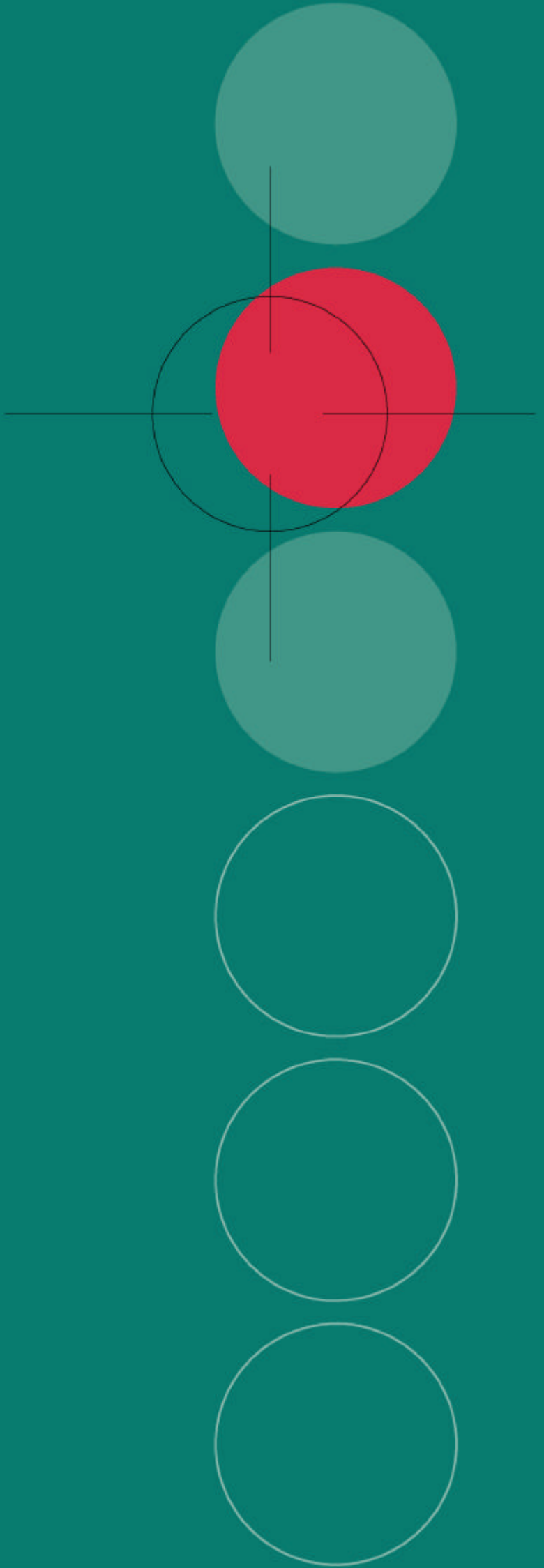
ÖSTERREICHISCHE
AKADEMIE DER
WISSENSCHAFTEN

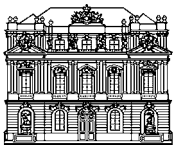
INSTITUT FÜR
TECHNIKFOLGEN-
ABSCHÄTZUNG

DATENVERMEIDUNG IN DER PRAXIS

INDIVIDUELLE UND GESELLSCHAFTLICHE VERANTWORTUNG

ENDBERICHT





DATENVERMEIDUNG IN DER PRAXIS

INDIVIDUELLE UND GESELLSCHAFTLICHE VERANTWORTUNG

ENDBERICHT

INSTITUT FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
DER ÖSTERREICHISCHEN AKADEMIE DER WISSENSCHAFTEN

Johann Čas
Walter Peissl

unter Mitarbeit von:
Thomas Strohmaier

STUDIE IM AUFTRAG DER BUNDESKAMMER FÜR ARBEITER UND ANGESTELLTE
WIEN, SEPTEMBER 2002

Inhalt

Zusammenfassung

Datenspuren durch Datenvermeidung verhindern

Der Alltag in der sogenannten „Informationsgesellschaft“ ist geprägt von elektronischen Systemen, die uns das Leben leichter machen sollen: (Mobil-)Telephon, Internet, Bankomatkarte, diverse Kundenkarten, in Zukunft auch die e-Card, der elektronische Krankenschein und die Bürgerkarte mit digitaler Signatur, die auch rechtsverbindliches Unterschreiben in der Online-Welt möglich machen soll. In dieser Online-Welt hinterlassen wir in immer größerem Ausmaß Datenspuren, viel mehr Spuren unserer Handlungen als etwa in der gewohnten Offline-Welt. Der Preis, den wir für die Bequemlichkeit bezahlen, ist die Durchschaubarkeit unseres Verhaltens und die mögliche Überwachung durch öffentliche Stellen ebenso wie durch private Unternehmen. Um dem Grundrecht auf eine unbeeinträchtigte Privatsphäre tatsächlich zum Durchbruch zu verhelfen, ist es notwendig, an der Wurzel zu beginnen: Datenvermeidung ist ein zentraler Faktor. Daten, die nicht entstanden sind, können auch nicht (missbräuchlich) verwendet werden. Ausgehend von diesem Befund wird in der Studie „Datenvermeidung in der Praxis – Individuelle und gesellschaftliche Verantwortung” der Frage nachgegangen, was die einzelnen KonsumentInnen tun können, wo die Grenzen individueller Schutzmaßnahmen liegen und wo Interessenvertretungen und Gesetzgeber gefordert sind. Konkret geht es dabei um folgende Forschungsfragen: In welchen Bereichen lässt sich Datenvermeidung ohne bzw. ohne gravierende Einbußen auf persönlicher Ebene erreichen, wo liegen die Grenzen dieser Strategie? Beispiele anhand derer diese Frage bearbeitet wird, sind die private Internetnutzung, die Verwendung von im Rahmen herkömmlicher Vertragsverhältnisse anfallender Daten durch Unternehmen (Stichwort Data Mining und Customer Relationship Management) sowie der Zugang zu öffentlichen e-Government Leistungen via Bürgerkarte. In welchen Bereichen sind gesetzliche Vorkehrungen bzw. Anpassungen geltenden Rechts notwendig, wo sind freiwillige Vereinbarungen denkbar, bei welchen Problemen sind technische Lösungen vorstellbar?

Forschungsfrage: Möglichkeiten und Grenzen individueller Vorsorge

Recht auf informationelle Selbstbestimmung

Grundlegend für die Studie und für modernen Datenschutz allgemein ist der Begriff des Rechts auf informationelle Selbstbestimmung (RaiS). Deshalb wird in einem ersten Abschnitt die Genese des mittlerweile klassischen Volkszählungsurteils des deutschen Bundesverfassungsgerichtshofes kurz skizziert und seine Implikationen für die juridische wie sozialwissenschaftliche Diskussion dargestellt. Kurz zusammengefasst ist das RaiS durch folgende Dimensionen gekennzeichnet:

- das Recht des Einzelnen, grundsätzlich selbst über die Verwendung und Preisgabe seiner Daten zu bestimmen und
- das notwendige aufgeklärte und freiwillige Einverständnis in Kenntnis des Verwendungszwecks.

Grundstein für EU-Datenschutzrichtlinie

Unumgängliche Einschränkungen dürfen nur im überwiegenden Interesse der Allgemeinheit erfolgen und müssen durch Gesetz (unter Beachtung der Normenklarheit und Verhältnismäßigkeit) legitimiert sein. Flankierend dazu sind organisatorische und verfahrensrechtliche Schutzvorkehrungen vorzusehen. Das RaiS bildet einen wesentlichen Grundstein auch für die Datenschutzrichtlinie der EU und die – soweit bereits umgesetzt – nationalen Regelungen der einzelnen EU-Mitgliedstaaten.

drei Säulen: gesetzliche Normen, freiwillige Selbstbeschränkungen und technische Vorkehrungen

Ein zunehmend wichtiger Bereich wird die private Internetnutzung, da die Zahl der NutzerInnen stetig ansteigt und durch die Entwicklung neuer Dienste von e-Commerce bis e-Government zusätzliche Bereiche erschlossen werden. Die Analyse einzelner Maßnahmen, durch die bewusste NutzerInnen ihre Privatsphäre schützen und bewahren können, zeigt, dass dies nur in dem Ausmaß gelingen kann, in dem auch die Säulen des Datenschutzes im Internet sich als tragfähig erweisen. Die drei wesentlichen Säulen, auf denen das Grundrecht auf Privatsphäre ruht, sind durch den Staat vorgegebene gesetzliche Normen, freiwillige Selbstbeschränkungen der Industrie und technische Vorkehrungen zur Datensparsamkeit und gegen missbräuchliche Datensammlung bei den Anbietern und den NutzerInnen von Informationstechnologien. Jede dieser Säulen ist notwendig, keine für sich allein ausreichend, um das Grundrecht auf Privatsphäre auch im Informationszeitalter absichern zu können. Was für verantwortliche, der Risken bewusste KonsumentInnen gilt, ist für sorglose NutzerInnen umso wichtiger. Natürlich kann und soll niemand gezwungen werden, aus seinem Privatleben ein gut gehütetes Geheimnis zu machen, ebenso wenig darf aber Unkenntnis oder Sorglosigkeit mit einem Verlust von Grundrechten verbunden sein. Unwissenheit schützt nicht vor Strafe, darf aber auch nicht dazu führen, dass Rechtsverletzungen ungehindert und ungestraft möglich werden.

bewusste NutzerInnen zentrales Element, aber auch Schutz für unbedachte Personen notwendig

Innerhalb der Wechselwirkungen zwischen dem Recht auf Privatsphäre jeder Einzelnen und den Säulen, auf denen es ruht, spielen die bewussten NutzerInnen eine zentrale Rolle. Dadurch, dass sie ihre Rechte wahrnehmen, tragen sie auch zur Stärkung von deren Basis bei. Indem sie auf ihre Rechte pochen, stärken sie sie; indem sie die Datenschutzpolitik der Anbieter bei ihren Konsumentscheidungen berücksichtigen, erhöhen sie die Bereitschaft zu datenschutzfreundlichen Selbstregulierungen; indem sie Privacy Enhancing Technologies für sich anwenden, fördern sie auch deren Weiterentwicklung und Verbreitung im Allgemeinen. Die Aufklärung und Schaffung von datenschutzbewussten KonsumentInnenen ist daher ein wesentliches Element einer umfassenden Strategie zur Wahrung des Grundrechts auf Privatsphäre, ohne aber dabei zu vergessen, dass gerade die unbedachten NutzerInnen eines besonderen Schutzes bedürfen.

vorbildliche rechtliche Rahmenbedingungen gefährdet

Bei den einzelnen Elementen eines umfassenden Schutzes der Privatsphäre ist ein uneinheitliches Bild zu erkennen. Die regulativen Rahmenbedingungen, die im Wesentlichen durch die EU-Richtlinien 95/46[1] und 97/66[2] vorgegeben sind, gelten (noch) als weltweit vorbildhaft. Sie sind aber auch den Bestrebungen von Ermittlungsbehörden ausgesetzt, die sich durch den erleichterten Zugang zu Telekommunikationsdaten bessere Aufklärungs- und Präventionsmöglichkeiten erhoffen. Diese Bestrebungen haben durch die Terroranschläge vom 11. September 2001 wesentlich an Gewicht und politischer Durchsetzbarkeit gewonnen und sind in eine Reihe von internationalen und nationalen Gesetzesnovellierungen gemündet, die erweiterte Überwachungsbefugnisse und die Speicherung von Verkehrs- und Inhaltsdaten beinhalten. Jüngstes Ereignis in dieser Kette ist die Annahme der Richtlinie „über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation“ durch das Europaparlament am 30.5.2002. Diese Richtlinie wird die Richtlinie 97/66 ersetzen; in ihr werden derzeit noch geltende Verpflichtungen zur Löschung von Verbindungsdaten gelockert und die teilweise in einigen EU-Staaten bereits beschlossenen Verpflichtungen zur Speicherung durch die Telekommunikations- und Internetbetreiber auf europäischer Ebene legalisiert. Es bleibt noch abzuwarten, welche konkreten Auswirkun-

[1] Europäisches Parlament und der Rat 1995.

[2] Europäisches Parlament und der Rat 1997.

gen die jüngsten Entwicklungen in einzelnen Staaten haben werden; die Weichen sind aber jedenfalls in Richtung gläserne BürgerInnen und KonsumentInnen gestellt.

geringe Durchsetzungskraft gesetzlicher Regelungen

Zurzeit sind die größten Defizite noch bei der Transformation des durch die EU-Richtlinien angestrebten Schutzniveaus und dessen Durchsetzung durch nationale Gesetze zu beobachten. Ein krasses Beispiel hierfür ist etwa der sehr geringe Anteil an ECG-konformen Webshops in Österreich (siehe Seite 18). Maßnahmen, die diese Diskrepanz verringern sollen, bilden daher einen wesentlichen Teil der Empfehlungen im entsprechenden Abschnitt weiter unten. Sie betreffen gesetzliche Änderungen zur Stärkung und Erweiterung der Kompetenzen der Datenschutzbehörden, zur Erleichterung des Zugangs zum Recht für die KonsumentInnen sowie die Rücknahme oder Verhinderung von Reformen, die das Grundrecht beeinträchtigt haben bzw. schmälern würden.

Erweiterung bestehender Ansätze zur Selbstregulierung

Im Bereich der Selbstregulierung zielen die Vorschläge darauf ab, vorhandene Ansätze wie das e-Commerce-Gütesiegels zu stärken und zu erweitern. Dazu gehört etwa eine forcierte Verankerung des österreichischen e-Commerce-Gütesiegels auf EU-Ebene und die Integration zusätzlicher Aspekte – etwa maschinenlesbare Datenschutzpolitiken gemäß P3P oder der Verzicht auf die Datengewinnung durch Cookies –, um es auch als Datenschutzsiegel etablieren zu können.

verbesserter Zugang zu Privacy Enhancing Technologies

Im Bereich Datenschutz durch Technik sind zwei Maßnahmenbündel notwendig. Das erste Paket muss darauf abzielen, den KonsumentInnen den Zugang zu diesen Technologien zu erleichtern, indem sie sich etwa an eine vertrauenswürdige Stelle bspw. einen Datenschutz-Ombudsmann wenden können, um aktuelle Hilfestellungen zu erhalten. Die zweite Stoßrichtung zielt darauf ab, Datensparsamkeit an der Quelle, d. h. bei den Betreibern von Internetdiensten durch Technikeinsatz zu fördern.

„Surfen kann Ihre Privatsphäre gefährden!“

Als übergreifende Maßnahme zur Bewusstseinsschaffung bieten sich Warnhinweise an, die an geeigneter Stelle – etwa Rechnungen von Telekom- und Internetprovidern – zu platzieren sind und KonsumentInnen zugleich Zugangsmöglichkeiten für weitere Informationen eröffnen.

Schwieriger stellt sich die Frage des Datenschutzes im Bereich Data Mining – CRM dar:

wenig Wissen und Bewusstsein über Data Mining

Die einzelne KonsumentIn kann kaum wissen und umso weniger beeinflussen, inwieweit ihre Daten in Data Mining Prozessen erfasst und verarbeitet werden. Damit sind auch der individuellen Verantwortlichkeit enge Grenzen gesetzt. Data Mining findet im Verborgenen statt und entzieht sich weitgehend der Kenntnis und dem Bewusstsein der Betroffenen. Als aufgeklärte KonsumentIn muss man davon ausgehen, dass die meisten größeren Unternehmen, mit denen man in geschäftlichen Kontakt tritt, Data Mining betreiben. Eine bestehende Geschäftsbeziehung ist aber keine notwendige Bedingung, um von Datenanalysen erfasst zu werden. Im Gegenteil ist anzunehmen, dass die Daten professioneller Anbieter vielfach bei gezielten Werbeaktionen, bei der Selektion potentieller Neukunden oder der individuellen Angebotserstellung und Preisgestaltung herangezogen werden. „Profilhändler sind mittlerweile in der Lage, ganz spezifische Persönlichkeitsprofile zu liefern. Hierfür werden hochsensitive Daten aus der privaten Lebenssphäre erfasst, mit vielfältigen öffentlich zugänglichen Daten kombiniert und für Marketing- und andere Zwecke weiterverkauft oder zum Leasing angeboten“ (Roßnagel et al. 2001, 24).

kaum direkte Einflussmöglichkeiten

Angesichts der nur sehr geringen Einflussmöglichkeiten einzelner KonsumentInnen auf die Art und Weise, in welcher mit ihren Daten in Unternehmen verfahren wird, lassen sich dementsprechend wenige konkrete Empfehlungen

für KonsumentInnen formulieren. So mündet ein ausführlicher Bericht der kanadischen Datenschutzkommission über das Thema Data Mining in zwei Ratschlägen für KonsumentInnen; der erste zielt darauf ab, bei Unternehmenskontakten aktiv nach der Datenschutzpolitik zu fragen bzw. auf die Respektierung seiner Vorgaben zu pochen, der zweite Vorschlag lautet, nur die für die jeweilige Transaktion mindestens erforderlichen Daten bekannt zu geben (Cavoukian 1998). Die Empfehlungen setzen auf den Einfluss bewussten Konsumentenverhalten, indem etwa Daten nur sparsam freigegeben werden oder durch Einbeziehung des Datenschutzverhaltens bei den Konsumentscheidungen entsprechende Anreize für konformes Verhalten von Unternehmen geboten werden.

neue Gefahren durch Unternehmenskonzentrationen und Outsourcing

Wie bei Datensammlungen im Allgemeinen besteht auch bei Data Mining ein großes Gefahrenpotential darin, dass bei entsprechender Datenbasis sehr umfassende Persönlichkeitsprofile erstellt werden können. Der Umfang der Datenbasis ist durch eine zeitliche Dimension und die Menge an Beobachtungen determiniert. Die zeitliche Dimension lässt sich durch ein Verbot längerfristiger Speicherung personenbezogener Daten einschränken. Die Menge an Daten, die Data Mining Analysen zugeführt werden kann, hängt einerseits von den Möglichkeiten ab, auf Fremddaten zuzugreifen, andererseits vom Umfang der Geschäftstätigkeit des betroffenen Unternehmens. Kritische Bereiche sind hier etwa Telekommunikationsunternehmen; insbesondere wenn traditionelle Telekommunikation, Mobilkommunikations- und Internetdienste von einem Unternehmen bezogen werden, sind reale Gefahren des gläsernen Menschen nicht von der Hand zu weisen. Ein weiterer kritischer Bereich entsteht bei der Auslagerung von Geschäftsprozessen in externe Unternehmen. Ein prominentes Beispiel ist hierfür die Kundenbetreuung durch Call Centers. Da hier Kunden unterschiedlicher Unternehmen auf ein und derselben technischen Infrastruktur betreut werden, ist rechtlich und organisatorisch dafür Sorge zu tragen, dass keine unternehmensübergreifenden Datenauswertungen stattfinden können. Analoge Vorkehrungen werden im öffentlichen Bereich zu treffen sein, wenn im Rahmen von e-Government-Initiativen One-Stop-Zugangsmöglichkeiten zu öffentlichen Diensten realisiert werden. Wie in vielen Bereichen des Rechts auf Privatsphäre ist auch hier nicht eine grundsätzlich fehlende Regulierung das vorrangige Problem, es geht in erster Linie darum, die Effektivität und Durchsetzungskraft rechtlicher Normen zu erhöhen, und gegebenenfalls geltende Regeln an neue technische Herausforderungen anzupassen.

„freiwillige" Beschränkungen bedürfen unterstützender Maßnahmen

Data Mining ist in wesentlichen Schritten ein unternehmensinterner Prozess, der auch ohne rechtlich unzulässige Verwendungen von Fremdaten oder von Daten mit Personenbezug durchgeführt werden kann. Viele, auch für Unternehmen wertvolle, statistische Aussagen und Zusammenhänge können auf Basis anonymisierter Daten ermittelt werden. Freiwillige Einschränkungen auf Seite der Unternehmen können daher einen großen Beitrag zur Wahrung der Privatsphäre liefern. Allerdings widerspricht ein allgemeiner Verzicht auf personalisierte Auswertungen grundsätzlichen unternehmerischen Interessen. Für eine Vielzahl von Verwendungen, beispielsweise individualisierte Angebote oder gezielte Werbemaßnahmen im Rahmen des CRM, ist eine Personalisierung unumgänglich. Ein „freiwilliger" Verzicht auf personenbezogene Auswertungen oder Anwendungen ist ohne entsprechende regulative Beschränkungen oder öffentlichen Druck bzw. einem drohenden Verlust an Reputation kaum realistisch. Die Bereitschaft seitens der Unternehmen, die Privatsphäre der Kunden zu achten, wird zu einem wesentlichen Teil davon abhängen, ob es gelingt, den in zahlreichen empirischen Erhebungen festgestellten hohen Stellenwert des Datenschutzes den Unternehmen in spürbarer Weise zu vermitteln. Eine Voraussetzung dafür ist es, die KonsumentInnen auch in diesem Bereich zu sensibilisieren und ihnen Unterstützung dabei anzubieten, wie sie Informationen einholen oder ihre Interessen durchsetzen können. Es müssen

aber auch Unternehmen Möglichkeiten geboten werden, datenschutzkonformes Verhalten und die Einhaltung freiwilliger Vereinbarungen auf einfache Weise zu kommunizieren, sowohl um ihnen einen Wettbewerbsvorteil zu eröffnen als auch den KonsumentInnen eine Entscheidungshilfe zu bieten. Natürlich ist auch beim Zustandekommen von wirksamen Formen der Selbstregulierung der Gesetzgeber gefragt, indem er etwa Leitlinien und zu erfüllende Mindeststandards vorgibt und durch die Androhung von Zwangsausübung untermauert.

Für den Bereich Bürgerkarte stellen sich ausgehend von den Forschungsfragen der Studie folgende zentrale Fragen: Was kann die Einzelne selbst tun? Wie steht es um freiwillige Selbstbeschränkung und wie schaut die staatliche Regulierung aus?

Alternativen zur Bürgerkarte nutzen

Die Antwort auf die erste Frage lautet eindeutig: die e-Card nicht als Bürgerkarte zu verwenden. Obwohl elektronische Signaturen im Geschäftsverkehr für zusätzliche Sicherheit der Abwicklung sorgen werden, werden sie wohl eher im Bereich des B2B und nicht so sehr im B2C relevant sein. Für Abwicklungen, die elektronische Signaturen vorsehen, sind für KonsumentInnen über weite Strecken auch einfachere und damit billigere Zertifikate ausreichend. Wo sichere Signaturen und qualifizierte Zertifikate notwendig sein werden, können diese auf Basis von Pseudonymen genutzt werden. Wie im Bereich über die Internetnutzung ausgeführt, gibt es Ansätze auch im Internethandel Anonymität sicherzustellen. Diese sind zu stärken und zu nutzen. Was die Anwendungen im e-Government betrifft, so ist von einer langen Übergangszeit und einer nur geringen Anzahl von realen Einsatzmöglichkeiten auszugehen, sodass die Kosten für eine sichere Signatur mittelfristig den zu erwartenden Nutzen weit übersteigen werden. Erste Anwendungen werden für Unternehmen und bestimmte eng umgrenzte Gruppen von BürgerInnen (z. B. StudentInnen) zur Verfügung stehen. Für diese stellt sich die Frage ob nicht eine eigene „Signaturkarte“ (die dasselbe kostet wie die Signatur auf der e-Card) der bessere Weg ist. Darüber hinaus sind die Info-Boxen in ihrer rechtlichen Einordnung nicht hinreichend geklärt, was zu haftungsrelevanten Fragestellungen für die BürgerInnen führen kann. Auch hier ist Skepsis angebracht.

ungenütztes Potential zur Selbstbeschränkung im Bereich „e-Government“

Die Selbstbeschränkung der „Branche e-Government“ könnte aus Sicht des Datenschutzes effizienter ausfallen – das Konzept Bürgerkarte könnte datenschutzfreundlicher gestaltet werden: Keine Speicherung der ZMR-Zahl auf der Karte, da diese ein ungeheuer großes Potential zur universellen Verwendung in sich trägt (Problematik Personenkennzahl), aber auch Weglassen der verpflichtenden Personenbindung. Man sollte Möglichkeiten schaffen, die Anbringen auch mit elektronischen Signaturen lt. SigG (Pseudonyme) zuzulassen. Die zusätzliche Schaffung eines wirklich freiwilligen „elektronischen Ausweises“, den die BürgerInnen bei Bedarf einsetzen oder eben auch nicht, stünde dem nicht im Wege. Ein nicht zu unterschätzendes Problem stellen intransparente, komplexe Multifunktionskarten dar, weshalb auch hier eine Beschränkung wünschenswert erscheint. Insbesondere Bemühungen aus dem Bereich Private-Public-Partnership, die die Bürgerkarte gemeinsam mit der Bankomatkarte realisieren wollen, erscheinen problematisch. Die zu enge Verbindung von hoheitlichen und privaten Aktivitäten birgt ein zusätzliches Potential zum Profiling, dem entgegenzuwirken ist.

fehlende Vorbildfunktion des Staates

Die staatliche Regulierung ist derzeit eher zersplittert, da unterschiedliche Bereiche betroffen werden. Zu überlegen wäre, ob es nicht im Sinne eines klaren, die BürgerInnen transparent informierenden Ansatzes sinnvoll wäre, einen gesetzlichen Rahmen (e-Government-Gesetz) zu formulieren, der den Staat als Vorbild heraushebt, die Prinzipien modernen Datenschutzes ernst nimmt und in den Mittelpunkt der Überlegungen stellt.

mehr Bürgerbeteiligung bei der Einführung der Bürgerkarte

Zusammenfassend ist festzuhalten, dass die rechtliche Freiwilligkeit der Bürgerkarte eine notwendige aber nicht hinreichende Bedingung darstellt. Bei voller Diffusion der e-Card (99 % SV-Versicherte) kann ein hohes Maß an sozialem Druck zur Verwendung entstehen. Was den Bestrebungen insgesamt fehlt, ist eine öffentliche Diskussion der Vor- und Nachteile des e-Government unter Einsatz der Bürgerkarte und ihrer unterschiedlichen Ausprägungen. Insbesondere die sozialen und wirtschaftlichen Folgen wären zu diskutieren. Die Bürgerkarte im Kontext e-Government ist ein techno-organisatorisches System mit einem großen Maß an Gestaltungsfreiheit und auch für den Einzelnen interessanten Aspekten, die zudem in der tagespolitischen Debatte noch nicht zu einzementierten Positionen geführt hat – ein ideales Thema für eine vorausschauende, die Wünsche und Sorgen der Betroffenen einbeziehende partizipative Technikfolgen-Abschätzung.

