweitergabe an Porno-Industrie: Telekom
Austria stellt Auskünfte ein,
<http://derstandard.at/Text/?id=1224169825646> (6. Jänner 2009).

Anhang

Abkürzungsverzeichnis

Ajax	Asynchronous JavaScript and XML
AT&T	American Telephone and Telegraph Corporation
bPK	bereichsspezifische Personenkennzahl
dDoS	Distributed Denial of Service (-Attacken)
DNA	Deoxyribonucleic acid (Desoxyribonukleinsäure, DNS)
DSG	Datenschutzgesetz
DSK	Datenschutzkommission
E-Com.	E-Commerce
ELGA	Elektronischer Gesundheitsakt
EMRK	Europäische Menschenrechtskonvention
ETH	Eidgenössische Technische Hochschule
EuGH	Europäischer Gerichtshof, amtlich: Gerichtshof der Europäischen Gemeinschaft
GDA	Gesundheitsdiensteanbieter
GPS	Global Positioning System
IP	Internet Protocol
ISP	Internet Service Provider
ISSN	Internationale Standardseriennummer
ITA	Institut für Technikfolgen-Abschätzung an der Österreichischen Akademie der Wissenschaften
LAN	Local Area Network
RFID	Radio Frequency Identification
ÖAW	Österreichische Akademie der Wissenschaften
ÖH	Österreichische HochschülerInnenschaft
P3P	Platform for Privacy Preferences
PIA	Privacy Impact Assessment
RSS	Really Simple Syndication (früher auch „Rich Site Summary“ oder „RDF (Resource Description Framework) Site Summary“)
SMS	Short Message Service (steht aber auch für die Nachricht selbst)
SOAP	Simple Object Access Protocol
SPG	Sicherheitspolizeigesetz
TKG	Telekommunikationsgesetz
VoIP	Voice over IP
W3C	World Wide Web Consortium
WLAN	Wireless LAN
XML	Extensible Markup Language
ZMR	Zentrales Melderegister

Glossar

Ajax

Ajax steht für Asynchronous JavaScript and XML, und bezeichnet damit die asynchrone Datenübertragung zwischen einem Webserver und einem Browser, wodurch innerhalb einer HTML-Seite ein HTTP-Request abgesetzt werden kann. Damit ist es möglich nur bestimmte Teile einer Webseite bei Bedarf nachzuladen.

Algorithmus

Ein Algorithmus ist die klar definierte Vorgehensweise zur Lösung eines Problems in endlich vielen Schritten.

Ambient Intelligence

Ambient Intelligence ist ein Forschungsansatz, bzw. ein technologische Paradigma, in dem die Umgebung eines Menschen intelligent(er) gemacht werden soll, durch das Ausstatten der Alltagsgegenstände mit der Fähigkeit zur Erfassung, Aufzeichnung, Verarbeitung und Weitergabe von Daten. Im amerikanischen Raum ist dafür der Begriff des „Ubiquitous Computing“ gebräuchlicher, in der Industrie wird oft von „Pervasive Computing“ gesprochen.

Application Service Provider

Der ASP stellt seinen KundInnen eine bestimmte Anwendung, die bei ihm betrieben und gewartet wird, über ein öffentliches Netz zur Verfügung und unterstützt die UserInnen bei der Benutzung.

Atom

Atom ist der Überbegriff für zwei Standards: für das „Atom Syndication Format“, ein XML-Format zum plattformunabhängigen Austausch von Informationen, und das „Atom Publishing Protocol“, das das Erstellen und Bearbeiten von Webinhalten mit einfachem HTML und XML ermöglicht.

Awareness Raising

Schaffen beziehungsweise intensivieren des Problembewusstseins zu einem bestimmten Thema.

Barcamp

Ein Barcamp ist eine offene Form einer Konferenz, die den partizipativen Charakter stark betont, bei der die Teilnehmer sowohl Ablauf als auch Inhalt bestimmen.

Barcode

Barcode ist die englische Bezeichnung für Strichcode.

Begriffswolke

Eine Begriffswolke (Schlagwortwolke, Stichwortwolke, engl.: tag cloud) ist eine Form der Visualisierung, bei der eine Liste von Stichworten (alphabetisch sortiert) auf einer Fläche dargestellt wird. Die einzelnen Worte werden entsprechend ihrer Gewichtung (zum Beispiel nach der Häufigkeit des Vorkommens) unterschiedlich groß oder unterschiedlich fett angezeigt; manchmal werden auch inhaltlich verwandte Begriffe in Nachbarschaft zueinander positioniert.

Biometrie

Biometrie beschäftigt sich mit der Vermessung von Lebewesen. Im Sicherheitsbereich ist damit meist die Merkmalerfassung von Menschen gemeint, die ein maschinelles Erkennen ermöglichen soll.