1 Einleitung

In der Studie „Beeinträchtigung der Privatsphäre – Datensammlungen über ÖsterreicherInnen“ (Peissl und Čas 2000), wurde eine fundierte Abschätzung vorgenommen, welche Daten eines durchschnittlichen Österreichers von wievielen Institutionen gesammelt und verarbeitet werden. Dabei zeigte sich, dass insbesondere bei der Nutzung von Telekommunikationsdiensten und Neuen Medien viele und teilweise sehr sensible Daten generiert werden. Im Unterschied zur Offline-Welt hinterlässt jede Regung in der Online-Welt digitale Spuren, die gespeichert, gesammelt, kombiniert und ausgewertet werden können. Daraus lassen sich umfassende Informationssammlungen bilden, die nicht nur Auskunft geben, mit wem man kommuniziert und wo man sich aufgehalten hat, sondern auch persönliche Interessen, politische Einstellungen oder sexuelle Vorlieben preisgeben können. Sind diese Daten einmal digital erfasst, so bleiben sie für sehr lange Zeiträume zugreifbar und auswertbar. Damit sind vielfältigen Ge- und Missbräuchen Tür und Tor geöffnet, wobei die Grenzen zwischen diesen beiden Kategorien fließend sind. Dieser Problemkreis wird durch die zunehmende Nutzung von e-Commerce Anwendungen oder die beabsichtigte Einführung einer Bürgerkarte in Österreich für eine immer größere Anzahl von KonsumentInnen relevant. Auch in der entsprechenden EU-RL wird dem Zweckbindungsprinzip hohe Priorität eingeräumt. Um eindeutig von einer berechtigten Nutzung sprechen zu können, müsste aber jedes Mal eine bewusste Freigabe der Daten für einen bestimmten Zweck vorliegen. Angesichts der zunehmend unmerkbaren und daher nicht bewussten Erhebung von Daten, der Weitergabe und Nutzung in anderen Kontexten, und der Zeitspanne, die zwischen Erhebung und Auswertung liegt, werden diese klaren Vorgaben meist nicht eingehalten.

von digitalen Spuren zu Persönlichkeitsprofilen

Aus der Sicht des Datenschutzes spielt deshalb die Datenvermeidung eine zentrale Rolle für die Wahrung der Privatsphäre. Dabei wird direkt an der Quelle der Generierung der Daten angesetzt: Dem Vorsorgeprinzip entsprechend, soll durch technisch-organisatorische Gestaltung oder durch die Einhaltung von entsprechenden Verhaltensmaßregeln gar keine bzw. so wenig Daten mit Personenbezug als möglich entstehen, und auf diese Weise die Gefahr des Missbrauchs verhindert werden. In einem Abschnitt der ersten Studie wurden Empfehlungen und Maßnahmen ausgearbeitet, mit denen sich KonsumentInnen im Internet und bei Telekommunikationsdiensten vor allzu großem Datenhunger schützen können. Allerdings stoßen die individuellen Bemühungen oft auf Grenzen; sei es, dass Unbequemlichkeiten in Kauf genommen werden müssen, dass einzelne Angebote nicht oder nur eingeschränkt nutzbar sind, oder dass einfach die Kenntnisse nicht vorhanden sind, die notwendig sind, um bestimmte Gefahren zu erkennen oder Datenschutztools einsetzen zu können. In Zukunft wird es noch schwieriger werden, sich bei der Wahrung der Privatsphäre auf persönlich durchzuführende Maßnahmen zu stützen. Zum einen durchdringen Kommunikationstechnologien immer mehr Lebensbereiche und ein Verzicht oder eine Einschränkung von deren Nutzung ist mit einer vollen Teilhabe am wirtschaftlichen und sozialen Leben oft unvereinbar. Zum anderen wird die Generierung immer weniger an aktives Verhalten gebunden sein: biometrische Verfahren, oder Informationstechnologien, die in Gebrauchsgegenständen und in die alltägliche Umgebung integriert sind, bedürfen keiner aktiven Handlungen der NutzerInnen um Datenspuren zu hinterlassen.

individuelle Datenvermeidung wichtig, …

… aber nicht immer möglich

Die vorliegende Studie zeigt die Grenzen individueller Verantwortlichkeit auf und identifiziert jene Felder, in denen Interessensvertretungen, die Politik und die Industrie gefordert sind, zwingende oder freiwillige Vereinbarungen zum Schutz der Privatsphäre zu treffen. Diese Vereinbarungen können auch tech-

Unterstützung durch Politik und Wirtschaft notwendig

nisch-organisatorische Vorkehrungen betreffen, welche das Prinzip der Datenvermeidung in Hard- oder Software sowie in die Gestaltung von Zugangs- und Abrechnungssystemen integriert. Gerade dem Datenschutz durch die Technik ist besonderes Augenmerk zu schenken, wie die Ereignisse der letzten Monate zeigen, in denen es in Folge des 11. September 2001 in einigen Staaten ein prinzipielles Verbot der Speicherung von Telekommunikationsverkehrsdaten in eine generelle Verpflichtung zur langfristigen Aufbewahrung dieser Daten mutiert ist. Aktuellstes Beispiel dazu ist die Schweiz, in der eine verpflichtende Speicherung von Telekommunikationsdaten für 6 Monate eingeführt werden soll (Bleicher und Imfeld 2002).

1.1 Zu bearbeitende Forschungsfragen

Forschungsfrage 1: In welchen Bereichen lässt sich Datenvermeidung ohne bzw. ohne gravierende Einbußen auf persönlicher Ebene erreichen, wo liegen die Grenzen dieser Strategie? Als Beispiele, anhand derer diese Frage bearbeitet wird, dienen die private Internetnutzung, der Zugang zu öffentlichen e-Government Leistungen via Bürgerkarte und die Verwendung von im Rahmen von herkömmlichen Vertragsverhältnissen anfallenden Daten durch Unternehmen (Stichwort Data-Mining und Customer Relationship Management – CRM).

Forschungsfrage 2: In welchen Bereichen sind gesetzliche Vorkehrungen bzw. Anpassungen geltenden Rechts notwendig, wo sind freiwillige Vereinbarungen denkbar, bei welchen Problemen sind technische Lösungen vorstellbar?

2 Das Recht auf informationelle Selbstbestimmung als Basis modernen Datenschutzes

2.1 Datenschutz und informationelle Selbstbestimmung

Die rechtspolitische Zielsetzung von Datenschutzgesetzen ist nicht in allen Fällen eindeutig zu erkennen. Blickt man zum Beispiel in nationale Regelungen Norwegens, Dänemarks, Islands oder des Vereinigten Königreiches, findet man keinerlei Hinweise. Etwas deutlicher ist da beispielsweise schon Österreich, wo vom Anspruch auf Geheimhaltung personenbezogener Daten die Rede ist und der Achtung des Privat- und Familienlebens. Eine kurze Würdigung grundlegender Datenschutz-Konzepte lohnt deshalb und dient dem besseren Verständnis[3].

Zweckbindung ist ein entscheidendes Element

„Kontext-orientierte" Konzepte sehen Datenschutz vor allem als Interessenausgleich zwischen der von einer Datenverarbeitung betroffenen Person und dem Verantwortlichen einer Datenverarbeitung (folgend: der Verantwortliche). Ob ein Datum sensitiv ist, ist im konkreten Zusammenhang (im Kontext) mit seiner Verwendung zu bestimmen. Große Bedeutung wird der Relevanz, der Adäquanz und der sparsamen Verwendung von Daten in Hinblick auf den Zweck einer konkreten Datenverarbeitung beigemessen. Prominentes Beispiel für diesen Ansatz ist die Datenschutzkonvention des Europarates (Art 5 lit c)[4]. Wie noch gezeigt wird, ist gerade diese „Zweckbindung" zentrales Element wirksamer Datenschutzgesetzgebung. Das Kontext-Konzept soll zusammengefasst die Vertraulichkeit, die Sicherheit und die Transparenz der Datenverarbeitung gewährleisten. Letzteres etwa durch die Information der Betroffenen.

Kontrolle und Bestimmung durch die Betroffenen

„Personen-orientierte" Konzepte stellen hingegen die Person in den Mittelpunkt der Betrachtung. Hier finden sich Begriffe wie „privacy" oder „personal integrity". Als prominenter Vertreter lässt sich hier wiederum die Datenschutzkonvention des Europarates[5] nennen, aber auch die Datenschutzrichtlinie der EU.[6] Das Privacy-Konzept ist zwar schwer fassbar, es lassen sich aber drei Hauptkriterien festmachen. Neben dem Kriterium des „right to be let alone" (Warren und Brandeis 1890, 193ff) und dem Schutz der Autonomie und Kontrolle über die Intimsphäre, ist es vor allem die Informationskontrolle und die Selbstbestimmung. Mit den Worten von Alan F. Westin:

> „Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others." (Westin 1967, 7)

---

[3] Zu den Datenschutzkonzepten vgl. *Bygrave and Berg 1995.*

[4] Dieses Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten wurde in Österreich mit BGBl 1988/317 in innerstaatliches Recht umgesetzt und trat am 1.7.1988 in Kraft.

[5] Dort wird der Zweck der Konvention in Art 1 insbesondere mit dem „... right to privacy ..." umschrieben.

[6] Art 1 Abs 1 spricht vom „... Schutz der Privatsphäre"; Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

informationelle Selbstbestimmung

Der Kern dieser Aussage findet sich unter dem Titel „Recht auf informationelle Selbstbestimmung“ (folgend: RaiS) in jeder Datenschutzdebatte. Die rechtliche Fundierung fand das RaiS im weiter unten näher behandelten „Volkszählungsurteil“ des deutschen Bundesverfassungsgerichts vom 15.12.1983. Die beiden oben dargestellten grundsätzlichen Datenschutzkonzepte schließen einander nicht aus, sondern ergänzen einander. Nur in ihrer Kombination lassen sich wirksame Datenschutzlösungen finden, die sowohl dem Bedürfnis des Einzelnen, als auch dem Wunsch nach Datenverarbeitung Rechnung tragen.

2.2 Darstellung der Kriterien des RaiS anhand des „Volkszählungsurteils“des deutschen Bundesverfassungsgerichts

deutsches Volkszählungsurteil richtungsweisend

Das genannte Urteil[7] darf als datenschutzrechtlicher Meilenstein bezeichnet werden und hat den Begriff der „informationellen Selbstbestimmung“ wie kein anderes geprägt und Wirkungen auch außerhalb der rein juridischen Debatte gehabt. Gerade bei Volkszählungen wird regelmäßig eine Vielzahl personenbezogener Daten gesammelt und verarbeitet. Grundrechte können dadurch beeinträchtigt werden, sodass auch bei gesetzlich vorgeschriebenen Datenverarbeitungen durchaus Vorsicht geboten sein kann. Die nähere Betrachtung des Urteils lohnt unter anderem aus folgenden Gründen:

Beispielhaft dafür gelten:

1. Enthält das Urteil die wichtige Feststellung eines „letzten unantastbaren Kernbereiches privater Lebensgestaltung“?
2. Bietet gerade in Zeiten erhöhter „Überwachungstätigkeit“ die Argumentation des BVerfG eine fast zeitlose Richtschnur dafür, wie weit Datenverarbeitung in einer demokratischen Gesellschaft maximal gehen sollte?
3. Steht eine Volkszählung auch paradigmatisch für den weiten Bereich des Datamining; wo sonst als im Wege der Volkszählung bekommt man so viele personenbezogene Daten?

Grundrecht auf informationelle Selbstbestimmung

Das konkrete Urteil hat das RaiS aber auch als Grundrecht anerkannt.[8] Die Entscheidung wurde vom BVerfG zwischenzeitig mehrmals bestätigt und 1991 sogar ausdrücklich vom „Grundrecht auf Datenschutz“ gesprochen.[9] Schließlich hat das BVerfG den Anwendungsbereich des RaiS über das Verhältnis Staat – Bürger hinaus auf das Verhältnis Bürger – Bürger (dies wird als Drittwirkung von Grundrechten bezeichnet) erweitert. Die Entscheidung hat bis

---

[7] BVerfGE 65,1; Urteil vom 15.12.1983.

[8] Im Gegensatz zum österr. DSG, war (und ist) im deutschen BDSG der Datenschutz kein Grundrecht. Gerade aber dieser Umstand macht die Diskussion des Urteils interessant, da eine umfassende inhaltliche Würdigung des RaiS stattfand, die so in Österreich nie abgehalten wurde. Wie aktuell die Entscheidung im dt. Kontext noch immer ist, zeigen völlig „druckfrische Entscheidungen“, zuletzt vom 27.5.2002, BVerfG 2 BvR 742/02. Hier hat das BVerfG ausdrücklich auf seine „Volkszählungsentscheidung“ rekurriert (im Zusammenhang mit der Auslegung einer Bestimmung der Strafprozessordnung iVm. Vorschriften des Börsen- und Wertpapiergesetzes). Der Hinweis auf das RaiS findet sich auch in der erfolglos gebliebenen Beschwerde von n-tv, die gerne „Gerichtsfernsehen“ übertragen wollten (BVerfG-Urteil vom 24.1.2001 – 1 BvR 2623/95. 1 BvR 622/99).

[9] Abgedruckt in NJW 1991, 2129, 2132; vgl. dazu auch *Vogelgesang*, Verfassungsregelungen zum Datenschutz, CR 1995, 554.

heute nichts von ihrer Schlagkraft eingebüßt.[10] Schließlich findet das Instrument „Volkszählung“ auch weiterhin Verwendung[11], was eine kritische Auseinandersetzung schon mit Blick auf künftige Entwicklungen nötig macht.

2.2.1 Ausgangssituation

Anlass Volkszählungsgesetz 1983

Das deutsche Bundesverfassungsgericht (folgend BVerfG) musste sich aufgrund zahlreicher Verfassungsbeschwerden mit dem Gesetz über eine Volkszählung, Berufszählung, Wohnungszählung und Arbeitsstättenzählung – dem Volkszählungsgesetz 1983[12] – auseinandersetzen.

Die generelle Kritik der Beschwerdeführer richtete sich u. a. gegen die „veraltete“ Methode der „Zwangserhebung“ unter Hinweis auf das Instrument der „anonymen Datenerhebung“. Die Einzelperson werde der freien Selbstbestimmung beraubt und zum Gegenstand fremder Willensausübung und Kontrolle. Die Melderegister auf kommunaler Ebene könnten sich zunehmend zu Einwohnerdatenbanken entwickeln. Persönlichkeitsprofile seien möglich. Der Bürger sei nicht über die geplanten Verarbeitungen und Datenübermittlungen informiert.

In rechtlicher Hinsicht wurde – nicht zuletzt da auch ein Datenabgleich der Angaben der Betroffenen mit dem Melderegister vorgesehen war – die verfassungswidrige Verknüpfung von Statistik und Verwaltungsvollzug gerügt. Das Zählorgan habe damit eine Doppelrolle: „Kundschafter der örtlichen Meldebehörde und Vollzieher der Bundesstatistik“.

Widersprüche zu rechtsstaatlichen Prinzipien

Das aus dem allgemeinen Persönlichkeitsrecht folgende Gebot der Anonymität verbiete den Personenbezug zu Individuen und Gruppen. Die gesetzlich angeordnete Auskunftspflicht verletze das Grundrecht auf negative Meinungsfreiheit, nämlich bestimmte Tatsachen nicht mitteilen zu müssen. Auch das Rechtsstaatsprinzip sei verletzt, da der Bürger zur Selbstbezichtigung gezwungen werde. Niemand soll aber im (Verwaltungs-)Strafverfahren gezwungen sein, sich selbst zu beschuldigen. Kritisiert wurden auch die im VolkszählungsG sehr undeutlich formulierten Übermittlungsregelungen. Diese würden gegen das verfassungsrechtliche Bestimmtheitsgebot verstoßen.

Exkurs

die österreichische Situation im Vergleich

Die Situation heute in Österreich stellt sich einigermaßen anders dar. Hier regelt das Meldegesetz[13] und die dazu ergangene Durchführungsverordnung[14] den entsprechenden Bereich. Neu ist das Identitätsdatum der Melderegisterzahl (ZMR-Zahl). Die Behörden dürfen gemeinsam mit den Meldedaten Hinweise auf Verwaltungsverfahren verarbeiten. Nur die Ordnung der Daten nach dem Religionsbekenntnis ist verboten. Zur Aktualisierung des Melderegisters dürfen Daten auch aus Datenermittlungen ermittelt werden, die von Organen der Gemeinden geführt werden (diese sind übrigens auch zur Übermittlung verpflichtet). Das Register ist insofern ein öffentliches, als der (letzte) Hauptwohnsitz eines Menschen abgefragt werden kann, wenn man eine Anfrage mit Vor- und Familiennamen, Geburtsdatum und einem zusätzlichem Merkmal

---

[10] Vgl. zum RaiS auch EuGH-Urteil vom 5.10.1994, NJW 1994, 3005 ff, wonach davon auch das Recht einer Person auf Geheimhaltung ihres Gesundheitszustandes erfasst ist.

[11] Selbst wenn sein Einsatz angeblich schwindet; vgl. dazu die angeblich „letzte“ Totalerfassung in Österreich zuletzt im Jahr 2001.

[12] (deutsches) BGBL I S 369 – VZG 1983.

[13] BGBl. Nr. 9/1992, zuletzt geändert dr. BGBl. II Nr. 66/2002 (V über Idat).

[14] BGBL II Nr. 66/2002, in Kraft seit 1.3.2002.

(z. B. Geburtsort oder ZMR-Zahl)[15] angeben kann. Unter bestimmten Voraussetzungen kann dies auch durch Datenfernübertragung geschehen. Andere Wohnsitzauskünfte bedürfen des Nachweises eines berechtigten Interesses. Das Zentrale Melderegister ist ein Informationsverbundsystem iS § 4 Zif 13 DSG 2000. Für statistische Zwecke ist auch die gemeinsame Verarbeitung mit den von der Sozialversicherung zugeordneten Versicherungsnummern möglich (Gleichsetzungstabelle). Die Statistik Österreich hat die personenbezogenen Daten zu anonymisieren und den Ländern und Gemeinden (Wanderungsstatistik) zur Verfügung zu stellen.

bedenkliche Verschränkungen von Volkszählungs- und Meldedaten

Die im ZMR gespeicherten Daten dürfen weiters für statistische Zwecke u a. an Organe der Bundesstatistik übermittelt werden, und zwar zumindest in für den Empfänger indirekt personenbezogener Form, sofern der Personenbezug für die Durchführung der Untersuchung nicht unerlässlich ist (siehe § 16 b MeldG). In Österreich sind also gesetzlich personenbezogene Statistiken möglich. Auch dürfen anerkannte Religionsgesellschaften die Meldedaten ihrer zahlungspflichtigen Mitglieder weiterhin abfragen. Darüber hinaus wurden zur Überprüfung der Richtigkeit der in den Melderegistern enthaltenen Daten im Rahmen der Volkszählung 2001 diverse Daten gemeinsam mit der Volkszählung ermittelt. Diese Verschränkung wurde mehrfach kritisch diskutiert. Vor dem Hintergrund der deutschen Diskussion zeigt sich, dass das österreichische Meldegesetz einer näheren datenschutzrechtlichen Betrachtung wert wäre.

Zurück zur deutschen Diskussion: Hier lautete die Argumentationslinie der Befürworter etwa wie folgt: Das Einzelinteresse an Anonymität sei dem Informationsinteresse der Allgemeinheit gegenüberzustellen. Die Volkszählung sei Vorbedingung für die Planmäßigkeit staatlichen Handelns und es sei der Sozialstaat zur Daseinsvorsorge verpflichtet. Aus der Sicht des Datenschutzes und des mit ihm beabsichtigen Personenschutzes sei es notwendig, dass Volkszählung und andere Statistiken unabhängig von vorhandenen Verwaltungsunterlagen selbstständig durchgeführt würden. Die lesenswerte Begründung: Ein Personenkennzeichen[16] und damit verbunden die Möglichkeit der bloßen Verknüpfung von Verwaltungsdateien würde abgelehnt.[17] Dies wäre ein Schritt, den einzelnen Bürger in seiner ganzen Persönlichkeit zu registrieren und katalogisieren. Das VolkszählungsG 1983 entspreche auch dem Grundsatz der Verhältnismäßigkeit. Nur vollständige Ergebnisse innerhalb kürzester Zeit würden den Kostenaufwand rechtfertigen.

---

[15] Zur Problematik ZMR-Zahl siehe Abschnitt 5.4.2.

[16] Als Personenkennzahl wird eine Identifikationsnummer für Individuen üblicherweise dann bezeichnet, wenn diese (eindeutige) Identifikationsnummer unabhängig vom Sachbereich, flächendeckend in einer Gesellschaft zur Identifikation von Personen verwendet wird (Kotschy 2001, S 100 FN21). Art. 8 Abs. 7 EU-DS-RL nennt eine „nationale Kennziffer oder andere Kennzeichen“ und überlässt deren Verarbeitungsvoraussetzungen zur Gänze den Mitgliedstaaten (dies wurde deshalb auch kritisiert). Es handelt sich dabei um eine besondere Kategorie personenbezogener Daten (Art. 8 regelt ja gerade die Verwendung sensibler Daten), die eine eindeutige Identifizierung des „Nummernträgers“ ermöglichen (vgl. etwa in Norwegen die 11-stellige „Fødselnummer“, ohne die nicht einmal ein Bankkonto eröffnet werden kann). Der Vergleich mit der SV-Nummer (und zwischenzeitig der ZMR-Nummer) drängt sich auf. In den DS-Berichten von 1995 und 1997 hat der Datenschutzrat immer wieder aufmerksam gemacht, dass in verschiedenen Gesetzesentwürfen versucht wird, die Sozialversicherungsnummer als (weiteres) Identifikationskriterium einzuführen. Dies regelmäßig in Verbindung mit Gesetzesentwürfen, die von der Materie in keinem Zusammenhang mit dem Sozialversicherungs- und Gesundheitswesen stehen. Der Datenschutzrat hat sich bereits wiederholt gegen eine derartige „schleichende“ Einführung eines Personenkennzeichens gewandt.

[17] Für die österreichische Volkszählung 2001 wurde aber gerade damit geworben, dass es die letzte Totalerhebung sei und die Daten künftig automatisch abgeglichen würden.

2.2.2 Was ist das Recht auf informationelle Selbstbestimmung?

Persönlichkeitsrecht als Ankerpunkt

Die meisten Beschwerdegründe wurden vom BVerfG verworfen. Die (wahrheitsgemäße) Auskunftspflicht über die rechtliche Zugehörigkeit oder Nichtzugehörigkeit zu einer Religionsgesellschaft verstieß nicht gegen das Grundrecht auf Bekenntnisfreiheit.[18] Auch die (negative) Meinungsäußerungsfreiheit war mangels einer Meinungsäußerung nicht verletzt. Grund: es handelte sich nur um reine Tatsachenmitteilungen, keine Meinungen. Übrig blieb – als Prüfungsmaßstab – allerdings das allgemeine Persönlichkeitsrecht. Dieses verhalf den Beschwerdeführern schließlich zum Durchbruch.

Selbstbestimmung über Offenbarung persönlicher Lebensumstände

Das allgemeine Persönlichkeitsrecht war durch die Rechtsprechung nicht abschließend konkretisiert. Unter Verweis auf Vorjudikatur stellte das BVerfG aber klar, dass darunter

> „... auch die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen...“ zu verstehen sei, „... grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.“

Dieses Ergebnis ist stark von den Bedingungen der automatischen Datenverarbeitung geprägt. Die Gefährdung wurde gerade bei Entscheidungsprozessen auch darin gesehen, dass

neue Gefährdungen durch die EDV

> „... nicht mehr wie früher auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden muß, vielmehr heute mit Hilfe der EDV Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind; bei integrierten Informationssystemen – mit anderen Datensammlungen – teilweise oder weitgehend ein vollständiges Persönlichkeitsbild zusammengefügt werden kann, ohne daß der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann.“

Persönlichkeitsrechte umfassen auch die Verwendung persönlicher Daten

Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher vom Grundrecht auf die Unantastbarkeit der Würde des Menschen und dem Recht auf freie Entfaltung der Persönlichkeit umfasst. Er gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen. Ebenso zählt dazu das Recht auf Nichtwissen (Konferenz der DBvB&L 2001, 20).

unantastbarer Kern privater Lebensgestaltung festgeschrieben

Das BVerfG anerkennt auch einen letzten unantastbaren Kernbereich privater Lebensgestaltung, der der öffentlichen Gewalt schlechthin entzogen ist. Selbst schwerwiegende Interessen der Allgemeinheit können Eingriffe in diesen Bereich nicht rechtfertigen. Eine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes findet nicht statt.[19] Ob ein Sachverhalt allerdings dem unan-

---

[18] Zwar ist auch das Recht zu schweigen vom Grundrecht auf Bekenntnisfreiheit umfasst. Diese negative Bekenntnisfreiheit wird aber durch einen Vorbehalt der Weimarer Reichsverfassung (WRV) eingeschränkt, der Behörden gestattet, nach der Zugehörigkeit zu einer Religionsgesellschaft zu fragen, wenn davon Rechte und Pflichten abhängen oder eine gesetzlich angeordnete statistische Erhebung – wie hier der Fall – dies erfordert.

[19] Im Allgemeinen gibt es Einschränkungsmöglichkeiten eines Grundrechts durch überwiegende Allgemeininteressen, welche ihrerseits den Verhältnismäßigkeitsgrundsatz zu beachten haben. Die Zulässigkeit des Eingriffs wird daher durch die Abwägung zwischen Interesse des Betroffenen am RaiS und dem Interesse der Allgemeinheit an dem Eingriff vorgenommen. Zur Beurteilung der Verhältnismäßigkeit und Zu-

tastbaren Bereich oder jenem Teil des Privatlebens zugehört, der unter bestimmten Voraussetzungen dem staatlichen Zugriff offen steht, ist aber jedenfalls immer im Einzelfall zu beurteilen.[20] Interpretationskonflikte sind daher schwer zu vermeiden.

Im Ergebnis ist aber festzuhalten, dass der Schutz der Handlungs- und Partizipationsfähigkeit des Einzelnen eines der wichtigsten Grundrechte hinsichtlich der Anforderungen an die Verarbeitung personenbezogener Daten darstellt.[21]

2.2.3 Wozu ein Recht auf informationelle Selbstbestimmung?

Entscheidungsfreiheit gefährdet

Das BVerfG führte seine Gedankengänge konsequent weitsichtig auch in nicht rein-juristische Gebiete hinein. Durch die Erweiterung der Möglichkeiten der Einsichtnahme und Einflussnahme kann auf das Verhalten des Einzelnen schon durch den psychischen Druck öffentlicher Anteilnahme eingewirkt werden. Das RaiS setzt aber – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, dass dem Einzelnen Entscheidungsfreiheit über vorzunehmende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten.

Grundrecht auf freie Entfaltung der Persönlichkeit

Wer nicht einigermaßen abschätzen kann, welche Informationen in seinem sozialen Umfeld – etwa den Kommunikationspartnern – bekannt sind, kann in seiner Freiheit gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Nicht ohne Grund rekurriert das BVerfG zur Begründung der rechtlichen Grundlage des RaiS auf Art 2 des (deutschen) Grundgesetzes, der jedem Menschen das Recht auf freie Entfaltung seiner Persönlichkeit grundrechtlich absichert.

gesellschaftliche Folgen

Die Besonderheit der Entscheidung des BVerfG liegt aber auch darin, dass sie nicht nur beim Individuum als „Zielobjekt" des Datenschutzes stehen bleibt, sondern auch die Folgewirkungen würdigt. Etwa wenn jemand auf die Ausübung ihm zustehender Grundrechte nur aus der Angst heraus verzichtet, seine Teilnahme an einer Versammlung oder sein Engagement in einer Bürgerinitiative wäre mit persönlichen Nachteilen verbunden. Als mögliche Folge wird der Mensch versuchen, nicht durch abweichendes Verhalten aufzufallen. Das Ende jeglicher Risikobereitschaft?[22]

---

mutbarkeit des Eingriffs in das RaiS ist grundsätzlich auf die möglichen Verwendungs- und Missbrauchsmöglichkeiten abzustellen. In späteren Entscheidungen (wie etwa in der „Tagebuchentscheidung" BVerfGE 80, 367 v. 14.9.1989, erkennt das BVerfG auch „einen letzten unantastbaren Bereich privater Lebensgestaltung" an, der der öffentlichen Gewalt schlechthin entzogen ist. Es sprach aus, dass in diesem Fall selbst schwerwiegende Interessen der Allgemeinheit Eingriffe in diesen Bereich nicht rechtfertigen können; eine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes findet nicht statt (unter Berufung auf BVerfG 34,238 (245)). Dies folge aus der Garantie des Wesengehalts der Grundrechte, zum anderen würde es sich daraus ableiten, dass der Kern der Persönlichkeit durch die unantastbare Würde des Menschen geschützt sei.

[20] Siehe zum unantastbaren Bereich privater Lebensgestaltung auch BVerfG, Beschluss v. 14.9.1989 – 2 BvR 1062/87 über die Verwertung tagebuchähnlicher Aufzeichnungen im Strafprozess, CR 1990, 142.

[21] So Simitis in Simitis 1997; kritisch zum RaiS K. Vogelgesang 1987 der meint, dieses billige dem einzelnen ein Übergewicht zur Kommunikationsverhinderung zu, weil er die jederzeitige Steuerungsmöglichkeit über seine Daten haben soll.

[22] So die Prognose *Möllers*, zitiert von Opaschowski, Datenschutz Quo Vadis?, DuD 11/2001, 680 mwN.

Vor diesem Hintergrund stellte das BVerfG fest, mit dem RaiS sei

> „... eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.“

Weiters:

Selbstbestimmung als Grundlage der freiheitlich demokratischen Gesellschaft

> „Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“[23].

All diese Erörterungen zum RaiS hat das BVerfG getroffen, ohne – nach seiner eigenen Meinung – Anlass zur „erschöpfenden“ Erörterung des RaiS gefunden zu haben.[24] Das BVerfG hat seine Rechtsansicht zwischenzeitig in zahlreichen Folgeentscheidungen bestätigt.[25]

2.2.4 Grenzen des RaiS

überwiegendes Allgemeininteresse

Das BVerfG bestätigt im Gegenzug aber auch die Existenz überwiegender Allgemeininteressen. Information stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann. Aus diesem Grund spricht das BVerfG auch davon, dass ein solches überwiegendes Allgemeininteresse regelmäßig nur an Daten mit Sozialbezug unter Ausschluss unzumutbarer interner Angaben und von Selbstbezichtigungen bestehen kann.[26] [27] In neueren Entscheidungen nimmt das BVerfG ein solches Allgemeininteresse – unter Berufung auf das RaiS – auch dann an, wenn

---

[23] BVerfGE 65,1 (43).

[24] BVerfGE 65,1 (44f), Erörtert wurde „nur“ die Tragweite des RaiS für Eingriffe, bei denen der Staat die Angabe personenbezogener Daten vom Bürger verlangt.

[25] BVerfG, Beschluss v. 14.9.1989 – 2 BvR 1062/87, CR 1990, 142; BVerfG, Beschluss v. 24.7.1990 – 1 BvR 1244/87 betr. Datenschutz im Planfeststellungsverfahren, CR 1990, 798. Repräsentativ und aktuell ist die „Gerichtsfernsehen“-Entscheidung des BVerfG vom 24.1.2001. Abgewogen wurde hier zwischen dem RaiS und dem Grundrecht auf Informations- und Rundfunkfreiheit. Über den Persönlichkeitsschutz und unter Hinweis auf die wettbewerbsbestimmte TV-Branche kommt das BVerfG schließlich zu dem Schluss: „*Solche Gefahren für das Recht auf informationelle Selbstbestimmung abzuwehren, ist Ziel des generellen Ausschlusses von Aufnahmen und deren Verbreitung*“. Die Öffentlichkeit bleibt somit auf die Saalöffentlichkeit beschränkt. Zwei Richter hatten abweichende Meinungen.

[26] BVerfGE 65,1 (46).

[27] Bei „unzumutbaren internen“ Angaben – ohne dass das BVerfG in der konkreten Entscheidung darauf näher eingegangen wäre – man denke bspw. an diverse Gesundheits- oder Daten des Familienlebens (psychologische Unterstützung nach schweren persönlichen Schicksalsschlägen, guter schlechter Ehemann und – als österreichische Besonderheit und für die Allgemeinheit ohne jegliche Bedeutung – die Ermittlung des „Haushaltsvorstandes“ im Rahmen der letzten Volkszählung). „Selbstbezichtigung“ erklärt sich mit Rücksicht auf das in der Verfassung/EMRK normierte Selbstinkriminierungsverbot fast von selbst. Niemand muss sich selbst beschuldigen, selbst wenn das Allgemeininteresse noch so stark die „schonungslose Aufklärung“ bspw. eines Verbrechens fordert. Dieser Standpunkt wurde vom BVerfG bspw. in der „Tagebuchentscheidung“ weiterentwickelt (praktisch: aufgeweicht), wonach ein überwiegendes Allgemeininteresse auch dann vorliege, „wenn der einzelne als in der Gemeinschaft lebender Bürger in Kommunikation mit anderen tritt, durch sein Verhalten auf andere einwirkt und dadurch die persönliche Sphäre seiner Mitmenschen oder die Belange der Gemeinschaft berührt“ (siehe auch Antwort zu Punkt 8 unten).

„... der einzelne als in der Gesellschaft lebender Bürger in Kommunikation mit anderen tritt, durch sein Verhalten auf andere einwirkt und dadurch die persönliche Sphäre seiner Mitmenschen oder die Belange der Gemeinschaft berührt."[28]

Dies hat das BVerfG in seiner „Tagebuchentscheidung" v. 14.9.1989, BVerfGE 80, 367, 373 unter Berufung auf BVerfGE 35, 35 (39); 202 (220) ausgesprochen.

Grenzfall Tagebuchaufzeichnungen in Strafverfahren

Der zugrundeliegende Sachverhalt war, dass ein Mann in Verdacht stand, eine Frau erschlagen zu haben. Im auf Indizien beruhenden Strafverfahren wurden auch tagebuchähnliche Aufzeichnungen des Beschuldigten, die dieser mit dem vom Gericht bestellten Sachverständigen erörterte, zum Teil verwertet. Der Mann war psychisch krank und litt darunter, keine längeren Beziehungen zu Frauen aufbauen zu können. Auf Anraten eines Psychologen hat er Tagebuch geführt. Darin fanden sich zwar keinerlei konkrete Hinweise auf die Tat, jedoch wurde das „gestörte" Verhältnis zu Frauen deutlich erkennbar. Das BVerfG sprach aus, der Mensch als Person existiere notwendig in sozialen Bezügen. Die Zuordnung eines Sachverhaltes zum unantastbaren Bereich privater Lebensgestaltung oder zu jenem Bereich des privaten Lebens, der unter bestimmten Voraussetzungen dem staatlichen Zugriff offen steht, hängt daher nicht davon ab, ob eine soziale Bedeutung oder Beziehung überhaupt besteht, sondern welcher Art und wie intensiv sie ist. Dies lässt sich nicht abstrakt beschreiben; es kann befriedigend nur unter Berücksichtigung des Einzelfalles beantwortet werden. Der Senat hat sich daher auf den Kernbereich privater Lebensgestaltung im Strafverfahren konzentriert. Folgende Kriterien waren wichtig:

- ob der Betroffene einen Lebenssachverhalt geheim halten will oder nicht,
- ob der Sachverhalt höchstpersönlichen Charakters ist und in welcher Art und Intensität er aus sich heraus die Sphäre anderer oder die Belange der Gemeinschaft berührt und dass die
- Verwertbarkeit vielmehr von Charakter und Bedeutung des Inhaltes abhänge; die Verfassung gebiete nicht, Tagebücher oder ähnliche private Aufzeichnungen schlechthin von der Verwertung im Strafverfahren auszunehmen. Dies geht so weit, als auch das Durchsehen solcher Unterlagen erlaubt sei (unter größter Zurückhaltung).

keine Entscheidung gefällt

Gehören solche private Aufzeichnungen nicht zum absolut geschützten Kernbereich, so bedarf ihre Verwertung im Strafverfahren der Rechtfertigung durch ein überwiegendes Interesse der Allgemeinheit. Im konkreten Fall hat das BVerfG zwei verfassungsrechtlich bedeutsame Prinzipien gegenübergestellt: die Erfordernisse einer wirksamen Rechtspflege und die freie Entfaltung der Persönlichkeit. Im 8-Richter-Senat des BVerfG bestand Stimmengleichheit. Nur aus diesem Grund konnte nicht festgestellt werden, dass die Verwertung der Aufzeichnungen zu Beweiszwecken gegen das Grundgesetz verstößt. Vier Richter waren der Meinung, die Notizen könnten grundsätzlich im Strafverfahren verwertet werden. Die Argumentation überzeugt nicht so richtig: die Aufzeichnungen gehören nicht dem absolut geschützten Bereich an, da Gedanken schriftlich niedergelegt; damit haben sie den beherrschbaren Innenbereich verlassen und der Gefahr des Zugriffs preisgegeben (Anm: e contrario besteht also wohl zumindest Gedankenfreiheit); jedenfalls hätten sie einen Inhalt, der über die

---

Diese Entwicklung geht vom Verständnis des deutschen Grundgesetzes (= Verfassung) aus, dass die Spannung Individuum – Gemeinschaft im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden hat.

[28] BVerfGE 80,367, 373, zitiert mwN in Schmitz, TDDSG und das RaiS, München – Beck 2000.

Rechtssphäre des Verfassers hinausweist und Belange der Allgemeinheit nachhaltig berührt; auch liege eine enge Verknüpfung zwischen Inhalt der Aufzeichnungen und dem Verdacht der außerordentlich schwerwiegenden strafbaren Handlung vor; zeigen auch konkrete Gefahrenlagen für Dritte auf; der konkrete Eingriff sei auch verhältnismäßig. Die anderen vier Richter des BVerfG meinten eine Grundrechtsverletzung liege vor; die Aufzeichnungen würden sehr wohl zum absolut geschützten Bereich privater Lebensgestaltung gehören; deshalb müssten sie staatlichem Zugriff entzogen sein, soweit dieser über die – für ihre persönlichkeitsrechtliche Qualifizierung erforderliche – erste Sichtung hinausginge; Art und Weise der Aufbewahrung der Aufzeichnungen lassen klar auf Geheimhaltungswillen schließen; es schade nicht, wenn diese mit Sachverständigen erörtert werden; die Aufzeichnungen haben höchstpersönlichen Charakter; sie enthalten eine offene, von keiner Rücksichtnahme sich selbst gegenüber beeinflusste Wiedergabe, diese verlor ihren höchstpersönlichen Charakter nicht weil sie dem Papier anvertraut wurde … und

> „so gewiss es ist, dass die Gedanken frei sind – und deshalb frei bleiben müssen von staatlichem Zwang und Zugriff, wenn nicht der Mensch im Kernbereich seiner Persönlichkeit getroffen werden soll –, so gewiss muss gleicher Schutz für das schriftlich mit sich selbst geführte Gespräch gelten, bei dem das andere Ich durch die Niederschrift zum Sprechen gebracht und damit als Gegenüber besser verstanden wird.“

… da grundsätzlich jede Erkenntnis über den psychischen Zustand eines Verdächtigen geeignet ist, zusätzliche Hinweise sowohl auf seine Schuldfähigkeit als auch darauf zu geben, ob er die Tat begangen haben könnte oder nicht, wäre allein der Verdacht geeignet, den absoluten Schutz des Kernbereichs der Privatsphäre zu beseitigen. Diese überzeugend wirkenden Argumente des BVerfG-Halbsenates haben sich – mE leider – nicht durchgesetzt.

anonyme wissenschaftliche oder statistische Auswertung zulässig

Die Weitergabe zu wissenschaftlichen Zwecken wiederum sei mit dem Grundgesetz vereinbar. Dies aber mit der Zusatzbemerkung, dass für wissenschaftliche Zwecke regelmäßig der Personenbezug (iS Name und Anschrift) nicht erforderlich sei. Vielmehr sei nur das (anonyme) Individuum als Träger bestimmter Merkmale interessant.

Ebenso sei es keine Beeinträchtigung der Bürger, wenn erhobene Daten – nach Anonymisierung oder statistischer Aufbereitung – von Statistischen Ämtern anderen stattlichen Organen oder sonstigen Stellen zur Verfügung gestellt würden.

2.2.5 Anforderungen an den Gesetzgeber zur Sicherstellung des RaiS

Verwendungszusammenhang ist entscheidend

Hier hat das BVerfG eine Reihe von Kriterien angeführt: Generell hat der Gesetzgeber Art, Umfang und denkbare Datenverwendungen zu berücksichtigen; ebenso die Missbrauchsgefahr. Die verfassungsgemäße gesetzliche Grundlage hat der Normenklarheit zu entsprechen. Der Grundsatz der Verhältnismäßigkeit ist zu berücksichtigen. Wie bereits einleitend zum „Kontext“-Konzept des Datenschutzes erwähnt, hängt die Nutzbarkeit und Verwendungsmöglichkeit personenbezogener Daten vom Zweck der Erhebung und von den informationstechnischen Möglichkeiten ab. Vor diesem Hintergrund hat das BVerfG zutreffend festgehalten, gebe es „kein belangloses“ Datum mehr. Die Beurteilung der Sensibilität bedürfe vielmehr der Kenntnis des Verwendungszusammenhanges.[29]

[29] Auf dessen Bedeutung weist auch Simitis mwN wiederholt hin, in Simitis/Dammann/Geiger/Mallmann/Walz 1999.

Gefahr der Zweckentfremdung

Die Gefahren der EDV machen auch einen „amtshilfefesten" Schutz gegen Zweckentfremdung durch Weitergabeverbote und Verwertungsverbote erforderlich. Der freie Datenfluss zwischen Behörden im Rahmen der Amtshilfe ist daher zu untersagen. Dort wo er erlaubt ist, sind die Übermittlungen zu protokollieren, damit Betroffene ihre Rechte geltend machen können.

präzise Bestimmung des Zweckes gefordert

Der Verwendungszweck der Daten ist daher bereichsspezifisch und präzise zu bestimmen, wobei nicht zu jeder gesetzlichen Verpflichtung auch der konkrete Zweck selbst im Gesetz erläutert werden muss. Weiters müssen die Daten auch für diesen Zweck geeignet und erforderlich sein.[30] Aus diesem Grund hat der Gesetzgeber auch aufmerksam zu verfolgen, ob das Instrument der Totalerhebung überhaupt noch praktikabel ist oder ob nicht schon auf personenbezogenes Datenmaterial gänzlich verzichtet werden kann. Aufgrund des Verwendungszweckes ist auch die Sammlung personenbezogener Daten „auf Vorrat" bzw. für noch unbekannte Zwecke grundsätzlich verboten: Kein Verwendungszweck, keine Rechtfertigung für die Verwendung.

Verbot der Vorratshaltung

Schutzvorkehrungen und Verpflichtungen

An verfahrensrechtlichen Schutzvorkehrungen sind Aufklärungs-, (schriftliche) Belehrungs-, Auskunfts- und Löschungspflichten ebenso vorzusehen, wie die Beteiligung unabhängiger Datenschutz-Beauftragter. Es ist für den Betroffenen deutlich zu machen, welche Angaben auf freiwilliger Basis erhoben werden, etwa private Telefonnummern, und welche nicht. Gefordert wird auch das Erfordernis des aufgeklärten und freiwilligen Einverständnisses, etwa für eine Widerspruchslösung.[31] Schließlich sind die zur Identifizierung dienenden Merkmale zum frühest möglichen Zeitpunkt zu löschen und bis dahin von den übrigen Angaben getrennt unter Verschluss zu halten.

Zahlreiche hier kurz dargestellte Anforderungen haben ihre Grundlage in der Datenschutzkonvention des Europarates und dem deutschen BDSG und sind auch zum überwiegenden Teil in der DS-RL der EU (folgend: DS-RL) wiederzufinden.

2.2.6 Kurzzusammenfassung der Kriterien des RaiS

Selbstbestimmung und Kenntnis des Zweckes

Das RaiS umfasst im Einzelnen folgende Dimensionen:

- das Recht des Einzelnen, grundsätzlich selbst über die Verwendung und Preisgabe seiner Daten zu bestimmen und
- das notwendige aufgeklärte und freiwillige Einverständnis in Kenntnis des Verwendungszwecks.

Ausnahmen nur bei überwiegendem allgemeinen Interesse

Unumgängliche Einschränkungen dürfen nur im überwiegenden Interesse der Allgemeinheit erfolgen und müssen durch Gesetz (unter Beachtung der Normenklarheit und Verhältnismäßigkeit) legitimiert sein. Flankierend dazu sind organisatorische und verfahrensrechtliche Schutzvorkehrungen vorzusehen.

Das RaiS bildet einen wesentlichen Grundstein auch für die EG-DS-RL und die – soweit bereits umgesetzt – nationalen Regelungen der einzelnen EU-Mitgliedstaaten.

---

[30] Damit übernimmt das BVerfG eine der tragenden Bestimmungen der Datenschutzkonvention des Europarates (Art 5 lit c), nämlich der grundsätzlichen Vermeidung von unerheblichen Daten.

[31] Simitis, NJW 1984, 398ff.

2.3 Grundsätze moderner Datenschutzpolitik

vergleichbare Grundsätze in der EU und der OECD

Zusammengefasst zeigt sich, dass das RaiS ein wesentlicher Grundpfeiler in der Definition moderner Datenschutzpolitik ist. Neben der EU-RL sind es vor allem die Prinzipien in den OECD Guidelines,[32] die internationale Beachtung finden:

1. Collection Limitation;
2. Data Quality;
3. Purpose Specification;
4. Use Limitation;
5. Security Safeguards;
6. Openness;
7. Individual Participation; and
8. Accountability.

zusätzlich: Vermeidung von personenbezogenen Daten

Das Prinzip der Informationellen Selbstbestimmung, realisiert durch Zweckbindung und Verhältnismäßigkeit, sowie die Verhaltensanweisung an Datenverarbeiter und Betroffene, der Datenvermeidung und der limitierten Speicherung und Vernetzung hohe Priorität einzuräumen sind wichtige Maßnahmen im Rahmen moderner Datenschutzpolitik.. Da es in der sogenannten „Informationsgesellschaft“ immer schwieriger wird, aktive Datenvermeidung zu betreiben, ist jedenfalls der Personenbezug zu erschweren, was durch die Prinzipien von Anonymität und Pseudonymität gewährleistet werden soll.

[32] [OECD, 1980 #133]

3 Private Internetnutzung

3.1 Grenzen der individuellen Verantwortung bei der Internetnutzung

Praxistauglichkeit von Tipps zur Datenvermeidung

In der ersten Teilstudie „Beeinträchtigung der Privatsphäre in Österreich – Datensammlungen über ÖsterreicherInnen“ (Čas und Peissl 2000) wurden u. a. Tipps für InternetnutzerInnen formuliert, mit deren Hilfe unnotwendige Daten nicht preisgegeben werden und die Privatsphäre geschützt werden kann. In diesem Abschnitt wird auf diesen Tipps aufbauend analysiert, inwieweit sich die in ähnlicher Art von vielen Datenschutzorganisationen publizierten Empfehlungen in der Praxis umsetzen lassen. Die Praxistauglichkeit von Tipps zur Datenvermeidung kann aus vielen Gründen eingeschränkt sein. Diese reichen von einer schlichten Undurchführbarkeit aufgrund fehlender Voraussetzungen über fehlende Kenntnisse oder zusätzliche Kosten und Zeit, die dabei aufgewendet werden müssen, bis hin zu mehr oder weniger gravierenden Einbußen an Bequemlichkeit, die die Akzeptanz dieser Maßnahmen schmälern. Das Ziel dieser Analyse ist es, jene Bereiche zu identifizieren, in denen die Politik, Industrie oder Interessensvertretungen gefordert sind, die einzelnen NutzerInnen bei der Datenvermeidung zu unterstützen, und Schritte vorzuschlagen, die dafür geeignet erscheinen.

Unterstützung durch Politik und Industrie

individuelle Verantwortung und gesellschaftliche Regeln notwendig

In den meisten Fällen werden keine klaren und haarscharfen Grenzlinien zwischen individueller und gesellschaftlicher Verantwortung zu ziehen sein. Im Gegenteil, oft besteht eine unmittelbare positive Beziehung zwischen dem, was eine NutzerIn bewusst zum Schutz ihrer Privatsphäre tun kann und den freiwilligen oder gesetzlichen Auflagen, denen die Anbieter unterliegen. Um beispielsweise die Datenschutzpolitik des Gegenübers bei den Entscheidungen berücksichtigen zu können, müssen diese publiziert werden; um zwischen verschiedenen Optionen wählen zu können, müssen diese angeboten und in ihren Konsequenzen beurteilt und verglichen werden können.

Anreize zur Einhaltung von Regeln erforderlich

Welche Form der Regulierung – freiwillige Vereinbarungen oder gesetzliche Vorschriften – zielführender ist, lässt sich auf allgemeiner Ebene nicht beantworten, sondern hängt von einer Reihe von Faktoren ab. So hängt die Bereitschaft zur Selbstbeschränkung bei der Verarbeitung von persönlichen Daten u. a. von der Marktkonstellation, der daraus resultierenden Marktmacht der KonsumentInnen, dem allgemeinen Problembewusstsein und der Bereitschaft ab, das Bewusstsein in konkrete Handlungen münden zu lassen. Diese Faktoren bestimmen, inwieweit überhaupt Reaktionen bzw. spürbare positive oder negative Folgen in Abhängigkeit von der gewählten Datenschutzpolitik zu erwarten und somit Anreize zu deren Adaption gegeben sind. Gesetzliche Regeln wiederum bedürfen Möglichkeiten, deren Einhaltung zu kontrollieren und Verstöße dagegen wirksam zu sanktionieren.

grundlegendes Wissen über Datenschutz unverzichtbar

Bewusstes Handeln setzt auch voraus, dass überhaupt Wissen darüber vorhanden ist, welche Daten bei der Internetnutzung entstehen, auf welche Weise sie gesammelt und verwertet werden können. Dabei ist es nicht notwendig, dass sich jede InternetnutzerIn zu einer DatenschutzexpertIn ausbilden lässt, genauso wenig wie jede AutofahrerIn ExpertIn für Unfallursachen und -vermeidung sein muss. Allerdings sollte man über potentielle Gefahren informiert sein, um beim Navigieren im Internet den eigenen Präferenzen entsprechend Risken eingehen oder vermeiden zu können.

Datenschutz durch Technik

Ein weiterer Bereich, in dem neben dem Konsumenten auch die Anbieter gefordert sind, betrifft den Einsatz von Privacy Enhancing Technologies (PETs). Die hier analysierten Tipps betreffen zwar primär Software-Tools und Dienste für individuelle AnwenderInnen, das wesentlich größere Potential, „Datenschutz durch Technik" zu realisieren, liegt aber sicher in der Integration von datenschutzfreundlichen Technologien auf Seiten der Anbieter und EntwicklerInnen von Informationssystemen und -diensten. Ein populäres Beispiel dafür sind die Pre-Paid-Cards für Mobiltelefone. In diesem Beispiel lag die Intention zwar nicht darin, durch anonyme Nutzungsmöglichkeiten die Privatsphäre zu schützen, sondern den Kundenkreis auf Kreise auszudehnen, bei denen eine nachträgliche Verrechnung mit zu hohem Risiko für die Betreiber verbunden wäre, etwa Jugendliche ohne eigenes Einkommen oder generell wenig kreditwürdige Personen. Es zeigt aber sehr gut, dass Sicherheit und Anonymität einander nicht ausschließen müssen. Im Allgemeinen geht es bei der Integration von Privacy Enhancing Technologies in Informationssysteme aber darum, die Nutzung von Diensten in anonymer Weise zu ermöglichen. Wenn eine Autorisierung notwendig ist, etwa weil der Dienst bezahlt werden muss oder nur einem eingeschränkten Personenkreis zugänglich sein soll, so werden die Sphären durch kryptographische Verfahren voneinander getrennt. Diese Systeme lassen sich auch so gestalten, dass bei normaler Nutzung die Anonymität gewährleistet wird, im Fall von Missbrauch dieser aber aufgedeckt werden kann. Dieses Prinzip lässt sich in unterschiedlichen Bereichen einsetzen, für sensible Bereiche wie den Gesundheitsbereich oder die Betreuung von Drogenabhängigen gibt es konkrete Anwendungsbeispiele (Hes et al. 1998). Bei der Systemgestaltung sind aber naturgemäß nur minimale Einflussmöglichkeiten durch einzelne KonsumentInnen gegeben. Diese können zwar innerhalb bestimmter Grenzen entscheiden, welche Daten sie wem zur Verfügung stellen und diese Entscheidung an die Datenschutzpolitik des Empfängers knüpfen, sie können aber in der Regel nicht mitbestimmen, welche technischen Systeme private oder öffentliche Organisationen einsetzen oder welche Vorkehrungen gegen Datenmissbräuche getroffen werden.

anonyme Nutzung von Diensten

Integration in Informationssysteme

Datenschutzempfehlungen in der Praxis

Welchen Grenzen individuellen Maßnahmen und Handlungen unterliegen, lässt sich anhand von Erfahrungen verdeutlichen und veranschaulichen, die eine datenschutzbewusste InternetnutzerIn macht, wenn sie versucht, die Empfehlungen zum verantwortlichen Umgang in die Tat umzusetzen. Da in der Literatur, in Fachzeitschriften und auf mit dem Thema befassten Internetseiten zwar einzelne Hinweise zu möglichen Problemen bei der Umsetzung von datenschutzbewusstem Handeln zu finden sind, aber keine zufriedenstellende umfassende Analyse gefunden werden kann, wurde am Institut für Technikfolgen-Abschätzung ein eigenes Experiment entwickelt und durchgeführt. Im Rahmen dieses Experiments wurden zwei „virtuelle" Nutzer kreiert, die sich einzig in der Bedeutung unterscheiden, die sie dem Schutz ihrer Privatsphäre beimessen. Die beiden Nutzer haben jeweils die selben Aufgaben am Internet zu erfüllen, wobei einer der beiden dabei versucht, die Datenschutzempfehlungen so weit als möglich einzuhalten, während der zweite Nutzer möglichen Verletzungen der Privatsphäre keinerlei Bedeutung zumisst. Ein großer Block an Aufgabenstellungen wurde Anfang 2001 durchgeführt und im Rahmen der Science Week Austria 2001 präsentiert. Die Experimentierplattform wird zur laufenden Einschätzung neuer Fragestellungen genutzt und regelmäßig zur Evaluierung der Wirksamkeit eines datenschutzgerechten Handelns genutzt. Das Design des Experiments ist natürlich nicht geeignet, empirisch abgesicherte quantitative Werte zu liefern, es eignet sich aber sehr gut, um Diskrepanzen zwischen vielfach erhobenen Forderung an mündige KonsumentInnen und den realen Möglichkeiten zu deren Umsetzung aufzuzeigen und somit auch die Aufmerksamkeit der Forschung und der Politik auf bislang zu wenig beachtete Faktoren zu lenken.

Experiment mit „virtuellen" NutzerInnen

Die im folgenden Abschnitt durchgeführte Analyse einzelner Empfehlungen bezieht die diesem Experiment gewonnenen Erfahrungen ein; für einzelne Fragestellungen wurden Aufgabenstellungen erneut durchgeführt bzw. das Versuchsdesign um zusätzliche Aufgaben erweitert, um die Erkenntnisse angesichts neuer technischer und regulativer Entwicklungen zu überprüfen.

3.2 Empfehlungen für KonsumentInnen in der Praxis

In der ersten Teilstudie (Čas und Peissl 2000) wurden folgende Empfehlungen und Vermeidungsstrategien für die Internetnutzung entwickelt:

Tipps zum Schutz der Privatsphäre

- AGBs nach Datenschutzaspekten vergleichen bzw. Informationen über Datenschutzrichtlinien besorgen
- mehrere Provider nutzen
- Zurückhaltung bei Preisgabe von Daten
- andere Identitäten und anonyme e-mail-Adressen verwenden; insbesondere bei Chats und Newsgroup-Beiträgen
- gegebenenfalls eigene Beiträge aus Newsgroup-Archiv entfernen und Archivierung blockieren
- Verschlüsselungssoftware nutzen
- anonyme Mail- und Webdienste nutzen
- spezialisierte Softwarepakete zum Schutz der Privatsphäre und des eigenen Rechners einsetzen

Berücksichtigung der Datenschutzpolitik

Die ersten beiden Empfehlungen bezogen sich primär auf die Auswahl der oder des Providers, über den private NutzerInnen Zugang zum Internet erhalten. Der erste Punkt gilt aber ebenso gut für die Nutzung jedweder Dienste, die über das Internet angeboten werden. Die Frage, wie mit den Daten der KonsumentInnen umgegangen wird, ist sowohl bei entgeltlichen als auch bei unentgeltlichen Angeboten am Internet von höchster Relevanz. Im ersten Fall, weil mit dem Bezahlvorgang beim e-Commerce in der Regel die Anonymität aufgegeben wird, im zweiten Fall, weil bei „kostenlosen" Diensten vielfach gerade die Verwertung der generierten Daten für eigene Zwecke oder deren Verkauf die Motivation oder die Einnahmenquelle zur Finanzierung von Gratisangeboten darstellt.

Datensparsamkeit, Anonymität und Verfügung über generierte Daten

Die zweite Gruppe von Empfehlungen betrifft die unmittelbaren Beiträge, die die Einzelne zur Wahrung ihrer Privatsphäre leisten kann, ohne auf das Verhalten der KommunikationspartnerIn vertrauen zu müssen und ohne dafür spezielle technische Hilfsmittel einsetzen zu müssen. Der erste Punkt stellt die individuelle Umsetzung des Prinzips der Datensparsamkeit dar, der zweite Punkt empfiehlt die Verwendung von Pseudonymen in jenen Fällen, die denen persönliche Merkmale preisgegeben werden müssen, um einen Dienst zu nutzen, eine Identifizierung aber nicht notwendig oder erwünscht ist. Der dritte Punkt betrifft die Möglichkeiten, „Fehler aus der Vergangenheit wieder gut zu machen" bzw. auf selbst generierte Daten zugreifen und über sie verfügen zu können.