Blog

Siehe „*Weblog*“.

Bot-Net

Ein Bot-Net (Roboter-Netzwerk) ist ein Zusammenschluss fernsteuerbarer Computer im Internet. Die Kontrolle über die einzelnen Rechner mittels Fernsteuerung wird meistens mit Hilfe von Trojanern und Würmern übernommen, die nach der „Infizierung“ unauffällig auf weitere Befehle warten. Bot-Netze werden meistens zum Versand von Spam und für verteilte Angriffe auf andere Server genutzt.

Chat

Das englische Wort für „plaudern, unterhalten“ steht hier für eine Kommunikationsform über das Internet, bei der in Echtzeit kommuniziert wird; meistens in Form eines Textchats.

Chip

Bezeichnet einen Speicher aus Halbleitern, oder einen Mikroprozessor zur Verarbeitung von Anweisungen.

Cookies

Cookies sind kleine Textdateien, die Webseiten über den Browser auf der lokalen Festplatte ablegen und von dort wieder auslesen können. Dadurch können beispielsweise Besucher einer Webseite, wenn sie diese zuvor schon einmal aufgerufen haben, wiedererkannt werden, oder ihre Einstellungen können gespeichert und beim nächsten Besuch wieder hergestellt werden.

Cross-Media-Marketing

Aufeinander abgestimmte Kommunikations- und/oder Werbemaßnahmen, die verschiedene Medien benutzen, um eine Zielgruppe auf unterschiedlichen Wegen zu erreichen, oder mehrere Zielgruppen durch ihr bevorzugtes Medium zu erreichen.

Crowd-Sourcing

Crowd-Sourcing bezeichnet im Gegensatz zum Outsourcing nicht die Vergabe einer Aufgabe an eine Drittfirma, sondern die Auslagerung einer Aufgabe an eine breite Masse von unbezahlten FreizeitarbeiterInnen. Beispiele sind Wikipedia, OpenStreetMap u. a.

Datencenter

Siehe „*Rechenzentrum*“.

dDoS-Attacke

Das ist ein Angriff von verschiedenen Computersystemen auf eine Server mit dem Ziel diesen oder die Netzwerkverbindung zu diesem soweit zu überlasten, dass der Dienst, der darauf läuft, zusammenbricht oder nicht mehr erreichbar ist.

Digitale Signatur

Die digitale Signatur ist ein Wert, der sich mit kryptographischen Verfahren zu einer Nachricht (oder anderen digitalen Daten) errechnen lässt, und deren Zugehörigkeit und Unverfälschtheit von jedem kontrolliert werden können.

Direct-Marketing

Direct-Marketing ist eine Werbeform, die die potentiellen KundInnen direkt anspricht und zu einer Antwort an das Unternehmen auffordert.

Drohne

Eine Drohne ist ein unbemanntes Luftfahrzeug.

Feed

Ein Feed, oder Newsfeed, ist eine Transportform für elektronische Nachrichten.

Fotohandy

Ein Fotohandy ist ein Mobiltelefon mit integrierter Digitalkamera.

Funkzelle

Eine Funkzelle in einem Mobilfunknetz ist der Bereich, den ein Sendemast abdecken kann.

Geotagging

Geotagging ist das Zuordnen von (GPS-)Positonsdaten zu anderen Informationen (zum Beispiel zu Bildern).

Groupware

Groupware bezeichnet Software zur Zusammenarbeit in Computernetzen, oft in Zusammenhang mit E-Mail-Systemen, Wikis und dergleichen.

Herding

Herding (engl.) ist die Bezeichnung für das Hüten einer Herde, das im übertragenen Sinn verwendet wird, um die Betreuung eines Bot-Nets und der darin enthaltenen Rechner zu bezeichnen.

HTML-Editor

HTML-Editoren sind Programme, mit denen sich komfortabel HTML-Seiten erzeugen lassen, ohne dass man die Sprache HTML beherrschen muss.

Identitätsdiebstahl

Das Annehmen einer fremden Identität, meist um sich einen Vorteil daraus zu verschaffen.

Identity Management

Identity Management ist einerseits der bewusste und zielgerichtete Umgang mit seiner Identität, Pseudonymen und Anonymität. Andererseits kann damit auch das Management von verschiedenen Identitäten gemeint sein, die nicht zu einer Person, sondern zu einer Gruppe von Personen (zum Beispiel alle Mitarbeiter einer Firma) gehören.

IP-Adresse

IP-Adressen werden in IP-basierten Netzen (zum Beispiel dem Internet) dazu verwendet, Rechner, Netzknoten und andere erreichbare Systeme voneinander zu unterscheiden.