Einsatz technischer Hilfsmittel

Die dritte Gruppe umfasst die individuellen Möglichkeiten, Privacy Enhancing Technologies einsetzen zu können. Als Basistechnologie für PETs lassen sich Verschlüsselungstechnologien zwar in zahlreichen Anwendungen wiederfinden, bei der ersten Empfehlung in dieser Gruppe geht es aber um die individuelle Verwirklichung des Briefgeheimnisses in der elektronischen Kommunikation. Der zweite Punkt empfiehlt die Anwendung von Diensten, die dazu

entwickelt wurden, das Internet unter Wahrung seiner Anonymität nutzen zu können, beim dritten und letzten Punkt werden Möglichkeiten angesprochen, durch am eigenen PC installierte Software zum Schutz der Privatsphäre beizutragen.

3.2.1 AGBs nach Datenschutzaspekten vergleichen

das „Kleingedruckte" lesen

Diese Empfehlung entspricht in vielen Aspekten dem in der Offline-Welt oft gehörten und auf den Bereich Privatsphäre umgemünzten Rat, das „Kleingedruckte" zu lesen; insbesondere jene Passagen in den Allgemeinen Geschäftsbedingungen (AGBs), die den Datenschutz betreffen, sollen beim Surfverhalten oder vor der Aufnahme von Geschäftsbeziehungen berücksichtigt werden. Für die Auswahl des Internetproviders oder von Anbietern von e-Mail- oder SMS-Diensten gilt dies in besonderem Maße. Bei ihnen fallen Daten über besuchte Webseiten und kontaktieren Kommunikationspartner ebenso an, wie die Inhalte von übermittelten Nachrichten, die aus technischen Gründen zwischengespeichert werden. Wie lange diese Daten gespeichert bleiben, zu welchen Zwecken sie eventuell ausgewertet oder an wen sie weitergegeben werden.

besondere Vorsicht bei sensiblen Daten

Für kritische Bereiche, in denen besonders umfangreiche und umfassende oder sensible Daten anfallen, ist auch ein Blick in die Datenschutzpolitik des potentiellen Diensteanbieters sinnvoll, die – im Unterschied zu den meist pauschalen Hinweisen auf gesetzliche Bestimmungen in den AGBs – in der Regel detaillierte Vorgaben zum Umgang mit den gewonnenen Daten enthält. Sofern keine Datenschutzpolitik publiziert wird, empfiehlt es sich, diese anzufordern, oder nach alternativen Anbietern zu suchen.

Ähnlich wie im Offline-Leben, verhallen auch hier viele gut gemeinte Appelle. Im Unterschied dazu stoßen aber jene KonsumentInnen, die die Datenschutzpolitik berücksichtigen wollen, oftmals auch auf neue und zusätzliche Probleme.

Informationen zur Datenschutzpolitik fehlen oft

Oft sind die gesuchten Informationen zur Datenschutzpolitik auf der Homepage des potentiellen Anbieters einfach nicht vorhanden oder nicht zu finden. Da das Internet ein globales Medium ist, in dem viele Aspekte keinen oder sehr unterschiedlichen nationalen Regeln oder Gepflogenheiten unterworfen sind, sind Unterschiede und Mängel bei der Auskunftsbereitschaft nicht überraschend. Allerdings sieht sich auch eine KonsumentIn, die sich bei österreichischen Diensteanbietern informieren möchte, vielfach mit Problemen konfrontiert. In Österreich ist seit dem 1. Januar 2002 ein e-Commerce-Gesetz (ECG) in Kraft, welches unter anderem allgemeine Informationspflichten und die Verpflichtung, Geschäftsbedingungen zur Verfügung zu stellen, enthält. Erste Untersuchungen über Einhaltung der Bestimmungen des ECG durch österreichische Diensteanbieter zeigen gravierende Mängel. In einer von der ARGE Daten im Februar 2002 durchgeführten Analyse[33] von 1200 Webshops entsprachen nur 19 % der österreichischen Anbieter dem ECG in allen Punkten. Die relativ kurze Zeit, die das ECG zum Zeitpunkt der Erhebung in Kraft war, mag zwar ein Faktor sein, der hilft, den extrem hohen Anteil an nicht konformen Anbietern zu erklären. Da es sich bei einem großen Teil der verletzten Informationspflichten aber um Selbstverständlichkeiten handelt, wie etwa die Angabe des Namens und der Anschrift des Unternehmens, wird dadurch die Notwendigkeit von gesetzlichen Verpflichtungen besonders deutlich. Mehr als 30% der Web-Shops publizieren keine AGB und lassen daher die KonsumentInnen im Unklaren.[34]

[33] http://www.ad.or.at/news/20020423.html

[34] http://www.ad.or.at/news/20020322.html

Informationen versteckt oder wenig verständlich

Selbst dort, wo AGB veröffentlicht werden, kann es mühsam sein, diese auf den oft sehr umfangreichen und verschachtelten Websites zu finden. Und selbst wenn diese Hürde überwunden ist, hat man das Ziel noch nicht notwendigerweise erreicht. Wie bei dem „Kleingedruckten" wird auch beim elektronischen Pendant oft auf die entsprechenden Paragraphen in den geltenden Gesetzen verwiesen, ohne deren Inhalt und Konsequenzen näher zu erläutern. Für den allgemeinen Geschäftsverkehr mag dies noch eher vertretbar sein, wenn man annehmen kann, dass ein großer Teil der Bevölkerung die geltenden Bestimmungen des allgemeinen Geschäftslebens zumindest in groben Zügen kennt. Wenn aber auf einzelne Paragraphen im Telekommunikationsgesetz (TKG) oder im Datenschutzgesetz (DSG) verwiesen wird, wird diese Voraussetzung weniger oft zutreffen.

unzugänglich und in Widerspruch zu geltendem Recht

Neben diesen Problemen muss man manchmal noch mit technischen Hürden kämpfen. Bei einem im Rahmen des Experiments untersuchten Anbieter von personalisierten Web- und Kommunikationsdiensten erschien ein Ausschnitt aus den AGBs in einem kleinen Fenster ohne Navigationsmöglichkeiten. Auf einen Scrollbalken war „vergessen" worden, und auch mit dem Cursor konnte man nicht im Text navigieren. Der im sichtbaren Teil erkennbare Hinweis auf die entsprechenden Paragraphen des TKG wird wahrscheinlich jeden durchschnittlichen Nutzer beruhigt zu den Angeboten greifen lassen. Über einen Umweg[35] gelang es doch, in die gesamten AGBs Einsicht zu nehmen und ernüchternde Erkenntnisse zu gewinnen. Der Anbieter kündigte an, zur Verhinderung von Missbräuchen die Inhalte von e-Mails und SMS für die Dauer von acht Wochen zu speichern. Dies stellt einen glatten Bruch des Telekommunikationsgesetzes dar, welches die Speicherung von Inhaltsdaten nur zulässt, solange dies für die Erbringung des Dienstes notwendig ist. Die Inhalte von e-Mails und von SMS müssen daher nach deren Zustellung gelöscht werden.

aufwändige Informationsbeschaffung

Natürlich gibt es auch vorbildliche Anbieter. Im Surfalltag muss man aber damit rechnen, immer wieder mit fehlenden, schwer zugänglichen, kaum verständlichen oder auch im Widerspruch zum geltenden Recht stehenden Informationen betreffend Datenschutz konfrontiert zu werden. Ganz grundsätzlich stellt sich die Frage, welcher Aufwand der StandardnutzerIn zugemutet werden kann, wenn sie sich über Verwendung ihrer Daten informieren will. Die gegenwärtige Situation ist in dieser Hinsicht jedenfalls vollkommen unbefriedigend.

Vertrauensbildung durch Gütesiegel

Es sind aber auch Bemühungen im Gange, den datenschutzbewussten KonsumentInnen das Leben wesentlich leichter zu machen. Eine schon etwas längere Tradition haben Versuche, mittels Gütesiegeln Vertrauen zu schaffen. Betreiber von Websites, die das Gütesiegel auf ihren Websites nutzen wollen, müssen sich verpflichten, die mit dem Gütesiegel verbundenen Bestimmungen einzuhalten; die Anbieter des Gütesiegels kontrollieren deren Befolgung. Der Beitrag dieser Gütesiegel zum Schutz der KonsumentInnen hängt in erster Linie von deren Verbreitung ab. Mit größerer Verbreitung steigt sowohl die Bekanntheit und somit das Vertrauen in das Siegel, als auch die Wahrscheinlichkeit, bei der Suche nach einem bestimmten Angebot auf einen durch das Gütesiegel als vertrauenswürdig anerkannten Anbieter zu stoßen.

Gütesiegel vorwiegend von großen Anbietern genutzt

Die bisherigen Erfahrungen mir Gütesiegeln sind jedoch nicht einfach zu interpretieren. So weist das 1996 gegründete und wohl bekannteste internationale Gütesiegel im Bereich Datenschutz TRUSTe[36] mit nur rund 1500 Teilnehmern eine insgesamt nicht besonders ermutigende Beteiligung auf; unter

---

[35] Mittels Kontextmenü <Alles markieren>, und den Befehlen <Kopieren> und <Einfügen> in ein normales Dokument wurde der ganze Text der AGBs sichtbar.

[36] http://www.truste.org/

den Top 100 und den Top 20 der Websites finden sich aber mehr als 50 bzw. 75 % Lizenznehmer von TRUSTe[37]. NutzerInnen, die große und bekannte Webshops frequentieren, haben somit gute Chancen, auf geprüfte Anbieter zu stoßen, jene die lokale oder international wenig bedeutende Anbieter bevorzugen, dürften angesichts der kleinen Gesamtanzahl nur sehr selten das Gütesiegel von TRUSTe zu Gesicht bekommen. Den österreichischen NutzerInnen wird das nationale Pendant zur Zeit auch nur gelegentlich helfen: mit 37 durch das e-Commerce-Gütezeichen[38] zertifizierten Webshops (Stand Mitte Mai 2002) ist auch hierzulande die Wahrscheinlichkeit noch recht gering, es mit Unternehmen zu tun zu haben, die sich dieser freiwilligen Prüfung unterziehen. Die Gesamtzahl an Unternehmen, die Waren oder Dienstleistungen über das Internet anbieten, wurde für den Jänner 2001 auf etwas mehr als 3000 hochgerechnet (Statistik Austria 2001), eine Zahl, die sich in der Zwischenzeit sicher erhöht haben wird. Allerdings haben sich zum selben Zeitpunkt mehr als 90 weitere Unternehmen für das Gütesiegel beworben und die im Vergleich zum Vorjahr sich rascher verändernden Teilnehmerzahlen deuten auf eine dynamischere Entwicklung hin, die sich auch in Richtung Erweiterung auf EU-Ebene abzeichnet.

EU-weites e-Commerce-Gütezeichen notwendig

National beschränkte Schritte können im grenzüberschreitenden e-Commerce grundsätzlich nur einen teilweisen Schutz mit sich bringen. Dementsprechend sind auch Bestrebungen im Laufen, diese Gütesiegel auf EU-Ebene zu etablieren. Als erster Schritt sind seit dem 15. April 2002 die Gütezeichen Deutschlands, Frankreichs und Österreichs in allen drei Ländern gültig.

Gütesiegel ist nicht gleich Gütesiegel

Das Vorhandensein eines Gütesiegels sagt prinzipiell noch wenig über die tatsächlich verfolgte Politik des Unternehmens aus, da sich die einzelnen Gütesiegels stark voneinander unterscheiden. Das erwähnte TRUSTe-Siegel bezieht sich einzig auf die Privacy-Politik und gibt auch in diesem Bereich keine materiellen Vorgaben vor. Anbieter mit diesem Gütesiegel verpflichten sich nur, ihre Datenschutzpolitik zu publizieren und deren Einhaltung überprüfen zu lassen. So ist auch das oft als Synonym für ungezügelte Datensammelleidenschaft geltende Unternehmen DoubleClick Inc. im Besitz eines TRUSTe-Siegels und Teilnehmer von mehreren Übereinkünften der Selbstregulierung. Im Gegensatz zu den Erwartungen, die durch diese Siegel geweckt werden, sammelt dieses Werbe- und Marketingunternehmen eine Reihe sensibler Daten, die von persönlichen Neigungen und Abneigungen bis zu Details der finanziellen Situation reichen.

österreichisches e-Commerce-Gütezeichen vorbildhaft

Im Gegensatz dazu umfasst das österreichische e-Commerce-Gütezeichen eine Reihe von Kriterien und Qualitätsmerkmalen bei der Abwicklung von elektronischen Geschäften, die über die gesetzlichen Verpflichtungen hinausgehen. Beim Datenschutz enthalten die Vergabekriterien beispielsweise folgende Passage: „Übermittlungen von personenbezogenen Daten an Dritte werden nicht vorgenommen, außer dies ist für die Abwicklung des konkreten Vertrages unumgänglich.“ [39]

mehr Transparenz durch P3P

Jüngeren Datums sind die Bemühungen, KonsumentInnen durch technische Maßnahmen bei der Durchsetzung ihrer Anforderungen an den Schutz seiner Privatsphäre zu unterstützen. Im Kern geht es bei der unter dem Akronym P3P (Platform for Privacy Preferences)[40] bekannten Projekt, welches vom World Wide Web Consortium (W3C) entwickelt wurde, um ein standardisier-

---

[37] http://www.truste.org/about/truste/about_whitepaper.html

[38] http://www.guetezeichen.at/

[39] http://www.guetezeichen.at/kriterien/kriterien.pdf

[40] http://www.w3.org/P3P/

tes Softwareprotokoll zur Beschreibung der Datenschutzpolitik der Anbieter einerseits und Präferenzen der Nutzer andererseits. Auf diese Art und Weise lassen sich viele der in diesem Abschnitt angesprochenen Schwierigkeiten mildern oder beseitigen. Die vom Nutzer zu machenden Vorgaben werden automatisch mit den Gepflogenheiten des jeweiligen Anbieters verglichen und dementsprechend die Abläufe gesteuert oder Warnungen an den Nutzer ausgegeben. Die Version 1.0 der P3P-Spezifikation wurde zwar erst am 16. April 2002 offiziell bekannt gegeben, da aber im W3C die größten IT-Unternehmen vertreten sind, sind bereits einige Produkte verfügbar, die auf diesem Standard aufbauen oder ihn integriert haben. Ebenso publiziert bereits eine Reihe von Internetdiensteanbietern ihre Datenschutzpolitik in maschinenlesbarer Form. Neuere Browsergenerationen erkennen und zeigen an, ob die besuchte Internetseite P3P-konform ist, wenn ja wird die Datenschutzpolitik des Anbieters mit den eigenen Vorgaben verglichen. Durch die standardmäßige Integration von P3P in Benutzersoftware und das automatische Aufzeigen nichtkonformer Internetanbieter wird ein gewisser Druck zum Einsatz dieses Protokolls ausgeübt. Eine Einschätzung des möglichen Beitrags von P3P zum Schutz der Privatsphäre wird in Abschnitt 3.2.6 über Privacy Enhancing Technologies (PETs) vorgenommen.

3.2.2 Mehrere Provider nutzen

Schutz durch verteilte Aktivitäten

Die Grundidee dieser Empfehlung besteht darin, der Generierung von umfassenden Persönlichkeitsprofilen entgegenzuwirken, indem man seine Internetaktivitäten auf mehrere Internetprovider aufteilt. Mangelndes Vertrauen in das Verhalten der Provider oder in die Sicherheit der bei ihnen anfallenden Daten wird durch eine Aufsplitterung dieser Daten kompensiert. Diese Aufsplitterung setzt sich im Außenverhältnis zu Diensteanbietern fort, da die IP-Adresse nicht nur dynamisch vergeben wird[41], sondern auch noch aus unterschiedlichen Pools stammt; ebenso lassen sich die von jedem Provider üblicherweise zur Verfügung gestellten e-Mail-Adressen zur Trennung von einzelnen Sphären seiner Persönlichkeit nutzen. Es handelt sich dabei um die Annäherung an ein aus der Kryptographie und der Sicherheitstechnik bekanntes Prinzip: je häufiger man den Schlüssel wechselt, umso sicherer werden die Transaktionen. Im Extremfall wird für jede Transaktion ein eigener Schlüssel generiert und verwendet.

Empfehlung abhängig von Marktstruktur

Offensichtlich wird dabei höhere Sicherheit bzw. geringere Gefahr, seine Privatsphäre zu verlieren, mit zusätzlichem Aufwand erreicht. Zum Zeitpunkt, zu dem diese Empfehlung gemacht wurde, war dieser zusätzliche Aufwand aufgrund der Marktkonstellation durchaus vertretbar, da er auch mit Kosteneinsparungen verbunden oder zumindest nicht zusätzliche Ausgaben für den Internetzugang verursachte. Angesichts der in den letzten beiden Jahren eingetretenen Veränderung beim Angebot an Internetzugängen lässt sich diese Empfehlung nicht länger aufrechterhalten. Die Marktkonstellation, auf der diese Empfehlung basierte, war gekennzeichnet durch eine Vielzahl von Call-by-Call-Zugangsanbietern mit relativ homogener Preisgestaltung. Dabei konnte man aufgrund der fehlenden Grundgebühren noch Ersparnisse durch zeitlich

[41] Bei der Einwahl ins Internet mittels Modems über einen herkömmlichen Telefonanschluss ist immer nur ein gewisser Prozentsatz der Kunden online. Durch statistische Analysen des Verkehrsaufkommens lässt sich die Zahl der Modems und der IP-Adressen beim Provider ermitteln, die eine ausreichende Erreichbarkeit garantiert und die Kosten für den Provider minimiert. Da insgesamt eine wesentlich geringere Anzahl an Adressen als Kunden notwendig ist, wird bei jeder neuen Einwahl die nächste freie Adresse zugewiesen.

unterschiedlich gestaffelte Tarifstrukturen lukrieren. Diese Situation hat sich durch zwei Entwicklungen verändert. Zum einen haben sich Internetzugänge über ADSL oder Kabelmodems unter Nutzung des herkömmlichen Telefonnetzes bzw. der Kabel-TV-Infrastruktur am Markt etabliert. Sie bieten permanente Anbindungen mit höheren Geschwindigkeiten zu pauschalierten Preisen an. Auch wenn die ADSL-Zugänge vielfach noch im Downloadvolumen limitiert sind, würde ein zusätzlicher Zugang neben dem zeitlichen Aufwand auch höhere Kosten verursachen. Zum anderen versuchen die Internetprovider auch die über Modem angebundenen Kunden durch zusätzliche Leistungen oder Freiminuten bei Paketen mit Grundgebühr längerfristig an sich zu binden.

nur für versierte PC-Nutzer realisierbar

Es sind aber nicht die geänderten Kosten allein, die diesen Tipp nicht mehr besonders empfehlenswert erscheinen lassen. In der Theorie ist zwar die parallele Installation von mehreren Internetverbindungen auf einem PC kein Problem, in der Praxis wird dies durch „falsch verstandene" Benutzerfreundlichkeit der von den Providern zur Verfügung gestellten Installationssoftware manchmal zu einem Martyrium für die BenutzerIn; eventuell vorhandene aktuellere Versionen der Internetbrowser werden erbarmungslos und ohne Rückfrage durch die Version des Providers ersetzt, und die Auswahl für die KonsumentIn erschwert oder verunmöglicht, indem sich die Einwahlsoftware mit trickreichen Eingriffen in das Betriebsystem an die erste Stelle setzt. Natürlich arbeiten nicht alle Provider mit solchen Methoden, ein unbedarfter Internetnutzer muss aber auf unliebsame Überraschung gefasst sein, wenn er die Installations-CD eines neuen Providers in sein Laufwerk steckt.

Effektivität zunehmend in Frage gestellt

Der erreichbare Zugewinn an Anonymität bzw. die Erschwerung bei der Erstellung von gesamthaften Persönlichkeitsprofilen rechtfertigt den damit verbundenen Aufwand in der Regel nicht. Durch die zunehmende Tendenz die gesetzlichen Regelungen zugunsten einer umfassenden Überwachung auf Kosten der Privatsphäre abzuändern führt zu Bestrebungen, eine verpflichtende Speicherung der Logfiles von Internetprovidern vorzuschreiben, womit auch eine nachträgliche Zusammenführung von Daten verschiedener Provider ermöglicht wird. Der schon lange bestehende Wunsch von Ermittlungsbehörden, auch nachträglich auf Daten Telekommunikations- und Internetnutzung zugreifen zu können, hat durch die Anschläge vom 11. September 2001 sehr viel an politischer Unterstützung und Durchsetzungskraft gewonnen. Entsprechende Regelungen sind etwa in den EU-Staaten England und Frankreich bereits eingeführt worden, in der Schweiz oder den USA werden auch die Inhalte von e-Mails gespeichert oder überwacht, und auch die EU hat die Wege für erweiterte nationale Überwachungsmöglichkeiten geebnet (siehe dazu die Erläuterungen zur neuen Richtlinie „über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation" auf Seite 36). Welchen Weg Österreich dabei beschreiten wird, ist noch nicht eindeutig zu beantworten. Österreichische KonsumentInnen werden aber jedenfalls von den neuen Überwachungsinstrumenten erfasst, sofern sie Internetseiten aus betroffenen Ländern besuchen. Wer einen verlässlichen Grad an Anonymität erreichen will, sollte besser entsprechende Dienste in Anspruch nehmen oder Internet-Cafes für seine privaten Informations- und Kommunikationsbedürfnisse nutzen.

3.2.3 Zurückhaltung bei Preisgabe von Daten

Vergleich mit Offline-Gepflogenheiten

Auch bei dieser Empfehlung ist ein Vergleich mit dem Verhalten im nichtelektronischen Geschäftsverkehr hilfreich. Eine Identifizierung und Beobachtung des individuellen Verhaltens würde wohl die meisten Kunden vom Betreten eines Geschäftes abhalten, und Fragen des Verkaufspersonals nach per-

sönlichen Interessen und Vorlieben, die in keinerlei Zusammenhang zu den nachgefragten Produkten stehen, würden eher auf Entrüstung und Ablehnung als auf eine große Auskunftsbereitschaft stoßen. Im Internet ist das meist unbemerkte Erspähen der individuellen Interessen gang und gäbe, und auch die Erfragung persönlicher Daten unter Einbeziehung umfassender Fragen zu den Lebensumständen oder zur Freizeitgestaltung ist gängige Praxis. Da eine Vielzahl an Diensten im Internet unentgeltlich zur Verfügung steht, ist der Datenhunger durchaus verständlich. Die Nutzung der Daten für zielgerichtete Marketing- oder Werbekampagnen oder deren Verkauf an andere Unternehmen ist oft die wichtigste Finanzierungsquelle für die Anbieter von Gratisdiensten.

Schutz vor Missbrauch durch sparsame Datenweitergabe

Es bleibt natürlich der einzelnen KonsumentIn überlassen, wie viel an persönlichen Daten sie herzugeben bereit ist, um Dienste zu konsumieren oder an die eigenen Vorlieben adaptierte Informationsangebote oder Werbebotschaften zu erhalten. Man muss aber grundsätzlich damit rechnen, dass diese Daten sehr lange gespeichert und verwertbar bleiben, und auch weitergegeben und in völlig anderen Kontexten verwendet werden können. Es gibt sicher eine Reihe von Ausnahmen, in denen ein besonderes Vertrauensverhältnis besteht oder die Art des Dienstes umfangreiche und wahrheitsgemäße Angaben erfordert, in der Regel ist aber eine strikte Zurückhaltung bei der Preisgabe von persönlichen Daten oder die Nutzung unterschiedlicher Identitäten eine kaum verzichtbare Maßnahme, um künftigen missbräuchlichen Verwendungen vorzubeugen. Das heißt man verwendet Pseudonyme nicht, weil man jetzt „etwas zu verbergen hat“, sondern weil man nicht wissen kann, wer wann was mit den Daten machen wird.

mühsamer Schutz vor unbemerkter Datensammlung

Um der oft automatisch und unbemerkt durchgeführten Beobachtung des Surfverhaltens, zu entgehen, bedarf es einiger Kenntnisse und Mühen sowie den Einsatz technischer Hilfsmittel, zusätzlich muss man mit Einschränkungen bei der Verfügbarkeit von Webangeboten rechnen (siehe Abschnitt 3.2.6 über Privacy Enhancing Technologies). Eine bewusste Sparsamkeit bei der freiwilligen Angabe von zur persönlichen Identifikation geeigneten Daten kann aber die Zuordnung der einzelnen Beobachtungen zu einer Person und deren Zusammenführung zu umfassenden Profilen zwar nicht vollkommen verhindern, aber doch wesentlich erschweren.

Nutzung von Pseudonymen

Die meisten Gratisangebote lassen sich auch ohne vollständige oder wahrheitsgetreue Angaben uneingeschränkt nutzen. Und an die eigenen Bedürfnisse angepasste Dienste können ebenso gut mit Pseudonymen realisiert werden. Insbesondere wenn keine Datenschutzpolitik publiziert wird oder ein Einverständnis zur Weitergabe der Daten abverlangt wird, sind das Prinzip der Datensparsamkeit und die Nutzung von Pseudonymen unverzichtbar, wenn man Verletzungen der Privatsphäre vorbeugen möchte. Eine derart reduzierte Auskunftsbereitschaft ist nicht nur ein effizientes Mittel, das den KonsumentInnen zur Verhinderung von Missbräuchen zur Verfügung steht, sie ist auch eine der wenigen Maßnahmen, die den Zeitaufwand reduzieren kann, anstatt zusätzliche Ressourcen zu beanspruchen.

Vorsicht bei Gewinnspielen

Für eine Reihe von Aktivitäten gibt es aber keine Möglichkeit der anonymen Nutzung. So verlangen Anbieter von Online-Gewinnspielen in der Regel zumindest vollständige Kontaktdaten (Name, Adresse, Telefon, e-Mail), teilweise auch weit umfangreichere Angaben zur eigenen Person, bevor man als Teilnehmer registriert wird. Aus technischer Sicht würde die Angabe einer pseudonymen e-Mail-Adresse ausreichen, um im Falle eines Gewinnes verständigt werden zu können, da aber zumeist die Sammlung von Daten das wichtigste oder einzige Motiv des Veranstalters darstellt, ist dieses Vorgehen durchaus verständlich. Die KonsumentInnen müssen sich deshalb im Klaren sein, dass ihre im Rahmen von Gewinnspielen bekannt gegebenen Daten für Werbezwecke verwendet oder weiterveräußert werden. Wesentlich unsicherer

ist aber die Gegenleistung dafür. Abgesehen davon, dass bei Gewinnspielen prinzipiell keine Garantie besteht, jemals zu den GewinnerInnen zu gehören, lässt die Gestaltung des Spieles oder der Geschäftsbedingungen des Öfteren vermuten, dass ohnehin nicht daran gedacht wird, jemals Gewinne zu vergeben.

anonymes Einkaufen im Netz prinzipiell möglich

Die insgesamt wesentlich wichtigere Kategorie von Internetanwendungen, bei der eine anonyme Nutzung (bislang noch) nicht möglich ist, umfasst den Bereich entgeltlicher Dienste bzw. e-Commerce. Es gibt zwar eine Reihe von Ansätzen anonymes oder pseudonymes Einkaufen und Bezahlen im Internet zu ermöglichen, in der Praxis sind die KonsumentInnen aber spätestens beim Bezahlvorgang zumeist gezwungen, ihre Identität preiszugeben. In dem 1998 in Deutschland begonnenen Forschungsprojekt DASIT[42] (Datenschutz in Telediensten) wurden technische, rechtliche und organisatorische Aspekte der datenschutzkonformen Abwicklung von e-Commerce-Transaktionen untersucht und die praktische Umsetzbarkeit der Forderung nach anonymen Einkaufsmöglichkeiten mit einer Pilotinstallation bewiesen.[43]

Vielzahl an Bezahlsystemen erschwert Auswahl

In der jüngsten Zeit sind eine ganze Reihe neuer Bezahlverfahren für e-Commerce-Anwendungen entwickelt worden. Sie sind aber nur zum Teil anonym, wie etwa die auf dem Prepaid-Card-Prinzip beruhende Paysafe-Card.[44] Die Vielzahl an konkurrierenden Systemen ist sowohl für Händler als auch für KonsumentInnen problematisch, trägt sie doch zur jeweils nur geringen Verbreitung einzelner Verfahren bei. Vielversprechende Systeme zum anonymen Bezahlen im Internet scheiterten bereits wegen der Nichterreichung kritischer Massen. Ein ähnliches Schicksal wird der überwiegenden Mehrzahl der derzeit am Markt befindlichen Systeme vorhergesagt. Es bleibt abzuwarten, welche Systeme sich durchsetzen werden. Ohne gezielte Maßnahmen lässt sich kaum absehen, ob die Anonymität ein entscheidender Faktor bei der Auslese sein wird. Mögliche Maßnahmen können gesetzliche Vorschriften, die Integration in Kriterien für Gütesiegel oder Aufklärungskampagnen sein. Derzeit ist es für KonsumentInnen jedenfalls schwierig genug, ein sicheres und vertrauenswürdiges Bezahlsystem zu finden, das auch noch möglichst breit akzeptiert wird. Es ist daher anzunehmen, dass das zusätzliche Kriterium Anonymität für die Mehrzahl keine ausschlaggebende Rolle spielen wird. Eine KonsumentIn, die viel Wert auf ihre ungebrochene Privatsphäre legt, mag in einzelnen Fällen Wege finden, anonyme Einkäufe über das Internet zu tätigen, normalerweise wird die Wahl aber zwischen Verzicht auf die Transaktion via e-Commerce oder der persönlichen Zuordenbarkeit der konsumierten Leistungen zu treffen sein. Der e-Commerce ist jedenfalls noch weit davon entfernt, jene Natürlichkeit des anonymen Einkaufens bei gleichzeitiger Sicherheit bei mangelhafter Leistungserbringung zu bieten, die in der Offline-Welt als selbstverständlich vorausgesetzt wird.

---

[42] http://www.bmwi.de/Homepage/Politikfelder/Informationsgesellschaft/Aktionsprogramm/Dasit.jsp

[43] In diesem System bekommt jede der beteiligten Parteien nur die Informationen, die sie benötigt. Der Händler ist nur über das gekaufte Produkt und den bezahlten Preis informiert, nicht aber über den Namen und die Kreditkarteninformationen des Kunden; die Bank kennt die Identität des Käufers und den zu bezahlenden Betrag, nicht aber das Produkt; und die bestellte Ware wird an einen eingeschalteten Transportunternehmer übertragen. Dieser stellt die Verbindung zwischen Bestellung und Lieferanschrift her. Der Kunde selbst meldet sich mit einem zertifizierten Pseudonym an. Ein Rückschluss auf die wahre Identität ist nur im Konfliktfall möglich.

[44] http://www.paysafecard.com/at/de/

3.2.4 Andere Identitäten und anonyme Email-Adressen verwenden; insbesondere bei Chats und Newsgroup-Beiträgen

Schutz vor Belästigung

Dem Prinzip der Datensparsamkeit im vorigen Abschnitt folgend, gibt es für viele Angebote im Internet keine Veranlassung diese unter Bekanntgabe seiner wahren Identität zu nutzen. Neben den bereits genannten Gründen gibt es eine Reihe von weiteren Beweggründen, um Nicknames bzw. Spitznamen oder wechselnde Identitäten zu nutzen. Es ist bei bestimmten herkömmlichen geschäftlichen oder privaten Kontakten üblich, auf Chiffren oder Postfachadressen zurückzugreifen, um sich vor allzu aufdringlichen Interessenten oder unerwünschten Kontaktaufnahmen zu schützen. In der elektronischen Welt mit einer oft langen Speicherung und einem einfachen weltweiten Zugriff ist ein Wechsel der Identität umso mehr ratsam oder notwendig. Die Liste lässt sich um viele Argumente erweitern: So helfen unterschiedliche e-Mail-Adressen etwa die berufliche von der privaten Sphäre zu trennen. Pseudonyme können verhindern, dass etwa Suchanfragen zu physischen oder psychischen Leiden, die man interessenhalber oder im Auftrag von Bekannten durchführt, der eigenen Person zugeschrieben werden; und wenn man selbst davon betroffen ist, können Pseudonyme umso wichtiger sein, um zukünftige Diskriminierungen zu vermeiden. Sie erlauben es, in unterschiedliche Rollen zu schlüpfen und „personalisierte" Angebote zu nutzen, ohne damit für alle Zukunft mit bestimmten Charaktereigenschaften gebrandmarkt zu sein.

Trennung von Lebensbereichen

Chats nur vermeintlich kurzlebig

Die Empfehlung, insbesondere bei der Beteiligung an Chats und an Usenet-Newsgroups auf Pseudonyme zurückzugreifen, bezieht sich auf unterschiedliche Eigenschaften dieser Dienste. Chats bzw. Instant Messaging Dienste[45] verlocken durch die – oft nur vermeintliche – Kurzlebigkeit und Schnelligkeit zu unbedachten Äußerungen. Nun ist aber die Kurzlebigkeit keinesfalls garantiert, im Gegenteil, die Konversationen werden bei den zentralen Servern gespeichert und je nach gesetzlichen Vorgaben und Gepflogenheiten der Betreiber gewisse Zeitspannen aufbewahrt, viele Chat-Clients bieten auch standardmäßig die lokale Speicherung der ein- und ausgehenden Nachrichten an. Die prinzipielle Unsicherheit bei diesen Diensten, wer wirklich hinter den Pseudonymen steht und wer sonst noch die Chats belauschen und protokollieren kann, ist ein zusätzliches Argument für besondere Vorsicht. Bei Beiträgen zu Newsgroups ist die Langlebigkeit von gesendeten Anfragen oder Mitteilungen, die zu erhöhter Achtsamkeit und Zurückhaltung bei der Preisgabe seiner wahren Identität gemahnt. Die zahlreichen Usenet-Server, die den Zugang zu diesen Diskussionsforen eröffnen, bewahren die Beiträge zwar nur eine befristete Periode auf, die je nach Datenaufkommen und Politik der Betreiber von einigen Tagen aufwärts reicht, die Beiträge werden aber von anderen Unternehmen gespeichert und verfügbar gemacht. Nachdem der bekannte Usenet-Archivierungsdienst DejaNews seinen Betrieb eingestellt hat, war das Archiv für einige Zeit nicht verfügbar. Der Datenbestand wurde aber von Google.com[46] übernommen und ist wieder bis ins Jahr 1981 zurückreichend abrufbar. Beiträge, die unter einem wirklichen Namen bzw. mit e-Mail-Adressen, die Rückschlüsse auf die wahre Identität zulassen, publiziert werden, können unter Umständen vielfältige Aussagen über die politische Einstellung oder persönliche Interessen erlauben.

Usenet-Beiträge werden archiviert

---

[45] Bei textbasierten Chats oder Instant Messaging Diensten werden die Nachrichten wie bei e-Mails eingetippt. Allerdings sind der oder die Gesprächspartner gleichzeitig online; Nachrichten werden unmittelbar angezeigt und können auch sofort beantwortet werden. Neuere Clients bieten zumeist auch die Integration von Sprache oder Videos an. Bekannte Dienste sind etwa ICQ http://wwp.mirabilis.com/ oder der MSN Messenger von Microsoft http://messenger.msn.at/.

[46] http://groups.google.com/

Pseudonyme mit wenig Aufwand nutzbar

Grundsätzlich sind der Phantasie bei der Kreierung von Pseudoidentitäten keine Grenzen gesetzt, und auch die Generierung von pseudonymen e-Mail-Adressen ist bei diversen Freemail-Anbietern mit vertretbarem Aufwand durchführbar. Zusätzlich sind auch Software-Tools verfügbar, die die Generierung und Verwaltung von Pseudonymen weitgehend automatisieren und den NutzerInnen einen großen Teil des damit verbundenen Aufwands abnehmen, z. B. der weiter unten erwähnte CookieCooker.[47] In diesem Sinn ist die Nutzung unterschiedlicher Identitäten als Empfehlung ohne Einschränkung aufrechtzuerhalten und auch gängige Praxis bei einer Reihe von Aktivitäten am Internet. Allerdings sind zwei wichtige Faktoren zu beachten, die die Effektivität dieses Verhaltens zur Wahrung der Privatsphäre einschränken. Erstens ist die Verwendung von Pseudonymen nicht mit Anonymität gleichzusetzen, zweitens können andere Mechanismen im Internet wie Cookies oder Spyware die Wirksamkeit einer bewussten Zurückhaltung bei der Weitergabe von Daten und der Verwendung von Pseudonymen unterwandern, indem sie ohne Zutun und Wissen der NutzerInnen Informationen über sie sammeln. Die Funktionen von Cookies, Spyware und weiteren Möglichkeiten, unbemerkt Daten über die NutzerInnen zu sammeln, werden auf Seite 32 näher erläutert.

echte Anonymität nur schwer erreichbar

Zum Schutz der Privatsphäre gegenüber kommerziellen Datensammlern sind Pseudonyme bzw. wechselnde Identitäten in der Regel ausreichend, eine wirkliche Anonymität – d. h. es gibt auch keine Rückführbarkeit auf die wahre Identität über die verwendete IP-Adressen – ist aber nur eingeschränkt und mit Mühen erreichbar, sofern man nicht auf anonyme Zugangsmöglichkeiten wie Internet-Cafes ausweicht. Um zu verhindern, dass persönliche Daten, die etwa bei e-Commerce-Transaktion notwendigerweise preisgegeben werden müssen, mit Informationen, die bei vermeintlich anonymen Besuchen von Websites generiert wurden, miteinander verkettet werden, sind zusätzlich Maßnahmen notwendig. Dazu gehören Einschränkungen bei der Annahme von Cookies und die Verhinderung bzw. Entfernung von Spyware-Programmen. Dabei sind die NutzerInnen aber auf zusätzliche Tools angewiesen, die in Abschnitt 3.2.6 über Privacy Enhancing Technologies diskutiert werden.

3.2.5 Gegebenenfalls eigene Beiträge aus Newsgroup-Archiv entfernen und Archivierung blockieren

Anleitung zum Löschen und Blockieren nur indirekt zugänglich

Es ist heute in vielen Situationen gängiger Brauch, eine Suche über Personen im Internet durchzuführen, um sich ein Bild über sie machen zu können, ehe man Entscheidungen fällt oder sich zu persönlichen Treffen verabredet. Angesichts dieser Praxis kann der Wunsch, eigene Beiträge aus dem öffentlich zugänglichen Archiv zu löschen, durchaus verständlich sein. Wie Deja.com bietet auch der Nachfolger Google diese Möglichkeit an, allerdings nur, wenn man die englische Suchseite von Google Groups anwählt; von dort gelangt man zu einer Unterseite[48], die weitere Anweisungen enthält. Auf den entsprechenden deutschsprachigen Seiten fehlen unverständlicherweise diese Anleitungen; ebenso der Hinweis, wie die Archivierung neuer Beiträge unterbunden werden kann. Wird im Beitrag (Posting) der Text „X-No-Archive: yes“ entweder als Header oder als erste Zeile des Beitrags eingetragen, so wird dieser Beitrag von Google Groups und den meisten, aber nicht allen Usenet-Archiven

[47] Wird für den Zugang zu einem Internetangebot eine Anmeldung gefordert, so kann dieses Tool auf Wunsch ein Pseudonym inklusive einer gültigen e-Mail-Adresse generieren und das Anmeldeformular auf Basis dieser Daten ausfüllen. Nähere Informationen dazu finden sich auf http://cookie.inf.tu-dresden.de/index_de.html.

[48] http://www.google.com/googlegroups/help.html

nicht gespeichert. Im Zweifelsfall ist ein Pseudonym vorzuziehen, wenn man nicht für alle Zeit mit dem Inhalt des Postings verbunden werden möchte.

Die Entfernung alter Beiträge bzw. die Verhinderung der Archivierung neuer Postings verlangt ein kleines Maß an Grundwissen, das bei Neulingen, die von der Vielfalt der Themen und der auf den ersten Blick scheinbaren Kurzlebigkeit von Beiträgen zu Usenet Newsgroups geblendet sein mögen, nicht vorausgesetzt werden kann.

3.2.6 Privacy Enhancing Technologies (PETs)

Schutz der Privatsphäre bedarf auch technischer Hilfen

Ein bewusster Umgang mit dem Medium Internet kann viel dazu beitragen, die eigene Privatsphäre zu schützen und Missbräuchen persönlicher Daten vorzubeugen. Diese Strategie stößt aber oft auf Grenzen, weil etwa keine oder ungenügende Informationen über das virtuelle Gegenüber und dessen Umgang mit persönlichen Daten vorhanden sind, weil bestimmte Dienste nur unter Bekanntgabe personenbezogener Daten in Anspruch genommen werden können, oder weil Datenspuren ohne Kenntnis und Einverständnis der NutzerInnen gesammelt und ausgewertet werden. Nun sind Probleme des Datenschutzes nicht erst mit neuen Informations- und Telekommunikationstechnologien entstanden, sie haben aber durch sie vollkommen neue qualitative und quantitative Dimensionen erreicht. Es liegt daher nahe, diese Probleme ihrerseits durch technische Maßnahmen zu entschärfen oder zu beseitigen, die unter dem Akronym PETs (Privacy Enhancing Technologies) zusammengefasst werden. Der Begriff PETs umfasst eine Reihe von Technologien, die – oft gemeinsam mit organisatorischen Maßnahmen – das Prinzip der Datensparsamkeit in Informations- und Kommunikationstechnologien transformieren, eine anonyme oder pseudonyme Nutzung von Diensten ermöglichen, oder den Nutzer direkt bei der Wahrung seiner Privatsphäre unterstützen.

technische Umsetzung des Prinzips der Datensparsamkeit

Wirksamkeit und Eignung für durchschnittliche Nutzer

In diesem Abschnitt werden oft gegebene Empfehlungen zur Nutzung technischer Hilfsmittel in Hinblick auf ihre Benutzerfreundlichkeit und Wirksamkeit analysiert. Sie betreffen neben allgemeinen Ratschlägen, die Sichereinstellungen der benutzten Software zu erhöhen, vor allem Dienste, die eine anonyme Nutzung des Internets ermöglichen sollen und den Einsatz von Softwaretools zum Schutz der Privatsphäre am eigenen PC. Bei der Analyse steht nicht so sehr die prinzipielle Eignung der Empfehlungen im Vordergrund, als die Anwendbarkeit für durchschnittliche Nutzer, die über kein besonderes technisches Hintergrundwissen verfügen. Ebenso wenig ist eine Bewertung unterschiedlicher Dienste oder Softwaretools im Sinne eines Vergleichstests beabsichtigt, sondern vielmehr ein exemplarisches Aufzeigen der Möglichkeiten und Grenzen des individuellen Einsatzes von PETs anhand der drei zentralen Empfehlungen zur Verschlüsselung, zur Nutzung von Anonymisierungsdiensten und zum Einsatz von Datenschutzsoftware. Unausgesprochene Grundvoraussetzungen dafür sind natürlich Kenntnisse über Gefahren und ein Bedürfnis, die eigene Privatsphäre zu schützen, die erst die Motivation liefern, diese Maßnahmen zu ergreifen.

Verschlüsselungssoftware nutzen

oft empfohlen, kaum genutzt

Der Einsatz von Verschlüsselungssoftware, insbesondere zum Schutz der e-Mail-Kommunikation, ist wohl eine der am häufigsten gegebenen – und fast ebenso oft nicht befolgten – Empfehlungen. Die Verschlüsselung von e-Mails wird oft mit dem Verwenden von Briefumschlägen bei herkömmlichen Postsendungen verglichen. Dieser Vergleich ist aber (derzeit) nur auf den ersten

Blick berechtigt; und es ist nicht Nachlässigkeit allein, die die weit überwiegende Mehrzahl an e-Mail-Nutzern auf dieses in der nicht-elektronischen Kommunikation alltägliche Mittel verzichten lässt.

Nutzung erfordert eingehende Beschäftigung

Im Gegensatz zu Briefumschlägen verursacht die Verschlüsselung erhebliche Mühen und Kosten. Die Kosten werden in erster Linie nicht durch die virtuellen Briefumschläge bzw. die Tools zum Verschließen verursacht – es sind genügend Freeware-Versionen davon erhältlich –, sondern durch die Zeit, die zum Finden, Aussuchen, Installieren und Erlernen des Gebrauchs erforderlich ist. Der erste Teil, das Finden von leistungsfähiger und kostenfreier Verschlüsselungssoftware, ist schnell getan, gilt doch das von Phil Zimmermann entwickelte Programm PGP[49] (Pretty Good Privacy) seit Jahren als Standard für sichere Public Key Kryptographie für Privatpersonen. Aber schon bei der Frage, welche der vielen verfügbaren Versionen man verwenden soll, fällt die Entscheidung nicht so leicht. Eingeschworene PGP-Nutzer bevorzugen ältere Versionen, bei denen der Quellcode offen gelegt ist; Anfänger werden eher zur neuesten Version (7.0.3) greifen, die mehr Komfort und bessere Integration in Standard-e-Mail-Clients versprechen. Die neueren Versionen beinhalten auch leistungsfähigere Algorithmen und beherrschen längere, und damit sicherere Schlüssel, mit dem unerwünschten Nebeneffekt, dass Inkompatibilitäten zwischen den Versionen entstehen können.

ungewisse Zukunft des Standardprogramms PGP

Die Versionsfrage wird sich aber wahrscheinlich überhaupt nicht mehr stellen, da die weitere Entwicklung von PGP gestoppt wurde. Neben der Freeware-Version wurden auch kommerzielle Versionen entwickelt. Offensichtlich mit geringem Erfolg, da mit März 2002 diese Produktlinie von der Softwareschmiede Network Associates eingestellt wurde. Versuche, PGP zu verkaufen waren ebenso erfolglos wie Bestrebungen, den Quellcode der neuen Versionen freizubekommen. Es gibt zwar mit dem Projekt GnuPG[50] (GNU Privacy Guard) Bestrebungen, freie Versionen weiter zu entwickeln, allerdings sind damit Jahre an Entwicklungsarbeit verloren. Dies betrifft weniger die Sicherheit und Stärke der Verschlüsselungstechnologien, als die Benutzerfreundlichkeit und Integration in Standardsoftware. Als integrierte Lösung zur Verschlüsselung von lokalen Dateien, von standardisierten Lösungen für e-Mails, für VPNs (Virtuelle Private Netzwerke) und sichere Datensysteme war und ist PGP konkurrenzlos. Für den Nachfolger GnuPG ist derzeit nur ein grafisches Benutzerinterface im Beta-Stadium verfügbar; und bereits das Dateiformat des Softwaredownloads <gnupg-1.0.7.tar.gz> und das Fehlen einer Setup-Datei im Download zeigen, dass als Zielpublikum wohl nicht die DurchschnittsnutzerInnen gemeint sind.

Mangelware Kommunikationspartner

Dabei ist schon die Nutzung von PGP trotz der Integration in gebräuchliche Betriebssysteme und Anwendungen nicht trivial. Die Generierung und Verwaltung von Schlüsseln erfordert, dass man sich mit den Grundlagen der Public Key Kryptographie beschäftigt, die Nutzung der Anwendungen wird durch die zusätzlichen Funktionen komplexer, und wenn all diese Hürden genommen sind, lässt sich die Verschlüsselungsoption oft mangels entsprechender Kenntnisse und Softwareausstattung bei den Kommunikationspartnern nicht nutzen.

geringerer Schutz bei einfacheren Alternativen

Dass es auch einfacher und intuitiver geht, zeigt etwa das bei Kreditkartentransaktionen am Internet übliche SSL-Protokoll (Secure Socket Layer), welches eine verschlüsselte Datenübertragung ohne zusätzlichen Aufwand für den Nutzer bewerkstelligt. Neuere Versionen von e-Mail-Clients bieten ebenfalls eine SSL-Verschlüsselungsoption an, die automatisch in Kraft tritt, sofern der

---

[49] Dokumentation, Downloads und Hintergrundinformation finden sich auf der International PGP Home Page http://www.pgpi.org/.

[50] Weitere Informationen sowie Downloads dazu finden sich auf http://www.gnupg.org/en/gnupg.html.

e-Mail-Server dies bereits unterstützt. Allerdings betrifft die Verschlüsselung nur den Transport zwischen Client und dem eigenen e-Mail-Server; die Mails werden aber weiterhin unverschlüsselt abgespeichert und an die Zieladresse weitergeleitet. Die Funktionalität und der Schutz, den PGP bietet, werden somit in keiner Weise erreicht.

Empfehlung nur beschränkt umsetzbar

Die grundsätzlich sinnvolle Empfehlung, Verschlüsselungssoftware einzusetzen, kann deshalb nur mit Einschränkungen aufrechterhalten werden. Die NutzerInnen müssen jedenfalls bereit sein, sich mit elementaren Grundlagen der Kryptographie und der Funktionsweise der Software auseinanderzusetzen. Bei der Wahl der Software sind sie gezwungen, zwischen PGP, das von der Bedienbarkeit und den Leistungsmerkmalen her führend ist, aber nicht mehr weiterentwickelt wird, dem frei verfügbaren GnuPG, das noch weit mehr als nur grundlegende PC-Kenntnisse verlangt, oder aber auf eine der wenigen kommerziellen Lösungen zu setzen, wobei aber kaum Chancen bestehen, ohne vorherige Vereinbarungen auf Kommunikationspartner mit passender Ausstattung zu treffen.

Nachfolger von PGP nur für versierte PC-Nutzer

Anonyme Mail- und Webdienste nutzen

Anonymität des Alltags im Netz nicht gegeben

Bei dieser Empfehlung geht es darum, Selbstverständlichkeiten im normalen Alltag – etwa sich in einem Geschäft über Produkte zu informieren, ohne sich identifizieren zu müssen, oder etwa Briefe abzusenden, ohne eine Absenderadresse angeben zu müssen – bei der Nutzung elektronischer Medien ebenfalls zu realisieren. Im Internet ist aus technischen Gründen eine eindeutige Zuordnung notwendig, um die in Datenpakete transformierte Information abfragen und zustellen zu können. Anhand der IP-Adressen werden Abfragen an die zuständigen Server geleitet und die Antworten zugestellt. Anhand der IP-Adressen kann der Rechner identifiziert, und je nach dem Verhalten der NutzerInnen mehr oder weniger leicht, auch deren Identität festgestellt werden.

öffentliche Zugänge haben eingeschränkte Funktionalität

Eine sehr effektive Möglichkeit, Internetdienste anonym zu nutzen, besteht darin, auf anonyme Zugangsmöglichkeiten auszuweichen, etwa – anstatt des PCs zuhause oder am Arbeitsplatz – öffentliche Terminals oder Internet-Cafes zu nutzen. Diese Option kann aber mit vielfältigen Einschränkungen oder zusätzlichen Kosten verbunden sein, wie etwa fehlenden Möglichkeiten, Dokumente zu speichern oder auszudrucken, fehlende Privatsphäre im öffentlichen Raum, begrenzte Öffnungszeiten oder vergleichsweise hohen Gebühren. Die zweite Möglichkeit zur anonymen Benutzung von Internetangeboten bieten technische Hilfsmittel und Dienste. Die Prinzipien anonymer Internetdienste wurden bereits zu Beginn der achtziger Jahre entwickelt (Chaum 1981), und seit einigen Jahren können die technischen Probleme als gelöst gelten (Ian Goldberg 1997). Für normale NutzerInnen, die ohne technisches Detailwissen anonym surfen oder per e-Mail kommunizieren möchten, können die Probleme aber keinesfalls als gelöst angesehen werden.

anonyme Internetdienste prinzipiell verfügbar, ...

... aber oft nur für Spezialisten nutzbar

Eine Suche nach Stichwörtern wie „anonyme e-Mail“, „remailer“[51] etc. wird zwar zahlreiche Fundstellen hervorbringen. Beim Verfolgen dieser Links findet man sich aber oft auf Seiten wieder, die eine eingehende Beschäftigung mit Grundlagen der Kryptographie erfordern, um den Anweisungen folgen zu kön-

[51] Bei der einfachsten Konzeption von Remailern werden die Nachrichten an eine „vertrauenswürdige“ Stelle geschickt, die die wirkliche e-Mail-Adresse des Absenders durch eine pseudonyme Adresse ersetzt und die Antworten wieder an den ursprünglichen Absender weiterleitet. Aufgrund der Verletzlichkeit dieses Konzepts ist diese Form heute nicht mehr üblich. Stattdessen werden kryptographische Verfahren eingesetzt, die wesentlich mehr Sicherheit bieten, aber auch einen höheren Aufwand erfordern.

nen. Die Adressen von kostenfreien Remailern werden in themenspezifischen Newsgroups veröffentlicht und Hinweise gegeben, keine Listen zu verwenden, die älter als 24 Stunden sind, weil ansonsten die Wahrscheinlichkeit an eine nicht mehr aktive Adresse zu geraten zu hoch wird. Es sind überwiegend freiwillige und unbezahlte Aktivitäten, in denen die Software entwickelt wird und mit denen versucht wird, Netzwerke von Rechnern zur Anonymisierung aufzubauen. Privatpersonen, die ihre Rechner zur Verfügung stellen, ziehen sich oft schnell wieder zurück, wenn sie merken, dass die installierte Anonymisierungssoftware ihre sonstigen Aktivitäten am PC verzögert oder wenn sie von ihrem Provider gemahnt werden, weil unerlaubterweise Serverdienste[52] am Rechner aktiv sind. Viele Remailer-Dienste erweisen sich als dementsprechend kurzlebig und unzuverlässig. Technisch versierte Personen mit genügend Zeit finden genügend Möglichkeiten, ihre e-Mail-Kommunikation mit einigermaßen gesicherter Anonymität abwickeln zu können. Es gab auch Bemühungen, grafische Benutzerinterfaces zu erstellen, um die Nutzung zu vereinfachen. Teilweise sind sie noch am Internet erhältlich, „aktuelle" Versionen, die mehrere Jahre zurückliegen, Hinweise auf mehrere Generationen alte Betriebssysteme und auf nicht mehr aktive Internetserver zeigen, dass Enthusiasmus nicht immer ausreicht, um funktionsfähige Konzepte in für die breite Nutzung angepasste Formen zu bringen.

kommerzielle Alternativen zu freien Mail-Diensten nur bedingt geeignet

Ein Ausweichen auf kommerzielle Dienste ist aus mehreren Gründen keine wirklich empfehlenswerte Alternative. Erstens gibt es kaum Anbieter, zweitens wird mit dem Bezahlvorgang die Anonymität gegenüber dem Diensteanbieter aufgegeben und drittens wird im Gegensatz zu den freien Diensten das zugrunde liegende technische Konzept meist nicht veröffentlicht. Somit bleibt die Frage nach dem Vertrauen, das man in den Anbieter setzen kann, unbeantwortbar. Letztlich ist zwar eine absolute Anonymität ohnehin nicht erreichbar, allerdings reicht bei den modernen Konzepten, die teilweise hinter den freien Remailern stehen, ein einziges vertrauenswürdiges Element in der Kette von eingebundenen Servern, um einen relativ hohen Grad an Anonymität gewährleisten zu können.

wenig Möglichkeiten anonymen Surfens

Noch geringer ist die Auswahl bei den Anbietern von Diensten zum anonymen Surfen am Internet. Zwei der bekanntesten Dienste, Freedom.Net von Zero Knowledge Systems und Safeweb.Com stellten im vergangenen Herbst ihre Dienste ein. Insbesondere von Zero Knowledge Systems wurde betont, dass rein kommerzielle Gründe für die Einstellung verantwortlich waren, nämlich zu wenige NutzerInnen, die die kostenpflichtigen Premiumdienste in Anspruch genommen haben. Die zeitliche Nähe zu den Terroranschlägen vom 11. September 2001 hat aber Spekulationen über Druck von politischer Seite nicht verstummen lassen.

systembedingte Verzögerungen beim Seitenaufbau

Die Anonymisierung von Webzugriffen erfordert eine entsprechend leistungsfähige Infrastruktur, da hier im Gegensatz zu e-Mail-Diensten, jede Verzögerung unmittelbar für die NutzerInnen spürbar wird. Diese Verzögerungen beim Seitenaufbau sind aber systembedingt, je nach Grad der Anonymisierung müssen die Daten eine oder mehrere zusätzliche Zwischenstationen durchlaufen. Die Sicherheit gegen Attacken steigt mit der Zahl der NutzerInnen, d. h. mit der Auslastung der Anonymisierungsserver und entsprechend längeren Antwortzeiten.