Keylogger

Ein Keylogger ist ein Computerprogramm, das jeden einzelnen Tastenanschlag mitprotokolliert. Meistens laufen sie versteckt für die BenutzerInnen im Hintergrund und spähen durch das Mitschreiben jeder Eingabe Account-Daten aus, die dann an den übermittelt werden können, der das Programm auf dem Rechner installiert hat.

Kryptographie

Ist die Wissenschaft von der Verschlüsselung von Informationen.

location-based-services

Sind mobile Dienste, die abhängig von Zeit, Ort und Userdaten dem Benutzer bestimmte Informationen oder Dienstleistungen zur Verfügung stellen.

Log-In

Ist der Vorgang der Anmeldung eines Benutzers/einer Benutzerin an einem Computersystem.

Magnetstreifenkarte

Ist eine Karte, die Informationen auf einem magnetischen Streifen bereithält.

Mash-Up

Ein Mash-Up im Web 2.0 ist die Erstellung neuer Inhalte durch die Kombination bereits bestehender Inhalte.

Mass-Customization

Mass-Customization vereint die Begriffe mass production und customization also Massenfertigung und Personalisierung. Mit Mitteln der Massenproduktion werden auf einem Massenmarkt Produkte hergestellt und vertrieben, die an den einzelnen Kunden bzw. die einzelne Kundin angepasst wurden und damit dessen/deren Wunsch nach mehr Individualität entsprechen.

Naked Machine

Die Naked Machine ist ein Terahertz-Scanner, der an Sicherheitsschleusen eingesetzt wird, um durch das Gewand von Menschen zu sehen, um festzustellen, ob sich darunter unerlaubte Gegenstände, wie Waffen beim Besteigen eines Flugzeugs, befinden. Das lässt die einzelnen Personen auf dem Kontrollschirm der Sicherheitsangestellten nackt erscheinen.

Offshoring

Bezeichnet das Auslagern von bestimmten Diensten in andere Länder, wo die Dienste günstiger erbracht werden können.

One-2-One-Marketing (1-1 Marketing)

1-1 Marketing bezeichnet das Individualisieren verschiedener Marketingmaßnahmen für einen bestimmten Kunden. Es wird nicht mehr nur personalisiert, wie im Direct-Marketing, sondern, auf Grund von detaillierteren Kundenprofilen, die mit Data-Mining- und CRM-Systemen aufgebaut werden, das gesamte Konzept an den jeweiligen Kunden angepasst. Dadurch lassen sich in der Regel höhere Response-Werte, Markentreue und dergleichen mehr erreichen.

Out-of-Office-Assistant

Ist die Funktion eines Mailserver, die bei Abwesenheit eines Benutzers/einer Benutzerin dessen/deren KommunikationspartnerInnen über seine/ihre Abwesenheit informieren kann.

Outsourcing

Bezeichnet das Auslagern von Geschäftsprozessen in Drittfirmen, um dort Synergieeffekte nutzen zu können. In der Regel erwartet man sich davon eine Kostenersparnis, weil sich das Unternehmen auf sein Kerngeschäft konzentrieren kann, und die Outsourcingfirma die spezielle Dienstleistung, als ihr Kerngeschäft, mehreren Kunden anbieten kann, was zu einer Rationalisierung der Abläufe führen sollte.

Pervasive Computing

Siehe „*Ambient Intelligence*“.

Phishing

Phishing ist ein Kunstwort aus den englischen Begriffen „Password“ und „Fishing“. Dadurch wird auch schon recht genau beschrieben, was damit gemeint ist: der Versuch eines Täters durch Vortäuschen bestimmter Identitäten oder Sachverhalte an Zugangsdaten elektronischer Identitäten der Opfer zu gelangen.

Podcast

Ein Podcast ist eine Audio- oder Videodatei, die erstellt wurde, um sie über das Internet anzubieten. Das Wort setzt sich aus „iPod“ und „broadcast“ zusammen.

Privacy Impact Assessment

Ein Privacy Impact Assessment versucht die Folgen für die Privatsphäre abzuschätzen und zu bewerten.

Privacy-Policy

Eine Privacy-Policy ist das Regelwerk, das den Umgang mit Daten im Hinblick auf die Privatsphäre festschreibt.

Provider

Ein Provider ist umgangssprachlich die Bezeichnung für die Firma, die einen Telefon-, Mobilfunk- und/oder Internet-Zugang ins jeweilige Netzwerk anbietet.

Quantencomputer

Ein Quantencomputer ist ein Rechner, dessen Funktionsweise auf den besonderen Gesetzen der Quantenmechanik beruht.

Quantenkryptographie

Die Quantenkryptographie ist ein Verfahren der Quanteninformatik, bei dem die Gesetze der Quantenmechanik genutzt werden, um zwei Parteien gleichzeitig die selbe geheime Zufallszahl zur Verfügung zu stellen, die daraufhin als Grundlage der Verschlüsselung zwischen den Parteien verwendet werden kann.