---

[52] Die nichtkommerzielle Nutzung des Internets erlaubt den Zugriff auf beliebige Internetdienste, sie erlaubt aber nicht, selbst solche Dienste anzubieten bzw. einen Internetserver zu betreiben. Je nach Attraktivität des Angebots kann ein Server sehr viel Datenverkehr erzeugen. Unternehmen, oder auch Privatpersonen, die Serverdienste anbieten wollen, müssen daher auf wesentlich teurere Dienste der Internetprovider zurückgreifen.

oft kein merkbarer Qualitätsunterschied zwischen freien und bezahlten Diensten

Es ist daher auch verständlich, dass in der Regel die Betreiber von Anonymisierungsdiensten Gebühren für deren Nutzung einheben. Die meisten anonymen Webdienste bieten, wenn überhaupt, nur einen zeitlich oder funktional eingeschränkten Gratiszugang an, und führen zu wesentlich längeren Zeiten für den Aufbau von abgerufenen Seiten. Im Rahmen des – nicht repräsentativen – Experiments konnten allerdings keine gravierenden Geschwindigkeitsunterschiede zwischen bezahlten und freien Diensten festgestellt werden. Das mag aber daran gelegen sein, dass bis auf den im übernächsten Absatz erwähnten Dienst der Technischen Universität Dresden alle Server zumindest eine Zwischenstation in den USA einlegten. Eine Abfrage einer österreichischen Seite muss dabei viermal den Atlantik überqueren,[53] sodass auch eine tatsächlich vorrangige Abwicklung am Anonymisierungsserver wenig Auswirkung auf die Gesamtantwortzeit haben kann.

eingeschränkte Nutzbarkeit

Noch problematischer als der oft extrem langsame Zugriff ist aber die manchmal beobachtete komplette Unerreichbarkeit der Anonymisierungsdienste. Gerade NutzerInnen, die in datenschutzbewusster Absicht die Sicherheitseinstellungen ihrer Internetbrowser auf ein hohes Niveau setzen, bleiben bei einigen Anbietern ausgeschlossen, da diese Cookies oder am PC auszuführende Software voraussetzen. Dabei wird der Nutzer oft im Regen stehen gelassen; es findet sich kein Hinweis, dass bestimmte Browsereinstellungen den Zugang verhindern und welche Veränderungen vorzunehmen wären.

funktionierender Dienst mit offener Zukunft – JAP

Als relativ stabil und mit vertretbarer Verzögerung arbeitender Dienst erwies sich JAP (Java Anon Proxy).[54] Dieser im Rahmen eines Forschungsprojekts an der Technischen Universität Dresden erstellte Dienst basiert auf einem kleinen lokal zu installierenden Client, der die Kommunikation zu den Anonymisierungsservern übernimmt. Bis auf die bereits erwähnten Verzögerungen können die NutzerInnen wie gewohnt ihren Browser verwenden. Die Finanzierung und damit Aufrechterhaltung dieses Diensten nach dem Ende des Forschungsprojekts ist noch nicht geklärt.

Auswahl für KonsumentInnen schwierig

Die Empfehlung zur Nutzung anonymer e-Mail- und Webdienste kann grundsätzlich aufrechterhalten werden, allerdings sind auch hier einige einschränkende Anmerkungen notwendig. Für einige Dienste sind etwa derart umfangreiche Kenntnisse erforderlich, dass sie nur einem kleinen NutzerInnenkreis zugemutet werden können, der aber entsprechende Empfehlungen ohnehin nicht notwendig hat. Ein Neuling stößt bei Recherchen im Internet auf eine scheinbar große Auswahl an Diensten und Tools, die ihn bei der anonymen Nutzung des Internets unterstützen, die sich aber oft als veraltet oder nicht mehr verfügbar erweisen. Bei den wenigen verbleibenden Angeboten fehlen Informationen, die den KonsumentInnen die Auswahl erleichtern und das Vertrauen sichern könnten. Kommerzielle Angebote sind mit jährlichen Mindestkosten von etwa € 30,– verbunden, die aber je nach Leistungsumfang auch wesentlich höher liegen können, oft ohne merkbare Vorteile gegenüber vergleichbaren Gratisdiensten.

---

[53] Z. B. gelangt die Anfrage zuerst an den Server in den USA, diese wird anonymisiert an den österreichischen Anbieter gerichtet, der seine Antwort wieder in die USA sendet, von wo dann die Information erst an die NutzerIn in Österreich gesendet wird.

[54] http://anon.inf.tu-dresden.de/

Spezialisierte Softwarepakete zum Schutz der Privatsphäre und des eigenen Rechners einsetzen

zahlreiche Hilfsmittel zum Schutz des eigenen PCs

Es gibt zahlreiche Gefahren und Risken, die bei der Nutzung von Computern auftreten können, insbesondere wenn man sich in offenen Netzwerken wie dem Internet bewegt. Viren können Daten und Programme zerstören, Trojaner den eigenen PC für Attacken von außen öffnen, Kollegen oder Familienmitglieder Einsicht in nicht für sie bestimmte Dokumente nehmen, oder unbemerkt Mechanismen in Gang gesetzt werden, um Informationen über die BenutzerInnen aufzuzeichnen und zu sammeln. Dementsprechend zahlreich sind auch die Hilfsmittel, die diese Risken verhindern oder mindern sollen. Sie reichen von Antivirenprogrammen über Tools, die den lokalen oder externen Zugriff auf den Rechner steuern bis zu jener Kategorie, die in diesem Kontext wichtig sind, nämlich Werkzeugen, die dem unbemerkten Ausspionieren der NutzerInnen einen Riegel vorschieben.

heimliche Datensammlung weit verbreitet

Die heimliche Sammlung von Daten widerspricht zwar jeglichen Grundsätzen des Datenschutzes und eines verantwortlichen und fairen Umgangs mit den KundInnen, dennoch sind diese Methoden weit mehr verbreitet, als gemeinhin angenommen. Laut einer von Intelytics[55], einem Anbieter von Programmen zum Schutz der Privatsphäre im Jahr 2001 durchgeführten Überprüfung von mehrt als 50 Millionen kommerziellen Websites, benutzten beinahe ein Drittel davon sogenannte Web-Bugs, unter den Top 100 e-Commerce-Anbietern fanden sich 74 Unternehmen, die auf diese Art Daten von BesucherInnen sammelten.

Cookies: nützlich und gefährlich

Es werden vor allem drei Kategorien von Instrumenten genutzt, um unbemerkt und zumeist ohne Einverständnis der Nutzer Daten über sein Verhalten aufzeichnen zu können. Die erste Kategorie sind sogenannte Cookies, das sind kleine Textdateien, die von den besuchten Webseiten lokal am PC gespeichert werden. Sie dienen dazu, die BesucherInnen wiederzuerkennen, können angepasste Angebote erstellen, oder den BenutzerInnen etwa die wiederholte Eingabe von Passwörtern ersparen. Cookies können durchaus nützliche und hilfreiche Funktionen übernehmen. Sie können aber auch dazu dienen, Akten anzulegen und die NutzerInnen über lange Zeiträume zu beobachten. Insbesondere problematisch wird dies, wenn Cookies über die Grenzen einzelner Websites hinweg eingesetzt werden. Persönliche Angaben wie Name, Anschrift, oder e-Mail-Adresse, die z. B. anlässlich eines Einkaufs übers Internet bekannt gegeben wurden, können auf diese Weise mit Informationen verknüpft werden, die ein Konsument beim vermeintlich anonymem Surfen auf gänzlich anderen Seiten preisgibt, und die etwa Aussagen über politische Zugehörigkeiten, religiöse Anschauungen oder sexuelle Neigungen erlauben können.

Web-Bugs als vielfältige Instrumente zur Datensammlung

Web-Bugs bzw. e-Mail-Bugs bilden die zweite Kategorie. Zumeist basieren sie auf winzigen, transparenten und daher unsichtbaren Grafiken, die über einen Link in eine Webseite oder ein e-Mail eingebettet sind. Wird die mit Bugs versetzte Seite oder Nachricht aufgerufen, so wird die unsichtbare Grafik geladen. Im einfachsten Fall stellen diese Bugs eine Art von Empfangsbestätigung aus; Werberinge, wie etwa DoubleClick, können so die Spuren einzelnet Nutzer auf unterschiedlichen Webseiten verfolgen, oder Versender von Werbemails können abgerufene von toten e-Mail-Adressen unterscheiden. Zumeist werden Web-Bugs aber genutzt um Cookies zu setzen oder auszulesen und somit die unbemerkte Erstellung von umfassenden Benutzerprofilen zu ermöglichen. Sie können aber auch dazu eingesetzt werden, ausführbaren Code zu laden und zu versuchen, Zugriff auf am PC vorhandene Daten zu erhalten.

---

[55] http://www.intelytics.com/

unerwünschte Beigaben zu Gratissoftware ...

Die dritte Kategorie umfasst Adware und Spyware. Damit bezeichnet man Programme, die lokal am eigenen PC installiert werden und Werbung herunterladen oder das Surfverhalten des Benutzers ausspionieren. Während reine Adware sich auf die Präsentation von Werbeeinblendungen beschränkt und eher eine Belästigung und Aufblähung des Datendownloads darstellt – Umstände, die man bei Gratissoftware manchmal einfach in Kauf nehmen muss, dient Spyware allein zur Datensammlung, wobei die Grenzen oft fließend sind und beide Funktionen in Gratissoftware integriert werden. Spyware oder Adware finden sich meist als Beigaben zu freier Software, insbesondere Filesharing-Software ist in Verruf geraten, oft mit Spyware vollgespickt zu sein.

... installieren sich unbemerkt und permanent ...

Für die KonsumentInnen ist oft nicht oder nur schwer erkennbar, dass sie mit der Nutzung bestimmter Programme Spyware mit installierten. Wenn sich Hinweise dazu finden, sind sie im „Kleingedruckten" bei der Installationsroutine versteckt, welches zumeist ohne Gelesen zu werden übersprungen wird, oder die Formulierungen lassen die Funktion der zusätzlich installierten Komponenten nicht klar erkennen. Zumeist wird die Spionagesoftware ins System integriert und automatisch bei jedem Einschalten des PCs geladen, ohne dass dazu die Software verwendet werden muss, mit der man sich diese unliebsamen Gäste eingehandelt hat. Und die Spyware bleibt aktiv, selbst wenn die diesbezüglichen Programme wieder deinstalliert worden sind. Spyware kann daher sämtliche Aktivitäten am Internet protokollieren, unabhängig davon, ob man etwa Cookies zulässt oder sich auf Webseiten bewegt, die zu bestimmten Werberingen gehören.

... und umgehen die bewusste Zurückhaltung bei der Datenfreigabe

Das grundsätzliche Problem dieser drei Mechanismen zum Ausspähen von InternetnutzerInnen ist deren verstecktes und unbemerktes Funktionieren. Selbst bewusste NutzerInnen, die eine große Zurückhaltung bei der Weitergabe persönlicher Daten üben, können davon betroffen sein, sofern nicht Gegenmaßnahmen ergriffen werden. Ohne zusätzliche Tools fällt dies aber schwer oder ist undurchführbar. Zwar bieten neuere Versionen von Webbrowsern unter den Sicherheits- oder Datenschutzeinstellungen beispielsweise Optionen an, wie mit Cookies umzugehen ist, eine befriedigende und benutzerfreundliche Lösung fehlt aber. Eine grundsätzliche Ablehnung von Cookies sperrt den Nutzer von vielen Angeboten aus, oft ohne Hinweis, dass die eigenen Sicherheitseinstellungen dafür verantwortlich zu machen sind. Eine individuelle Anfrage bei jedem einzelnen Cookie schließt sich aus mehreren Gründen aus: Das dauernde Bestätigen bzw. Ablehnen ist nur für kurze Zeit zumutbar, zudem fehlt zumeist ohnehin die notwendige Information, um ein Annehmen oder Ablehnen rational begründen zu können. Traditionelle Tools zum Cookie-Management unterstützen die NutzerInnen dabei, indem sie die Auswahl erleichtern und automatisieren, etwa durch Listen von verdächtigen Cookie-Adressen. Wie bei anderen Tools zum Schutz der Privatsphäre finden sich auch hier einige Programme nur in veralteten Versionen. Ein anderes Konzept gegen das ungewollte Ausspionieren durch Cookies verfolgt der bereits bei Verwaltung von Pseudonymen genannte CookieCooker (siehe Kapitel 3.2.4). Nützliche und gewollte Cookies können wie gewohnt akzeptiert werden, ungewollte Cookies in einer Art Tauschbörse mit anderen Nutzern dieses Tools nach dem Zufallsprinzip austauschen. Dadurch soll die Erstellung von Nutzerprofilen mittels Cookies und deren Nutzung in der Werbeindustrie insgesamt ad absurdum geführt werden, ein Ziel, dass wahrscheinlich nur erreichbar sein wird, wenn eine hinreichende Anzahl von InternetnutzerInnen sich an derartigen Tauschdiensten beteiligt.

Trade-Off zwischen Sicherheit und Bequemlichkeit

Web-Bugs nur mit Zusatzsoftware beherrschbar

Eine Blockade von Webbugs ist nicht ganz einfach. Unsichtbare Grafiken können auch als Mittel zur grafischen Gestaltung von Webseiten eingesetzt werden, etwa um bestimmte Abstände zwischen einzelnen Elementen zu erzwingen; und Web-Wanzen können getarnt werden oder auf andere Weisen platziert werden. Spezielle Tools oder Firewalls mit Anti-Webbug-Funktionen, die auf

typische Merkmale oder aber auf Adresslisten von bekannten Datensammlern aufbauen, können daher keinen hundertprozentigen Schutz bieten. Zumeist werden lokale Proxyserver, die unerwünschte Werbebotschaften blockieren, auch zum Herausfiltern von Webbugs eingesetzt, da die Mehrzahl der Webbugs ohnehin von denselben Unternehmen verwendet wird. Eine für den Privatgebrauch freie Software ist etwa der Webwasher[56], neben dieser Funktion bietet diese Software noch eine Reihe weiterer Optionen zum Schutz der Privatsphäre. Ein aufschlussreiches Tool ist Bugnosis[57], das in der zum Zeitpunkt der Berichterstellung verfügbaren Version noch keine Schutzfunktion beinhaltet, aber die Webbugs sichtbar macht und versucht, die e-Mail-Adresse für Beschwerdemails zu eruieren.

Vorsicht bietet keinen 100 %igen Schutz

Einen gewissen, wenn auch nicht vollkommenen Schutz gegen Spyware bietet das sorgfältige Lesen der Bedingungen, die an die Installation und Nutzung von Freeware gebunden ist. Da die zusätzliche Installation von Adware oder Spyware aber nicht immer transparent gemacht wird, und Deinstallationsoptionen oft nicht vorgesehen sind bzw. die Programme manchmal mit Absicht für Nichtexperten unentfernbar in die Systemebene eingebettet sind, bleibt auch hier nur der Griff zu Tools, die zum Erkennen und Entfernen von Spyware entwickelt wurde. Der bekannteste Vertreter dieser Gattung ist AD-Aware,[58] eine kostenlos einsetzbare Software, die eventuell vorhandene Adware oder Spyware am eigenen PC identifiziert und die Option zur Entfernung anbietet. Eine weitere, auch nicht gänzlich sichere Option gegen Spyware stellen sogenannte Firewalls dar. Diese beschränken bzw. öffnen den Datentransfer je nach Anwendungen, verwendeten Ports oder Internet-Adressen. Wenn eine unbemerkt installierte Anwendung versucht, Daten über das Internet zu senden, wird dies dem Nutzer gemeldet und er um eine Erlaubnis gefragt. Allerdings versuchen manche Spyware- oder Adware-Programme ihren Transfer in den Nutzdatenstrom einzubetten. Eine Sperre verhindert somit die Nutzung der Software insgesamt.

Erkennung und Entfernung von Spyware oft nur durch spezielle Software möglich

P3P stößt auch auf Kritik

Welchen Beitrag P3P (siehe Seite 20) zum Schutz der Privatsphäre leisten kann und wird, lässt sich noch nicht endgültig beantworten. KritikerInnen dieses technikzentrierten Konzepts der Selbstregulierung durch maschinenlesbare Veröffentlichung der Datenschutzpolitik verweisen auf die Gefahr, dass dadurch rechtliche Absicherungen der Privatsphäre weniger dringlich erscheinen und somit ausbleiben könnten. BefürworterInnen setzen auf den faktischen Druck, der von den gebotenen Möglichkeiten des P3P-Konzepts zur wirksamen realen Implementierung führen soll.

erste Beispiele von P3P demonstrieren enthaltenes Potential

Erste Realisierungen zeigen jedenfalls deutlich das Potential, das in dieser Technologie steckt. Der erste P3P-fähige Browser, Microsofts Internet Explorer in der Version 6, weist zwar bis auf den vereinfachten Zugang zu Informationen über die Datenschutzpolitik nur wenig herausragende Merkmale auf. Insbesondere die Cookie-Verwaltung lässt nur grobe Einstellungen zu und akzeptiert auch in der höchsten Sicherheitsstufe Cookies von Werberingen, wenn diese angeben, Daten nur unter dem Cookie zu speichern. Bei Verwendung eines P3P-fähigen Browser kann man aber Datenschutzeinstellungen von vertrauenswürdigen Stellen verwenden, die über das Internet bezogen und in die eigene Browsereinstellungen importiert werden. Eine Konfigurationsdatei[59] inklusive Anleitung, die das erwähnte Manko des Internet Explorers 6.0 beim Cookie-Management beseitigt, findet sich auf den Seiten des JAP-Projekts

---

[56] http://www.webwasher.com/

[57] http://www.bugnosis.org/

[58] http://lavasoft.de/

[59] http://anon.inf.tu-dresden.de/ie6_privacy.html

der Technischen Universität Dresden. Der Import dieser Einstellungen bewirkt, dass Cookies nur mehr für die jeweilige Sitzung akzeptiert, aber nicht gespeichert werden. Um persönlich angepasste Webseiten von vertrauenswürdigen Seiten weiterhin nutzen zu können, müssen diese eigens freigegeben werden. Ein anderes bereits verfügbares P3P-Tool, der PrivacyBird,[60] signalisiert dem Internetnutzer auf sehr einfache und intuitive Weise, ob eine besuchte Website überhaupt eine Datenschutzpolitik publiziert und ob sie gegebenenfalls mit den eigenen Präferenzen übereinstimmt.

Auswahl der passenden Werkzeuge schwierig

In diesem Bereich sind genügend Tools zum Schutz der Privatsphäre verfügbar. Für den durchschnittlichen Nutzer stellt sich eher das Problem, die seinen Bedürfnissen entsprechenden Tools zu finden und zu nutzen. Die dazu notwendigen Informationen sind zwar am Internet vorhanden, aber über viele Quellen verteilt und oft nicht am aktuellen Stand der Technik und der Diskussion. NutzerInnen ohne spezifische Vorkenntnisse laufen leicht Gefahr, sich angesichts der Unübersichtlichkeit zu verirren und auf an sich vorhandene Schutzmöglichkeiten zu verzichten.

3.3 Schlussfolgerungen

drei Säulen: gesetzliche Normen, freiwillige Selbstbeschränkungen und technische Vorkehrungen

Die Analyse einzelner Maßnahmen, durch die bewusste NutzerInnen ihre Privatsphäre schützen und bewahren können, zeigt, dass dies nur in dem Ausmaß gelingen kann, in dem auch die Säulen des Datenschutzes im Internet sich als tragfähig erweisen. Die drei wesentlichen Säulen, auf denen das Grundrecht auf Privatsphäre ruht sind durch den Staat vorgegebene gesetzliche Normen, freiwillige Selbstbeschränkungen der Industrie und technische Vorkehrungen zur Datensparsamkeit und gegen missbräuchliche Datensammlung bei den Anbietern und den NutzerInnen von Informationstechnologien. Jede dieser Säulen ist notwendig, keine für sich allein ausreichend, um das Grundrecht auf Privatsphäre auch im Informationszeitalter absichern zu können. Was für verantwortliche, der Risken bewusste KonsumentInnen gilt, ist für sorglose NutzerInnen umso wichtiger. Natürlich kann und soll niemand gezwungen werden, aus seinem Privatleben ein gut gehütetes Geheimnis zu machen, ebenso wenig darf aber Unkenntnis oder Sorglosigkeit zu einem Verlust von Grundrechten verbunden sein. Unwissenheit schützt nicht vor Strafe, darf aber auch nicht dazu führen, dass Rechtsverletzungen ungehindert und ungestraft möglich werden.

bewusste NutzerInnen zentrales Element, aber ...

Innerhalb der Wechselwirkungen zwischen dem Recht auf Privatsphäre jeder Einzelnen und den Säulen, auf denen es ruht, spielen die bewussten NutzerInnen eine zentrale Rolle. Dadurch, dass sie ihre Rechte wahrnehmen, tragen sie auch zur Stärkung von deren Basis bei. Indem sie auf ihre Rechte pochen, stärken sie sie; indem sie die Datenschutzpolitik der Anbieter bei ihren Konsumentscheidungen berücksichtigen, erhöhen sie die Bereitschaft zu datenschutzfreundlichen Selbstregulierungen; indem sie Privacy Enhancing Technologies für sich anwenden, fördern sie auch deren Weiterentwicklung und Verbreitung im Allgemeinen. Die Aufklärung und Schaffung von datenschutzbewussten KonsumentInnenen ist daher ein wesentliches Element einer umfassenden Strategie zur Wahrung des Grundrechts auf Privatsphäre, ohne aber dabei zu vergessen, dass gerade die unbedachten NutzerInnen eines besonderen Schutzes bedürfen.

... auch Schutz für unbedachte Personen notwendig

[60] http://www.privacybird.com

vorbildliche rechtliche Rahmenbedingungen gefährdet

Bei den einzelnen Elementen eines umfassenden Schutzes der Privatsphäre ist ein uneinheitliches Bild zu erkennen. Die regulativen Rahmenbedingungen, die im Wesentlichen durch die EU-Richtlinien 95/46[61] und 97/66[62] vorgegeben sind, gelten (noch) als weltweit vorbildhaft. Sie sind aber auch den Bestrebungen von Ermittlungsbehörden ausgesetzt, die sich durch den erleichterten Zugang zu Telekommunikationsdaten bessere Aufklärungs- und Präventionsmöglichkeiten erhoffen. Diese Bestrebungen haben durch die Terroranschläge vom 11. September 2001 wesentlich an Gewicht und politischer Durchsetzbarkeit gewonnen und sind in eine Reihe von internationalen und nationalen Gesetzesnovellierungen gemündet, die erweiterte Überwachungsbefugnisse und die Speicherung von Verkehrs- und Inhaltsdaten beinhalten. Jüngstes Ereignis in dieser Kette ist die Annahme der Richtlinie „über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation“ durch das Europaparlament am 30.5.2002. Diese Richtlinie wird die Richtlinie 97/66 ersetzen; in ihr werden derzeit noch geltende Verpflichtungen zur Löschung von Verbindungsdaten gelockert und die teilweise in einigen EU-Staaten bereits beschlossenen Verpflichtungen zur Speicherung durch die Telekommunikations- und Internetbetreiber auf europäischer Ebene legalisiert. Es bleibt abzuwarten, welche konkreten Auswirkungen die jüngsten Entwicklungen in einzelnen Staaten haben werden; die Weichen sind aber jedenfalls in Richtung gläserne BürgerInnen und KonsumentInnen gestellt.

mangelhafte Durchsetzungskraft gesetzlicher Regelungen

Zurzeit sind die größten Defizite noch bei der Transformation des durch die EU-Richtlinien angestrebten Schutzniveaus und dessen Durchsetzung durch nationale Gesetze zu beobachten. Ein krasses Beispiel hierfür ist etwa der sehr geringe Anteil an ECG-konformen Webshops in Österreich (siehe Seite 18). Maßnahmen, die diese Diskrepanz verringern sollen, bilden daher einen wesentlichen Teil der Empfehlungen im entsprechenden Abschnitt weiter unten. Sie betreffen gesetzliche Änderungen zur Stärkung und Erweiterung der Kompetenzen der Datenschutzbehörden, zur Erleichterung des Zugangs zum Recht für die KonsumentInnen sowie die Rücknahme oder Verhinderung von Reformen, die das Grundrecht beeinträchtigt haben bzw. schmälern würden.

Erweiterung bestehender Ansätze zur Selbstregulierung

Im Bereich der Selbstregulierung zielen die Vorschläge darauf ab, vorhandene Ansätze wie das e-Commerce-Gütesiegels zu verstärken und zu erweitern. Dazu gehört etwa eine forcierte Verankerung des österreichischen e-Commerce-Gütesiegels auf EU-Ebene und die Integration zusätzlicher Aspekte – etwa maschinenlesbare Datenschutzpolitiken gemäß P3P oder der Verzicht auf die Datengewinnung durch Cookies –, um es auch als Datenschutzsiegel etablieren zu können.

verbesserter Zugang zu PETs und Integration auf Seiten der Anbieter

Im Bereich Datenschutz durch Technik sind zwei Maßnahmenbündel notwendig. Das erste Paket muss darauf abzielen, den KonsumentInnen den Zugang zu diesen Technologien zu erleichtern, indem sie sich etwa an eine vertrauenswürdige Stelle bspw. einen Datenschutz-Ombudsmann wenden können, um aktuelle Hilfestellungen zu erhalten. Die zweite Stoßrichtung zielt darauf ab, Datensparsamkeit an der Quelle, d. h. bei den Betreibern von Internetdiensten durch Technikeinsatz zu fördern.

„Surfen kann Ihre Privatsphäre gefährden!“

Als übergreifende Maßnahme zur Bewusstseinsschaffung bieten sich Warnhinweise an, die an geeigneter Stelle – etwa Rechnungen von Telekom- und Internetprovidern – zu platzieren sind und dem Konsumenten zugleich Zugangsmöglichkeiten für weitere Informationen eröffnen.

---

[61] Europäisches Parlament und der Rat 1995.

[62] Europäisches Parlament und der Rat 1997.

Übersicht: Einschätzung der Durchführbarkeit und Wirksamkeit individueller Maßnahmen

Maßnahme	Durchführbarkeit/ erforderliche Kenntnisse	Verfügbarkeit	Wirksamkeit	Nachteile	Kommentar	Link(s)/weitere Informationen*
AGBs nach Datenschutzaspekten vergleichen	von unmöglich (da nicht vorhanden) bis sehr einfach (Gütesiegel oder P3P)	insgesamt relativ gering (höherer Anteil bei großen Anbietern)	bei konsequenter Befolgung gut	teilweise zeitaufwändig; stark eingeschränktes Angebot	Gütesiegel teilweise wenig aussagekräftig in Hinblick auf konkrete Datenschutzpolitik	http://www.akwien.at/inet.html http://www.guetezeichen.at/ http://www.ombudsmann.at/ http://www.w3.org/P3P/
Zurückhaltung bei Preisgabe von Daten	sehr einfach	bis auf Bezahldienste praktisch immer möglich	gut, sofern nicht durch Spyware unterlaufen	einige Kategorien von Angeboten nicht nutzbar (z. B. Gewinnspiele oder Bezahldienste)	Pseudonyme verwenden, wenn die Angabe persönlicher Daten zur Bedingung gemacht wird	http://cookie.inf.tu-dresden.de/index_de.html http://www.privacybird.com/
Andere Identitäten und anonyme e-Mail-Adressen verwenden	einfach	bis auf Bezahldienste praktisch immer durchführbar	gut, sofern nicht durch Spyware Verknüpfung mit wahrer Identität erfolgt	zusätzlicher Zeitaufwand für die Generierung und Verwaltung mehrerer Identitäten	lässt sich auch für personalisierte Dienste und Trennung von Lebenssphären nutzen	http://cookie.inf.tu-dresden.de/index_de.html http://www.paysafecard.com/at/de/
Beiträge aus Newsgroup-Archiv entfernen und Archivierung blockieren	erfordert erweiterte Grundkenntnisse	nicht immer möglich; Zugang teilweise schwer zu finden	gut	aufwändig	besser von vornherein grundsätzlich Pseudonyme zu verwenden	http://groups.google.com/
Verschlüsselungssoftware nutzen	erfordert gute PC-Kenntnisse und eingehende Beschäftigung	noch gut (PGP), aber zukünftige Entwicklung offen	sehr gut, wenn Kenntnisse und Kommunikationspartner vorhanden	mangels Verbreitung kaum für Kommunikationszwecke einsetzbar	derzeit nur für Kommunikation innerhalb geschlossener Gruppen sinnvoll	http://www.pgpi.org/ http://www.gnupp.de/start.html
Anonyme Mail- und Webdienste nutzen	zumindest erweiterte Grundkenntnisse erforderlich	abhängig von den Kenntnissen: für normale NutzerInnen nur geringes Angebot	auch abhängig von den Kenntnissen	eingeschränkte Funktionalität und Zugänglichkeit, zeitaufwändig	Vertrauenswürdigkeit der Anbieter kaum zu beurteilen	http://www.allgemeiner-datenschutz.de/portal/portal.htm http://anon.inf.tu-dresden.de/index.html
Spezialisierte Softwarepakete zum Schutz der Privatsphäre einsetzen	erweiterte Grundkenntnisse erforderlich	sehr großes Angebot, aber oft nur veraltete Versionen	gut bei entsprechenden Kenntnissen und Konfiguration	Auswahl der Software schwierig, Kompatibilitätsprobleme möglich	praktisch einzige Möglichkeit, gegen Spyware vorzugehen	http://cookie.inf.tu-dresden.de/index_de.html http://www.lavasoft.de/ http://www.epic.org/privacy/tools.html http://www.zonealarm.de/

* *Die angegebenen Links sind als Beispiele zu verstehen. Aufgrund der häufigen Änderungen in den Angeboten empfiehlt es ich, auf allgemeine Suchmaschinen oder themenspezifische Linklisten* (z.B. http://www.oeaw.ac.at/ita/privacylinks.htm) *zurückzugreifen.*

4 Datenanalyse und Data Mining

Aufdeckung verborgener Beziehungen

Im Kapitel „Private Internetnutzung“ wurden die vielfältigen Möglichkeiten der Datensammlung über das Medium Internet aufgezeigt und die Wirksamkeit von individuellen Gegenmaßnahmen analysiert. In diesem Abschnitt wird ein weiteres Gefährdungspotential neuer Informationstechnologien für die Privatsphäre diskutiert. Die hier besprochenen Technologien zielen darauf ab, vorhandene Daten besser auswerten und nutzen zu können. Neue Methoden der Datenanalyse sollen in sprachlicher Analogie zur Rohstoffgewinnung im Bergbau verborgene Schätze in den Daten heben und ausschöpfen lassen. Anwendungen von Data Mining Techniken versuchen, auf möglichst alle verfügbaren Daten zuzugreifen und auf unbekannte Beziehungen hin zu analysieren. Sie beschränken sich daher nicht auf die Daten aktueller oder potentieller Kunden, die aus traditionellen oder elektronischen Transaktionen stammen bzw. zugekauft werden können, sondern versuchen generell Daten, die bei den betrieblichen Prozessen generiert werden einzubeziehen. Und die Optimierung der Kundenbeziehungen durch das Customer Relationship Management (CRM) ist zwar eine wichtige Anwendung, aber eben nur einer von vielen Prozessen, der durch Datenanalysen effizienter gestaltet werden soll. Sofern sich das Data Mining auf betriebliche Daten und Prozesse beschränkt, lässt sich dagegen aus datenschutzrechtlicher Perspektive kaum etwas einwenden.

möglichst umfassende Datenbasis

Widerspruch zu Datenschutzprinzipien

Sobald aber Daten mit Personenbezug ins Spiel gebracht werden, wird eine Reihe von problematischen Konstellationen sichtbar. Allein die Vorratshaltung von Daten für zukünftige Auswertungen mit unbekannten Zielen widerspricht gängigen Standards datenschutzgerechten Verhaltens. Ebenso lassen sich die Prinzipien der Zweckbindung und daran geknüpfte Einwilligungen zur Verarbeitung personenbezogener Daten durch die prinzipielle Unbestimmtheit der Ergebnisse von Data Mining Verfahren, und der damit verbundenen unabsehbaren Einsatzmöglichkeiten der Resultate, nur als Generalvollmachten betrachten. Die Grenzen unternehmensinterner Auswertungen lassen sich aus mehreren Gründen nicht genau bestimmen, wobei der Zukauf von Daten nur eine Problemlage darstellt. Weitere Abgrenzungsprobleme und Missbrauchspotentiale entstehen durch Auslagerung von Aktivitäten, etwa durch das Outsourcing von Data Mining Prozessen selbst, oder aber durch Call Centers, die die Kundenbetreuung für mehrere Unternehmen durchführen und so zu entsprechend umfangreichen Datenbeständen Zugriff erlangen.

Missbrauchsgefahr durch Outsourcing

Nutzung externer Daten bedenklich

Während die Analyse der Daten, die ein Unternehmen aus den Transaktionen mit den eigenen KundenInnen extrahiert, wohl nicht zu verhindern sein wird; und je nach Empfinden und Politik des Unternehmens von den KonsumentInnen als bessere Betreuung oder aber als Belästigung durch Werbeaktionen angesehen werden kann, ist die Einbeziehung externer Daten aus Sicht des Datenschutzes jedenfalls eine bedenkliche Praxis.

4.1 Was ist Data Mining

Entdecken von Mustern und Regeln

„Data Mining bezeichnet Techniken zum Finden von interessanten und nützlichen Mustern und Regeln in großen Datenbanken“ (Petrak 1997). Ein wesentliches Kriterium des Data Mining ist es, dass unterschiedliche Verfahren eingesetzt werden, um Beziehungen innerhalb der Daten zu entdecken, deren Existenz von vornherein nicht bekannt ist. Im Unterschied zu klassischen sta-

tistischen Verfahren, bei denen Hypothesen anhand des Datenmaterials überprüft werden, steht die Generierung von neuen Hypothesen im Vordergrund. Bei Anwendungen des Data Mining in der Praxis werden zumeist beide Aspekte eine Rolle spielen, d. h. sowohl die Überprüfung vermuteter Beziehungen aufgrund von Erfahrungen und Vorwissen als auch die Generierung neuen Wissens.

Die durch Data Mining gewonnenen Informationen lassen sich üblicherweise den folgenden Typen zuordnen: Assoziationen, Sequenzen, Klassifikationen, Cluster und Prognosen (Cavoukian 1998).

reichliches Anwendungspotential in Unternehmen

Ein typisches Beispiel für Assoziationen ist die Analyse von Warenkörben, d. h. z. B. die Bestimmung der Häufigkeit, mit der unterschiedliche Produkte oder Produktgruppen gemeinsam gekauft werden. Bei den Sequenzen stehen Regelmäßigkeiten im zeitlichen Ablauf im Vordergrund, etwa die Anschaffung von Haushaltsgeräten nach dem Bezug einer neuen Wohnung. Klassifikationsregeln dienen dazu, neue Objekte aufgrund der Eigenschaften bestehender Objekte Klassen zuteilen zu können; z. B. zuordnen von Neukunden zu unterschiedlichen Klassen der Kreditwürdigkeit auf Basis der Analyse der bestehenden Kundendatei. Beim Clustering wird im Unterschied zur Klassifikation nicht von Klasseneinteilungen ausgegangen, sondern aufgrund der Eigenschaften der Objekte werden Gruppen gebildet. Zusätzlich wird versucht, verständliche und verwertbare Beschreibungen der Gruppen und Klassifikationsregeln zu finden. Ein mögliches Ergebnis könnten beispielsweise Kundengruppen mit besonders hoher Neigung zum Anbieterwechsel sein, für die dann spezifische Kundenbindungsprogramme entwickelt werden. Prognosen stellen weniger eine eigene Kategorie von gewonnenen Informationen dar, als vielmehr eine zukunftsgerichtete Art der Datenauswertung.

Vorhersage und Steuerung des Kundenverhaltens

Der Vielfalt der Verfahren und der Art der erhobenen Daten entsprechend, sind auch die Ergebnisse und Einsatzgebiete des Data Mining mannigfaltig. Sie reichen von Mustern im KonsumentInnenverhalten, Assoziationen zwischen demographischen oder regionalen Charakteristika von KonsumentInnen, Vorhersagen über Reaktionen auf Werbekampagnen über die Identifikation von besonders loyalen oder ausgabefreudigen KonsumentInnen bis hin zur Entdeckung von KonsumentInnen, die höhere Kosten verursachen können, weil sie etwa Dienste wahrscheinlich besonders häufig in Anspruch nehmen werden, oder weil sie ein höheres Risiko von Zahlungsunfähigkeit oder betrügerischen Verhaltens aufweisen. Das Wissen über die Kunden dient nicht nur dazu, deren Bedürfnissen entgegenzukommen, sondern es wird natürlich auch dazu genutzt, deren Verhalten im Sinne des Unternehmens zu steuern.

4.2 Vor- und nachgelagerte Prozesse

Datenspeicherung in Data Warehouses

Voraussetzung für die Anwendung von Data Mining Techniken ist natürlich, dass der Rohstoff „Daten“ in möglichst umfassender Weise vorhanden ist. Die Zusammenführung aller nutzbaren Daten in einem vereinheitlichten Datenpool wird als „Data Warehousing“ bezeichnet. Im Data Warehouse werden die Daten losgelöst von ihrer ursprünglichen Verwendung gespeichert und für Data Mining Analysen zugänglich gemacht. Das Data Warehousing umfasst drei Aufgaben: die zentrale Sammlung der in den einzelnen Abteilungen eines Unternehmens verarbeiteten und gespeicherten Daten, die Überführung dieser Daten in ein einheitliches Format und die Bereinigung der Daten von eventuellen Fehlern und Inkonsistenzen. Die Integration der Daten in einem Data

Warehouse ermöglicht auch die unternehmensweite Anwendung konventioneller Analyseverfahren[63] und unterstützt den Einsatz von Wissensmanagement-Software.

Nutzung zur Gestaltung der Kundenbeziehungen

Die durch Data Mining gewonnenen Informationen lassen sich in vielfältiger Weise zur Optimierung interner unternehmerischer Prozesse und externer Beziehungen nutzen. In unserem Zusammenhang ist die Verwertung der extrahierten Informationen im Rahmen des Customer Relationship Management (CRM) relevant. Wie bei vielen neuen Konzepten herrscht auch bei CRM eine Vielfalt an Definitionen. Im Allgemeinen wird unter Kundenbeziehungsmanagement ein umfassendes Unternehmenskonzept verstanden, welches unter Einbeziehung von Informationstechnologien alle kundenbezogenen Prozesse integriert und optimiert. Ein wesentliches Unterscheidungsmerkmal der einzelnen Definitionsversuche ist die Dominanz von Kundenzufriedenheit oder der Unternehmensprofitabilität bei den Zielen des CRM. In den meisten Fällen wird zwar die Kongruenz der beiden Ziele betont, die Profitabilität lässt sich aber auch durch die negative Selektion von wenig kaufkräftigen oder risikobehafteten Kundengruppen erhöhen. Da gerade für Unternehmen, die gewissermaßen Basisdienste moderner Gesellschaften anbieten – z. B. Telekommunikationsanbieter, Banken oder Versicherungen –, der Einsatz von Data Mining und CRM besonders profitabel ist, wird durch diese Instrumente auch die universelle Versorgung mit Infrastrukturleistungen und der solidarische Risikoausgleich gefährdet.

globaler Austausch standardisierter Kundenprofile

Es gibt eine Reihe von Bereichen,[64] in denen besonders viele Kundendaten anfallen. Diese Sektoren weisen daher ein entsprechend hohes Potential auf, die Daten im eigenen Interesse auszuwerten oder diese an andere Parteien weiterzugeben bzw. zu veräußern. Um den globalen Austausch von Kundenprofilen zu vereinfachen, wurde von einigen großen Unternehmen ein offener Standard spezifiziert. Der CPEX-Standard (Customer Profile Exchange)[65] ermöglicht zwar analog zur P3P die Berücksichtigung von individuellen oder nationalen Vorgaben zum Schutz der Privatsphäre, stößt aber wegen der grundlegenden Zielsetzung und der Effekte auf Kritik von Datenschutzorganisationen. Der globale Austausch von Kundenprofilen widerspricht dem Prinzip der Zweckbindung bzw. droht diese zu unterlaufen. Er verhindert jede Möglichkeit für KonsumentInnen, Übersicht darüber zu wahren, wo und bei wem welche Daten gespeichert und verarbeitet werden, gleichzeitig bedeuten mehr Daten, dass präzisere und aussagekräftigere Profile erstellt werden können.

---

[63] Darunter werden unter dem Akronym OLAP (Online Analytical Processing) firmierende Verfahren verstanden, die im Gegensatz zum Data Mining Antworten auf gezielte Fragen geben.

[64] Eckhardt et al. 2000 zählen folgende Bereiche zu den prädestinierten Data Mining Anwendern: Banken und Kreditkartenorganisationen, Call Center, Handel, Internet-Dienstleistungen, Web-Agenten, Reiseveranstalter, Telekommunikation, Versicherungen, Bibliotheken, Pay-TV, Gesundheitswesen, Verwaltung und Aggregatoren.

[65] Nähere Informationen dazu finden sich auf http://www.cpexchange.org/

4.3 Data Mining und Datenschutz

fehlende Zweckbindung

Ein zentrales Problem dieser Technologien aus datenschutzrechtlicher Sicht ist die fehlende Zweckbindung der Verarbeitung, die ein konstituierendes Merkmal des Data Mining ist. Gemäß der Datenschutzrichtlinie der Europäischen Union (DS-RL)[66] ist die Verarbeitung personenbezogener Daten mit wenigen, für das Data Mining durch private Unternehmen nicht zutreffenden Ausnahmen an die zweifelsfreie Einwilligung der betroffenen Person geknüpft. Diese Richtlinie besagt auch, dass personenbezogene Daten nur für festgelegte eindeutige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Eine Frage, die sich stellt, ist, ob die Aufdeckung von verborgenen und unbekannten Beziehungen ein eindeutiger Zweck sein kann, und ob daher allfällige Zustimmungen von KonsumentInnen zur Analyse ihrer Daten im Rahmen von Data Mining Prozeduren überhaupt rechtlich wirksam sein können. Rechtskommentare und Entschließungen von Datenschutzbeauftragten sprechen dagegen (Entschließung der Konferenz der Datenschutzbeauftragten 2000), welche Konsequenzen daraus im Einzelfall zu ziehen wären, bleibt aber offen. Während Data Mining unter Einbeziehung persönlicher Daten generell bedenklich scheint, lässt sich eine eventuelle Rechtswidrigkeit nur in konkreten Einzelfall konstatieren. Neben den unterschiedlichen Konstellationen, unter denen Data Mining eingesetzt werden kann, machen divergierende Rechtsauffassungen und fehlenden höchstgerichtliche Entscheidungen eine allgemeingültige Beurteilung unmöglich.

Zustimmung rechtlich wirksam?

Weiterverarbeitung zu „Sekundärzwecken" eingeschränkt zulässig

So lässt Art. 6 der DS-RL die Weiterverarbeitung zu „Sekundärzwecken" zu, solange diese nicht mit dem Primärzweck unvereinbar sind. Data Mining wird in vielen Fällen mit den Daten ausgeführt, denen ein zulässiger Primärzweck zugrunde liegt (wie Kundendaten, Arbeitnehmerdaten, etc.). An „Sekundärzwecke" werden auf den ersten Blick über die „Vereinbarkeit mit dem Primärzweck" hinaus keine weiteren Anforderungen gestellt. Dies dürfte der Grund sein, weshalb der österreichische Gesetzgeber in seinem weitem Begriffsverständnis innerbetriebliche Verarbeitungen wie Rechnungswesen und Controlling sowie – eindeutig ungewiss und zukunftsorientiert – Analyse und Planung mit dem Primärzweck für vereinbar hält. Bei der Frage, inwieweit die Verwendung von Kundendaten für das eigene Marketing noch einen zulässigen Sekundärzweck darstellt, scheiden sich die Geister. Hier spricht auch die oft anzutreffende Praxis von Unternehmen, sich dafür nämlich eine ausdrückliche Zustimmung einzuholen, dafür, dass es sich hierbei um einen Grenzfall handelt. Würde es sich dabei um eine eindeutig mit dem Primärzweck vereinbare Verarbeitung handeln, wäre das Einholen des Einverständnisses überflüssig.

anonymisierte Auswertung generell erlaubt

Sofern Data Mining an bestimmte Zwecke gebunden durchgeführt wird, lässt sich im Einzelfall eine Beurteilung der Datenschutzkonformität durchführen. So sind nach Art. 6 DS-RLVerarbeitungen zu historischen, statistischen und wissenschaftlichen Zwecken im Allgemeinen mit dem Primärzweck vereinbar, „geeignete Garantien" der Mitgliedstaaten vorausgesetzt (im Sinne eines gleichwertigen Schutzes wie bei der eigentlich notwendigen Löschung). Diese Privilegierung erfolgte aber offensichtlich vor dem Hintergrund nicht-personenbezogener Verarbeitung. Rückt man für eine erste Beurteilung Data-Mining in die Nähe der Statistik, scheidet personenbezogenes Data-Mining daher als zulässiger Sekundärzweck jedenfalls aus. Auch das Begriffsverständnis des österreichischen Gesetzgebers ist auf zumindest pseudonymisierte Daten einzuschränken.

---

[66] Europäisches Parlament und der Rat 1995.

personenbezogenes Data Mining rechtlich bedenklich

Eine zentrale Streitfrage ist, ob Data Mining auch bei personenbezogener Verarbeitung ein zulässiger Sekundärzweck sein kann. Gemäß der DS-RL müssen die Zwecke eindeutig und rechtmäßig sein und bei der Datenerhebung festgelegt werden. Die Begründung zu Art. 6 DS-RL fordert ausdrücklich, dass eine allgemeine oder vage Definition oder Beschreibung des Gegenstandes der Verarbeitung wie z. B. „für kommerzielle Zwecke" nicht reicht. Die Grenzen zwischen traditionellen Verfahren der Datenanalyse und dem Data Mining sind oft nicht klar zu setzen, es bleibt aber ein konstituierendes Merkmal von Data Mining, dass nach unbekannten Beziehungen geschürft wird, und der Zweck sowie mögliche Verwendungen der Resultate somit unbestimmt sind. In diesem Zusammenhang meinten die deutschen Datenschutzbeauftragten zuletzt, dass eine Zweckänderung nur mit Einwilligung des Betroffenen zulässig, und eine Einwilligung in unbestimmte und zeitlich unbegrenzte Zweckänderungen unwirksam sei (Entschließung der Konferenz der Datenschutzbeauftragten 2000). Angesichts dieser Rechtsposition ist eine juristisch haltbare Formulierung des Zweckes von Data Mining unter Nutzung personenbezogener Daten schwer vorstellbar.

rechtsgültige Einwilligung kaum möglich

Dementsprechend ist aufgrund der genannten Schwierigkeit der Bestimmung des Zweckes auch eine rechtsgültige Einwilligung in Data Mining kaum möglich. Ebenso wenig kann eine betroffene Person durch eine Einwilligung die Zweckbindung überhaupt außer Kraft setzen. Die Zweckbindung selbst ist nicht „dispositiv" und in das Belieben der Vertragspartner gestellt. Zwar erlaubt die Privatautonomie auch Verträge über noch nicht Vorhersehbares, allerdings schreibt hier Art. 2 lit h DS-RL ganz klar vor, dass die Einwilligung *„... für den konkreten Fall ..."* zu erfolgen hat. Und dieser konkrete Fall stützt sich auf die Umschreibung des konkreten Zweckes der Verarbeitung.

besondere Regeln für Werbewirtschaft

Die Data-Mining- und CRM-Problematik spielt auch in Zusammenhang mit der „Direktwerbung" und Opt-Out-Regelung des Art. 14 b der DS-RL eine Rolle. Grundsätzlich muss jede Verarbeitung die beiden Hürden des Art. 6 und Art. 7 der Richtlinie überwinden. Werbung/Marketing mit eigenen internen Kundendaten wird beispielsweise mit dem eigentlichen Zweck der Verarbeitung (Abwicklung eines Kaufvertrages etc.) regelmäßig vereinbar sein. Die Hürde des Art. 6 scheint damit genommen, die Vereinbarkeit an sich kann aber bereits diskutiert werden. Bleibt Art. 7. Liegt keine Einwilligung vor, wird Direktwerbung im Ausgangspunkt als berechtigtes Interesse der Wirtschaftstreibenden im Sinne des Art. 7 lit f anzusehen sein. Auch die Weitergabe solcher Direktwerbedaten wird in Erwägungsgrund (30) der DS-RL als ein Interesse effektiven Wettbewerbs erwähnt. Zwar schreibt die DS-RL die Berücksichtigung überwiegender Interessen des Betroffenen vor, gibt dafür aber keine konkreten Anhaltspunkte. Für ein Mitverwenden externer Daten scheint bei rechtmäßiger Datenverarbeitung aber generell kein Raum gegeben.

Widerspruchsmöglichkeit muss eingeräumt werden

Selbst wenn man von der Zulässigkeit der Verarbeitung auch nach Art. 7 ausgeht, zieht Art. 14 doch die Grenze zulässiger Direktwerbung. Einerseits kann der Betroffene gegen die beabsichtigte (somit noch nicht erfolgte!) Verarbeitung Widerspruch einlegen. Oder er ist – vor der ersten Weitergabe seiner Daten oder vor erstmaliger Nutzung – zu informieren und ausdrücklich auf sein Recht hinzuweisen, gegen eine solche Weitergabe (somit wiederum noch bevor irgendwie geworben wurde) oder Nutzung (gemeint erstmalige Nutzung) Widerspruch einlegen zu können.

in Österreich in Gewerbeordnung geregelt

Bei der konkreten Umsetzung lässt die DS-RL den Mitgliedstaaten einigen Spielraum offen. Im österreichischen DSG sucht man die Umsetzung der Direktwerbungsvorschriften der DS-RL vergeblich. Fündig wird man im § 151 der jüngst novellierten Gewerbeordnung (GewO). Aus den jeweiligen Kunden- und Interessenkarteien dürfen gem. § 151 Abs. 5 GewO nur Namen, Ge-

schlecht, Titel, akademischer Grad, Anschrift, Geburtsdatum, Berufs-, Branchen- oder Geschäftsbezeichnung und die Zugehörigkeit des Betroffenen zu dieser Kunden- und Interessenkartei an den Adressenverlag oder das Direktwerbeunternehmen ermittelt werden. Gegenüber der vorhergehenden Fassung ist diese Liste um die Kategorie Geschlecht erweitert und das Geburtsjahr durch das Geburtsdatum ersetzt worden. Durch das exakte Geburtsdatum wird eine genauere Personalisierung ermöglicht und ein Abgleich mit anderen Registern vereinfacht.

Marketinganalyse-verfahren nur für Marketingzwecke erlaubt

In der Neufassung werden auch Data-Mining-Verfahren erstmals direkt angesprochen: lt. Abs. 6 dürfen für Marketingzwecke erhobene Marketinginformationen und -klassifikationen, die namentlich bestimmten Personen auf Grund von Marketinganalyseverfahren zugeschrieben werden, nur für Marketingzwecke verwendet oder an Dritte übermittelt werden. In Österreich ist bei Direktwerbung generell ein Opt-Out-Prinzip verwirklicht (Robinson-Liste etc.). Im Fall der in § 151 Abs. 4 GewO genannten sensiblen Daten ist aber eine ausdrückliche schriftliche Zustimmung erforderlich, somit „Opt-In" für die Verwendung sensibler Daten. Darüber hinaus beschränkt Abs. 4 auch den Umfang der erlaubten Ermittlung und Weiterverwendung sensibler Daten.

Datenschutz wird durch Konsumentenschutz unterstützt

In Zusammenhang mit der Frage, ob eine Zustimmung des Kunden zum Data Mining überhaupt konkret genug sein kann, wird auch der Konsumentenschutz (konkret § 6 Abs. 3 KSchG) eine wichtige Rolle spielen. So hat der OGH in der „Friends of Merkur"-Entscheidung vom 27.1.1999 (7 Ob 170/98) ausgesprochen, dass für den Kunden etwa die Bezeichnung „BWL-Konzern" schon aufgrund der sich ändernden Zusammensetzung von Konzernen nicht verständlich genug sei. Es müsse für den Kunden deutlich erkennbar sein, an wen die mittels Kundenkarte erhobenen Daten weitergeleitet würden. Ähnliches hat wohl für unkalkulierbare Zweckbindungen zu gelten. Der Konsumentenschutz kann also gerade im Zusammenhang mit nebulösen Einverständniserklärungen dem Datenschutz zum Durchbruch verhelfen.

Datenbevorratung allein ist bedenklich

Die datenschutzrechtliche Bedenklichkeit beginnt aber nicht erst mit der Analyse personenbezogener Daten durch Data Mining-Verfahren oder der Nutzung der dabei gewonnenen Informationen, sondern sie betrifft auch vorgelagerte Prozeduren der Datensammlung und Bevorratung. Die Rechtmäßigkeit der Vorratshaltung von Daten in Warehouses wird als präventive Datensammlungen in Hinblick auf künftige noch nicht feststehende Aktivitäten ebenso verneint, wie jene von Datendepots, die sich jederzeit für neue Ziele reaktivieren lassen.

Prinzip der Zweckbindung wird verletzt

Schließlich weisen auch die deutschen Datenschutzbeauftragten auf Gefahren und Risiken des Data Warehousing hin. Die Speicherung in allgemein verwendbaren Data Warehouses entferne sich vom ursprünglichen Verwendungszweck und stelle eine Speicherung auf Vorrat ohne Zweckbindung dar. Allerdings meinen sie auch, dass anonyme und pseudonyme Verfahren datenschutzrechtlich unbedenklich seien. Die permanente Speicherung in Daten-Lagerhäusern sei aber rechtswidrig in Hinblick auf gesetzliche Speicherfristen.

Verwendung der Ergebnisse entscheidend

Inwiefern eine anonyme oder pseudonyme Durchführung von Data Mining Prozessen unbedenklich ist, lässt sich nur in Zusammenhang mit der Verwendung der Resultate beantworten. So wird etwa gegen eine anonyme Analyse der Kreditwürdigkeit nach demographischen Kriterien kaum etwas einzuwenden sein. In der Regel wird der Zweck solcher Untersuchungen wohl sein, diese Informationen in konkrete Einzelentscheidungen des Customer Relation Managements einfließen zu lassen. Es mag in einzelnen Fällen durchaus zutreffen, dass derartige Verfahren beim angesprochenen Beispiel von Kreditvergaben zu einer „Objektivierung" im Vergleich zu subjektiven Beurteilungen des Kreditwerbers auf Basis persönlicher Gespräche beitragen können. Dennoch sind zwei grundsätzliche Einwände gegen diese Praxis vorzubringen.

Benachteiligungen aufgrund automatisierter Einzelentscheidungen verboten

Gemäß Artikel 15 DS-RL[67] sind Benachteiligungen aufgrund automatisierter Einzelentscheidungen nicht zulässig. Von den deutschen Datenschutzbeauftragten wird Data Mining als mögliches Instrument von Art. 15-Entscheidungen eingestuft. Dabei sind abstrakte und spezifische Personenprofile zu unterscheiden. Bei spezifischen Profilen ist Art. 15 jedenfalls zu beachten. Interessant ist auch Art. 15 Abs. 2 DS-RL und seine nationale Umsetzung. In Österreich wäre ein Data Mining im Falle eines Kreditantrages und seiner Stattgebung durch das betreffende Bankinstitut zulässig, selbst wenn dies mit diskriminierenden Folgen im Sinne von schlechteren Bedingungen aufgrund einer vollautomatisierten Beurteilung verbunden wäre. Die Ausnahmebestimmung des § 49 Abs. 2 lit 2 DSG 2000 scheint dies zuzulassen. Das grundsätzliche Verbot greift nur, wenn die betroffene Person keinen Kredit erhält. In jedem Fall aber steht gemäß § 49 Abs. 3 DSG 2000 ein Auskunftsrecht über den logischen Ablauf der Entscheidungsfindung zu.