Rechenzentrum

Mit „Rechenzentrum“ kann sowohl das Gebäude, der Raum oder die Abteilung gemeint sein, in dem bzw. von der eine große Anzahl, meist leistungsstarker, zentraler Computersysteme betrieben wird.

RSS

RSS (Really Simple Syndication) ist eine Technologie zum Abonnement von Webseiten.

Section Control

Die Überwachung des Tempolimits auf Straßen, bei der die Durchfahrts- geschwindigkeit einer bestimmten Strecke gemessen wird, indem die Fahrzeuge über Kameras identifiziert werden bei der Einfahrt in und der Ausfahrt aus diesem Abschnitt. Im Falle einer Geschwindigkeitsübertretung können die erstellten Bilder den Strafverfolgungsbehörden übergeben werden.

Semantic Web

Das Semantic Web ist eine Erweiterung des World Wide Web, die es ermöglichen soll, Informationen und deren Bedeutung auch Maschinen verständlich zu machen.

smart dust

Smart dust ist die angepeilte Größe zukünftiger Sensorknoten in einem Netzwerk aus Sensoren.

Smartphone

Ein Smartphone stellt die Funktionen eines Mobiltelefons und eines Handheld/Personal Digital Assistant (PDA) in einem Gerät zur Verfügung.

Social Media

Social Media (auch Soziale Medien) ist die Bezeichnung für Webdienste und Internet-Plattformen zum gegenseitigen Austausch von Meinungen, Kommentaren und Erfahrungen beschrieben werden.

Social Tagging

Beschreibt das gemeinschaftliche Verschlagworten von Webinhalten.

Soziales Netz

Ist die Bezeichnung für Gemeinschaften, die über Web 2.0-Plattformen entstehen.

Spam

Als Spam werden vom Empfänger unerwünschte, meist massenhaft auf elektronischem Weg übertragene Nachrichten bezeichnet.

(RFID) Tag

Ein Tag (engl.) ist ein Etikett. RFID-Tags bezeichnen Etiketten, bei denen die Information nicht nur aufgedruckt ist, sondern zusätzlich auch auf einem RFID-Chip gespeichert ist.

Terahertz-Scanner

Sind Geräte, die mit Strahlung im Terahertz-Bereich Objekte und Menschen abtasten können. Je nach Intensität der Strahlung können verschiedene Barrieren damit durchdrungen werden.

Transistor

Ein Transistor ist ein elektronisches Halbleiterbauelement zum Schalten und Verstärken von elektrischen Signalen ohne mechanische Bewegungen.

Transponder

Ein Transponder ist ein Funk-Kommunikationsgerät, das eingehende Signale aufnimmt und automatisch beantwortet bzw. weiterleitet. Das Wort Transponder ist zusammengesetzt aus den Begriffen Transmitter und Responder. Transponder können passiv oder aktiv sein.

Twitter

Twitter ist ein soziales Netzwerk aus den UserInnen eines Mikro-Blogging-Dienstes. Angemeldete BenutzerInnen können Textnachrichten mit maximal 140 Zeichen senden und die Nachrichten anderer Benutzer empfangen.

Ubiquitous Computing

Siehe „*Ambient Intelligence*“.

Usenet-Group

Das Usenet ist ein weltweites, elektronisches Netzwerk, das Diskussionsforen („Newsgroups“ oder „Usenet-Groups“) bereitstellt und an dem jede/r teilnehmen kann. Die TeilnehmerInnen benutzen dazu meistens einen Newsreader.

Viral Marketing

Virales Marketing ist eine Marketingform, die existierende soziale Netze und Medien benutzt, um Aufmerksamkeit auf Marken, Produkte oder Kampagnen zu lenken, indem sich Nachrichten epidemisch wie ein Virus ausbreiten sollen.

Web-Portale

Als Web-Portale werden Websites bezeichnet, die entweder verschiedene Information bündeln oder für die AnwenderInnen sammeln, oder Sites, die der Startpunkt für die Benutzung einer Applikation, zum Beispiel eines Forums, sind.

Webcast

Ist ein Podcast, der über eine Webseite angeboten und über einen Browser konsumiert wird

Weblog

Das Wort „Weblog“ setzt sich aus (World Wide) Web und Log zusammen. Damit wird ein einem Tagebuch ähnliches Journal bezeichnet, das in Form einer Webseite geführt und veröffentlicht wird.

Wiki

Ein Wiki ist ein System für Webseiten, bei dem die BenutzerInnen die Inhalte nicht nur lesen, sondern auch online verändern können.

Zombie-Rechner

Ein Zombie-Rechner ist ein vernetzter Computer, der unter der Kontrolle eines Fremden, meist eines aus kriminellen Motiven handelnden Crackers, steht.