Datenqualität nicht gewährleistet

Der zweite Einwand betrifft die Vermengung von auf Fakten beruhenden Daten mit Resultaten von Datenanalyseverfahren. Die Ergebnisse des Data Mining sind als statistische Zusammenhänge für eine Gruppe geltende Aussagen, für einzelne Individuen sind sie Wahrscheinlichkeitsaussagen, dass bestimmte Eigenschaften zutreffen könnten. Durch die Zusammenfassung der beiden Arten von Daten in persönlichen Profilen wird damit ein weiteres Prinzip der datenschutzkonformen Gestaltung von Datenverarbeitungen gebrochen, nämlich dem Prinzip der Datenqualität. Als eines von acht von der OECD entwickelten Prinzipien[68] (OECD 1980) besagt es, dass Daten genau, vollständig und aktuell sein müssen. Es ist aber durchaus anzunehmen, dass Beurteilungen aufgrund statistischer Verfahren in die Persönlichkeitsprofile direkt einfließen und mit diesen längerfristig verhaftet bleiben.

4.4 Schlussfolgerungen

wenig Bewusstsein über Data Mining

Die einzelne KonsumentIn kann kaum wissen und umso weniger beeinflussen, inwieweit ihre Daten in Data Mining Prozessen erfasst und verarbeitet werden. Damit sind auch der individuellen Verantwortlichkeit enge Grenzen gesetzt. Data Mining findet im Verborgenen statt und entzieht sich weitgehend der Kenntnis und dem Bewusstsein der Betroffenen. Als aufgeklärte KonsumentIn muss man davon ausgehen, dass die meisten größeren Unternehmen, mit denen man in geschäftlichen Kontakt tritt, Data Mining betreiben. Eine bestehende Geschäftsbeziehung ist aber keine notwendige Bedingung, um von Datenanalysen erfasst zu werden. Im Gegenteil ist anzunehmen, dass die Daten professioneller Anbieter vielfach bei gezielten Werbeaktionen, bei der Selektion potentieller Neukunden oder der individuellen Angebotserstellung und Preisgestaltung herangezogen werden. „Profilhändler sind mittlerweile in der Lage, ganz spezifische Persönlichkeitsprofile zu liefern. Hierfür werden

[67] Die Mitgliedstaaten räumen jeder Person das Recht ein, keiner für sie rechtliche Folgen nach sich ziehenden und keiner sie erheblich beeinträchtigenden Entscheidung unterworfen zu werden, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht, wie beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens. Ibid.

[68] Diese auch unter dem Begriff „fair information practices" bekannten Regeln betreffen folgende Bereiche: (1) Collection Limitation; (2) Data Quality; (3) Purpose Specification; (4) Use Limitation; (5) Security Safeguards; (6) Openness; (7) Individual Participation; and, (8) Accountability.

hochsensitive Daten aus der privaten Lebenssphäre erfasst, mit vielfältigen öffentlich zugänglichen Daten kombiniert und für Marketing- und andere Zwecke weiterverkauft oder zum Leasing angeboten“ (Roßnagel et al. 2001, 24).

wenig direkte Einflussmöglichkeiten

Angesichts der nur sehr geringen Einflussmöglichkeiten einzelner KonsumentInnen auf die Art und Weise, in welcher mit ihren Daten in Unternehmen verfahren wird, lassen sich dementsprechend wenige konkrete Empfehlungen für KonsumentInnen formulieren. So mündet ein ausführlicher Bericht der kanadischen Datenschutzkommission über das Thema Data Mining in zwei Ratschlägen für KonsumentInnen; der erste zielt darauf ab, bei Unternehmenskontakten aktiv nach der Datenschutzpolitik zu fragen bzw. auf die Respektierung seiner Vorgaben zu pochen, der zweite Vorschlag lautet, nur die für die jeweilige Transaktion mindestens erforderlichen Daten bekannt zu geben (Cavoukian 1998). Die Empfehlungen setzen auf den Einfluss bewussten Konsumentenverhalten, indem etwa Daten nur sparsam freigegeben werden oder durch Einbeziehung des Datenschutzverhaltens bei den Konsumentscheidungen entsprechende Anreize für konformes Verhalten von Unternehmen geboten werden.

neue Gefahren durch Unternehmenskonzentrationen und Outsourcing

Wie bei Datensammlungen im Allgemeinen besteht auch bei Data Mining ein großes Gefahrenpotential darin, dass bei entsprechender Datenbasis sehr umfassende Persönlichkeitsprofile erstellt werden können. Der Umfang der Datenbasis ist durch eine zeitliche Dimension und die Menge an Beobachtungen determiniert. Die zeitliche Dimension lässt sich durch ein Verbot längerfristiger Speicherung personenbezogener Daten einschränken. Die Menge an Daten, die Data Mining Analysen zugeführt werden kann, hängt einerseits von den Möglichkeiten ab, auf Fremddaten zuzugreifen, andererseits vom Umfang der Geschäftstätigkeit des betroffenen Unternehmens. Kritische Bereiche sind hier etwa Telekommunikationsunternehmen; insbesondere wenn traditionelle Telekommunikation, Mobilkommunikations- und Internetdienste von einem Unternehmen bezogen werden, sind reale Gefahren des gläsernen Menschen nicht von der Hand zu weisen. Ein weiterer kritischer Bereich entsteht bei der Auslagerung von Geschäftsprozessen in externe Unternehmen. Ein prominentes Beispiel ist hierfür die Kundenbetreuung durch Call Centers. Da hier Kunden unterschiedlicher Unternehmen auf ein und derselben technischen Infrastruktur betreut werden, ist rechtlich und organisatorisch dafür Sorge zu tragen, dass keine unternehmensübergreifenden Datenauswertungen stattfinden können. Analoge Vorkehrungen werden im öffentlichen Bereich zu treffen sein, wenn im Rahmen von e-Government-Initiativen One-Stop-Zugangsmöglichkeiten zu öffentlichen Diensten realisiert werden. Wie in vielen Bereichen des Rechts auf Privatsphäre ist auch hier nicht eine grundsätzlich fehlende Regulierung das vorrangige Problem, es geht in erster Linie darum, die Effektivität und Durchsetzungskraft rechtlicher Normen zu erhöhen, und gegebenenfalls geltende Regeln an neue technische Herausforderungen anzupassen.

zukünftiges Problemfeld e-Government

Data Mining ist in wesentlichen Schritten ein unternehmensinterner Prozess, der auch ohne rechtlich unzulässige Verwendungen von Fremdaten oder von Daten mit Personenbezug durchgeführt werden kann. Viele, auch für Unternehmen wertvolle, statistische Aussagen und Zusammenhänge können auf Basis anonymisierter Daten ermittelt werden. Freiwillige Einschränkungen auf Seite der Unternehmen können daher einen großen Beitrag zur Wahrung der Privatsphäre liefern. Allerdings widerspricht ein allgemeiner Verzicht auf personalisierte Auswertungen grundsätzlichen unternehmerischen Interessen. Für eine Vielzahl von Verwendungen, beispielsweise individualisierte Angebote oder gezielte Werbemaßnahmen im Rahmen des CRM, ist eine Personalisierung unumgänglich.

„freiwillige" Beschränkungen bedürfen unterstützender Maßnahmen

Ein „freiwilliger" Verzicht auf personenbezogene Auswertungen oder Anwendungen ist ohne entsprechende regulative Beschränkungen oder öffentlichen Druck bzw. einem drohenden Verlust an Reputation kaum realistisch. Die Bereitschaft seitens der Unternehmen, die Privatsphäre der Kunden zu achten, wird zu einem wesentlichen Teil davon abhängen, ob es gelingt, den in zahlreichen empirischen Erhebungen festgestellten hohen Stellenwert des Datenschutzes den Unternehmen in spürbarer Weise zu vermitteln. Eine Voraussetzung dafür ist es, die KonsumentInnen auch in diesem Bereich zu sensibilisieren und ihnen Unterstützung dabei anzubieten, wie sie Informationen einholen oder ihre Interessen durchsetzen können. Es müssen aber auch Unternehmen Möglichkeiten geboten werden, datenschutzkonformes Verhalten und die Einhaltung freiwilliger Vereinbarungen auf einfache Weise zu kommunizieren, sowohl um ihnen einen Wettbewerbsvorteil zu eröffnen als auch den KonsumentInnen eine Entscheidungshilfe zu bieten. Natürlich ist auch beim Zustandekommen von wirksamen Formen der Selbstregulierung der Gesetzgeber gefragt, indem er etwa Leitlinien und zu erfüllende Mindeststandards vorgibt und durch die Androhung von Zwangsausübung untermauert.

5 Bürgerkarte

Datenverabeitungen im öffentlichen Sektor

In den vorangegangenen Abschnitten über private Internet-Nutzung und Data-Mining ging es vor allem um Handlungsspielräume der KonsumentInnen hinsichtlich der Datengenerierung und -verwendung durch private Einheiten (Unternehmen). Im folgenden Abschnitt steht eine Anwendung des e-Government und damit öffentlicher Datenverarbeitung im Zentrum der Überlegungen.

Chipkarte mit digitaler Signatur als technische Basis

Die möglichen effizienzsteigernden Wirkungen des Einsatzes neuer Informations- und Kommunikationstechnologien sollen zunehmend auch im Bereich der öffentlichen Verwaltung genutzt werden. Stichworte dazu sind „e-Government", „one-Stop-Shop", der „elektronischer Akt", und „Transparenz der Verwaltung". Zentrales Element dabei ist die Chipkarte – oder ein anderes Trägermedium, welches es mit der darauf realisierten digitalen Signatur den BürgerInnen ermöglichen soll, unkompliziert und sicher mit Behörden in Kontakt zu treten und Behördenwege abzuwickeln. Im Jahr 2000 wurde deshalb eine „e-Europe Smart Cards" Initiative gestartet, die sich in zwölf Arbeitsgruppen damit beschäftigt, eine EU-weite Identität für sichere Transaktionen mit der dazu notwendigen Public-Key-Infrastruktur aufzubauen (Hassler 2000). Die Umsetzung innerhalb Österreichs wird vom BMöLS koordiniert und umfasst die „Aufstellung gemeinsamer Grundspezifizierungen für die Interoperabilität und Sicherheit intelligenter Chipkarten … angestrebt wird eine einheitliche sichere elektronische Signatur für alle Anwendungen, sowohl im elektronischen Geschäftsverkehr als auch im e-Government." (BKA 2001) Wesentliches Element dabei ist die Einführung der Sozialversicherungskarte und die flächendeckende Versorgung und Vollausstattung bis Mitte 2003. Geplant ist die „Sozialversicherungskarte auf Bürgerkarte mit digitaler Signatur und weitere mögliche Anwendungen … zur Erledigung von Amts- und Behördenwegen mittels elektronischer Signatur" auszubauen (vgl. BKA 2001). Diese in die europäischen Aktivitäten (Smart Card Charta vom März 2000) eingebettete Einführung der Bürgerkarte wurde am 20.11.2000 in einer Regierungsklausur beschlossen.

Ausgangspunkt Sozialversicherungskarte

Gestaltungsvarianten der e-Card

Vor diesem Hintergrund erscheint es notwendig, zu klären wie Chipkarten als Schlüsselkarten aus Sicht des Datenschutzes bzw. der Privatsphäre des Einzelnen grundsätzlich einzuschätzen sind bzw. welche Wirkungen auf die BürgerInnen von unterschiedlichen Gestaltungsvarianten ausgehen. Insbesondere die enge Verquickung der geplanten „Bürgerkarte" mit der SV-Karte (neu: e-Card) und der damit einhergehenden flächendeckenden Verbreitung macht diese Analyse dringlich.

5.1 Bürgerkarte was ist das überhaupt?

unterschiedlichen Definitionen der „Bürgerkarte"

Vorerst sind einige definitorische Klärungen notwendig, da es auf Anhieb nicht deutlich wird, was womit gemeint ist. Selbst die Betreiber des Projekts gehen in unterschiedlichen Kontexten von unterschiedlichen Definitionen aus: „Der Name Bürgerkarte ist ein Arbeitstitel für das Chipkartenprojekt der österreichischen Verwaltung. Es stellt dies eine Schlüsseltechnologie auf der Seite des/der Bürger(s)In und der Verwaltung bei der Nutzung von e-Government dar." (Posch und Leitold 2001). Oder aber: „Die Bürgerkarte ist die Sozialversicherungskarte, die durch die elektronische Signatur Ausweis zur Iden-

tifikation auf der Reise am Datenhighway wird. Sie kann zusätzlich zu den Identifikationsdaten auch private Infoboxen zum einfachen Transport von Informationen beinhalten." (Posch 2001a)

die aktuelle Definition

Im aktuellsten Dokument zur Bürgerkarte dem Weißbuch Bürgerkarte (Posch et al. 2002, 4) wird mit Stand 15. Mai 2002, das „Konzept Bürgerkarte" wie folgt definiert: „Konzept Bürgerkarte ist der Arbeitstitel der österreichischen Verwaltung für jenes Werkzeug, das es dem Bürger und der Verwaltung ermöglicht, an e-Government sicher und authentisch teilzunehmen. Es stellt dies eine Schlüsseltechnologie bei der Nutzung von e-Government dar. In einem möglichst offenen und daher für die weiteren Entwicklungen des hoch dynamischen Bereiches der e-Technologien geeigneten System ermöglicht ein dem Konzept Bürgerkarte entsprechender Token die notwendige Identifikation der Betroffenen. Transaktionen, die bislang nur durch persönliches Erscheinen oder mit konventionellen Mitteln (unterfertigte Formulare) möglich waren, können damit online durchgeführt werden."

das Konzept wird breiter

Wenn man sich die unterschiedlichen Definitionen und Absichtserklärungen vor Augen führt, wird deutlich, dass es im Zeitablauf eine Verschiebung der Terminologie und Zielrichtung des Projektes gegeben hat. War zu Beginn der Diskussion vor allem von der „SV-Card als Bürgerkarte" bzw. dem „Chipkartenprojekt der Verwaltung" die Rede, hat sich der offene Ansatz nun durchgesetzt, sodass durchgängig von einem „entsprechendem Token" die Rede ist. Die angestrebte Technologieneutralität des Konzeptes kann aber nicht darüber hinweg täuschen, dass in den meisten Anwendungsfällen eine Chipkarte das Trägermedium sein wird. Das größte Potential (quantitativ) wird die e-Card der Sozialversicherung haben, da sie mit etwa acht Millionen „bürgerkartenfähigen" Chipkarten die weitestverbreitete Karte im Feld sein wird. Das größte Potential (qualitativ) wird wohl von Anwendungen ausgehen, deren NutzerInnen direkt erkennbare Vorteile aus e-Government Anwendungen ziehen können (Unternehmen, StudentInnen etc.). Doch auch diese Anwendungen werden in den meisten Fällen auf Chipkarten realisiert werden. Sodass die Bürgerkarte etwa wie folgt charakterisiert werden kann: *Bürgerkarte = (SV-)Chipkarte + sichere elektronische Signatur + „Datenhandtaschen" vulgo „InfoBoxen"*. Zu diesen Basiselementen kommt als dritte Funktionalität noch die „Identifikation und Authentifikation durch die Personenbindung" hinzu (Posch et al. 2002, 5). Die Funktionalität „sichere elektronische Signatur" ist geeignet auch aus Sicht von KonsumentInnen und BürgerInnen eine Erhöhung des Sicherheitsniveaus elektronischer Abwicklungen zu gewährleisten. Technische Details, sowie Vor- und Nachteile unterschiedlicher Verfahren können hier nicht näher behandelt werden. Soziale Implikationen der elektronischen Signatur sowie die Funktionalitäten „Datenspeicher (InfoBoxen)" und „Identifikation und Authentifikation durch die Personenbindung" werden aber weiter unten unter Datenschutz Gesichtspunkten noch zu diskutieren sein.

unterschiedliche Realisierungen angedacht

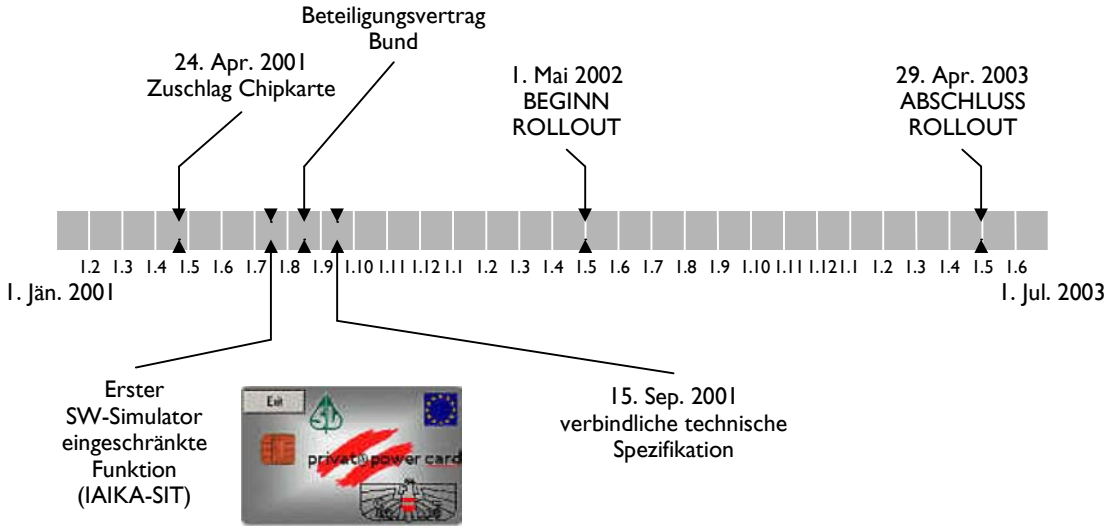
Da es sich, wie aus der ersten Definition hervorgeht, bei der Bürgerkarte grundsätzlich um ein „offenes Konzept" (Posch 2002, 29) handeln soll, sind auch andere Realisierungen (als jene auf der e-Card) möglich. Angedacht sind derzeit eine Verbindung von Bürgerkarte und Personalausweis, die Einführung eines EU-Reisedokuments, die Verknüpfung von Bürgerkarte und zukünftig auf Chipkartentechnologie basierendem Reisepass, eine österreichische StudentInnen Card, die Verbindung von Dienstausweis öffentlich Bediensteter mit der Bürgerkarte oder auch eine zukünftige Verquickung von Führerschein und Bürgerkarte. Als eines der ersten konkreten Projekte wird die Österreichische Computergesellschaft (OCG) ihre Mitgliedskarten mit Bürgerkarten Funktionalität ausstatten (Posch et al. 2002, 12).

elektronische Signatur als gemeinsames Merkmal

Gemeinsames Kernelement aller angedachten Varianten ist die Verwendung einer Chipkarte (oder eines anderen Tokens) als Trägermedium für eine sichere elektronische Signatur. Das Konzept Bürgerkarte ist demgemäß der Versuch eine informationstechnische Umgebung für e-Government zu schaffen, die es über einheitliche Schnittstellen erlaubt, mit Hilfe einer sicheren Signatur mit qualifiziertem Zertifikat lt. SigG an die Verwaltung heranzutreten und auch Erledigungen durchzuführen.

5.2 Zeitplan

Die folgende Graphik zeigt – bezogen auf die e-Card – den ursprünglich beabsichtigten Zeitplan der Einführung der Bürgerkarte in Österreich:



Quelle: Posch 2001b

5.3 Ziele

elektronische Behördenwege

Die Ziele, die mit der Einführung der Bürgerkarte verfolgt werden, liegen vor allem in der Ermöglichung des elektronischen Aktes bzw. der Öffnung der Verwaltung für Online-Zugänge. Der elektronische Behördenweg soll es den BürgerInnen (so sie Zugang zu neuen elektronischen Kommunikationsmitteln haben) leichter machen und der Verwaltung helfen, effizienter zu arbeiten. Da aber noch geraume Zeit davon auszugehen ist, dass eine große Anzahl von BürgerInnen keinen Internetzugang haben bzw. diesen nicht für Behördenwege nutzen können oder wollen, ist für lange Zeiträume eine Parallelstruktur notwendig, die sowohl den herkömmlichen, wie auch den elektronischen Zugang ermöglicht.

Potential für weniger zentrale Register

Eine weitere Motivation für den Einsatz der Bürgerkarte als Schlüsselkarte könnte das Bestreben sein, zentrale Register zu verringern. Dazu kann die Karte theoretisch beitragen, nur dies setzt eine entsprechende Systemgestaltung voraus. Mit Hilfe der Karte könnten tatsächlich die Vernetzung im Bereich der öffentlichen Verwaltung und auch die Weitergabe von Daten zwischen Behörden hintan gehalten werden. Die Karte könnte als „Ermächtiger" dienen, die es im Sinne des Rechts auf informationelle Selbstbestimmung den BürgerInnen selbst in die Hand gibt, den BeamtInnen Zugriff auf bestimmte Daten zu ermöglichen. Unklar bleibt aber inwieweit man durch die Multifunktionalität (SV-Karte, in Zukunft vielleicht auch Bankomatkarten etc.) und insbesondere durch das Aufbringen von „Info-Boxen" die Akzeptanz beeinträchtigt. Sobald Daten auf der Karte gespeichert werden, hat man/frau das Problem des notwendigen Back-Up. Hier hängt es sehr von der gewählten Strategie des Einzelnen bzw. der Provider ab, ob es zu der angestrebten Dezentralisierung oder zum Ausbau zentraler Register kommt.

zweischneidige „elektronische Identität"

Weitere Ziele der Einführung der Bürgerkarte könnten in der Schaffung einer „elektronischen Identität" liegen. Diese ist unter modernen Dateschutzgesichtspunkten besonders kritisch zu hinterfragen, da eine eineindeutige Zuordnung von Online-Aktivitäten zu einer konkreten Person den Grundsätzen von Datenvermeidung, Pseudonymität und Anonymität widerspricht. Eine elektronische Signatur kann aber andererseits auch dazu führen, das Vertrauen der KonsumentInnen in den e-Commerce anzuheben und so den e-Commerce – zumindest in Teilbereichen – durch die höhere Sicherheit bei der Abwicklung mittels elektronischer Signatur, ankurbeln. Nicht zuletzt ist auch der Aufbau einschlägiger Kompetenzzentren in einem österreichischen Sicherheitscluster ein wirtschaftspolitisches Ziel.

5.4 Problemfelder

5.4.1 Offene Fragen zur digitalen Signatur

grundlegende Funktionen einer Unterschrift

Die Grundfunktionalitäten der Bürgerkarte zeichnen sich durch unterschiedliche Nutzungsszenarien und dementsprechende Bedrohungsbilder aus. Die sichere elektronische Signatur ist in ihren rechtlichen Wirkungen im SigG geregelt. Die technischen Fragestellungen (Verfahren etc,) werden in der breiten technischen Literatur abgehandelt. Allenfalls zu fragen wäre, ob neben den rechtlichen und technischen Vorkehrungen auch die sozialen Rahmenbedingungen hinreichend gut entwickelt sind, sodass sie einen problemlosen Einsatz erwarten lassen. Um diese Frage zu klären, werden zuerst die Funktionen einer Unterschrift (vgl. Fox 1995) dargestellt. Soll die digitale Signatur nicht nur dieselbe Rechtsverbindlichkeit erhalten, wie sie der eigenhändigen Unterschrift zukommt, sondern auch in ähnlicher Weise Verwendung finden, so ist zu untersuchen, ob die digitale Signatur auch bzw. inwieweit sie die fünf grundlegenden Funktionen jener erfüllt.

Abschlussfunktion

Die wichtigste Funktion einer Unterschrift im Alltagsleben ist die *Abschlussfunktion*: Eine Unterschrift ist der Abschluss einer Willenserklärung. Hier bringt die elektronische Signatur eine Verbesserung, da ein elektronisch signiertes Dokument nicht mehr unbemerkt verändert werden kann.

Warnfunktion

Unmittelbar mit dem Abschluss hängt die *Warnfunktion* einer Unterschrift zusammen. Es ist lange Tradition und sozial gelernt, dass man sich den Inhalt und dessen Auswirkungen gut überlegen sollte bevor man ein Schriftstück unterfertigt. Das Unterschreiben soll so vor übereilten Handlungen schützen.

Das leisten elektronische Signaturverfahren nur bei entsprechender Systemgestaltung (Rückfrage des Programms, extra Eingabe eines PIN etc.). Eine komfortable, schnelle Signierung mit einmaligem Mausklick allein, wäre in diesem Sinn alles andere als unproblematisch.

Echtheitsfunktion

Die dritte Funktion einer Unterschrift ist die *Echtheitsfunktion*: Sie soll sicherstellen, dass das signierte Dokument tatsächlich vom Signator kommt. Die Herkunft der Erklärung ist aber durch elektronische Signaturen nur bedingt gesichert, da die Dokumentenerstellung getrennt von der Signierung und zudem mit Hilfe eines technischen Hilfsmittels (PC) vor sich geht. Hier sind hohe Anforderungen an die sichere Arbeitsumgebung zu stellen, die im Büro oder auch am Heimcomputerplatz nicht immer leicht zu gewährleisten sein werden.

Identitätsfunktion

Die *Identitätsfunktion* steht in engem Zusammenhang mit der Echtheitsfunktion. Sie soll die Identität des Ausstellers bekunden. Dies wird in der vorgestellten Bürgerkarte durch die so genannte Personenbindung (s.w.u.) zu erzeugen versucht. Umfassend kann dies aber nicht gewährleistet werden, da das Signieren auch von anderen Personen vollzogen werden kann (wenn z. B. der/die Berechtigte die Chipkarte an eine MitarbeiterIn oder KollegIn weitergibt).[69]

Beweisfunktion und zusätzlich Unleugbarkeit

Schließlich haben Unterschriften auch noch eine *Beweisfunktion*: Diese ist nach SigG bei sicheren elektronischen Signaturen bzw. qualifizierten Zertifikaten gegeben. Eine Steigerung der rechtlichen Sicherheit von Unterschriften wird auch dadurch erreicht, dass zu den o. a. Grundfunktionen einer Unterschrift noch die *Unleugbarkeit* hinzutritt. Durch Einbindung gesicherter Zeitstempel wird eindeutig geklärt, wann eine Willenserklärung unterfertigt und übermittelt wurde. Dies führt dazu, dass dieser Prozess nicht mehr im Nachhinein abgestritten werden kann (vgl. Posch et al. 2002, 17).

(noch) kein Äquivalent

Wie sich zeigt, bietet die elektronische Signatur nicht in allen Bereichen ein absolutes Äquivalent zur eigenhändigen Unterschrift. Dies wird auch noch einige Zeit in Anspruch nehmen. Formal sind mittlerweile die institutionellen Voraussetzungen für eine geeignete Sicherheitsinfrastruktur geschaffen. Als Aufsichtsstelle fungiert die RTR-GmbH, Zertifizierungsdiensteanbieter mit den Produkten a-sign, e-sign sind, wenn auch noch sehr kurz, am Markt und auch eine Bestätigungs-/Prüfstelle wurde mit dem Verein a-SIT eingerichtet. Durch das SigG wurden schon zu Beginn des Jahres 2000 die legistischen Rahmenbedingungen richtlinienkonform umgesetzt. Allein die Frage nach den sozialen Rahmenbedingungen bleibt noch unbeantwortet. Werden die KonsumentInnen diese Art der Zeichnung akzeptieren? Kann die abstrakte Unterschrift mittels Mausklick ihrer Warnfunktion nachkommen? Wer wird bereit sein für seine Unterschrift in Hinkunft zu zahlen? Ist der Zugewinn der elektronischen Abwicklung den Preis wert? Welche Produkte werden den Markt beherrschen? Wird man in Zukunft gezwungen sein die digitale Signatur zu verwenden? Was geschieht mit jenen MitbürgerInnen, die sich die digitale Signatur nicht leisten können bzw. überhaupt am elektronischen Leben nicht teilhaben können oder wollen? Kommt es zu Diskriminierungen in der Abwicklung, je nach Art des Anbringens? Fragen über Fragen, die nur einen Auszug aus den sich stellenden Problemen darstellen. Bei vorsorglicher Systemgestaltung unter Einbeziehung der Betroffenen könnten möglicherweise noch einige andere in die Diskussion eingebracht und einige davon auch einer Lösung zugeführt werden.

soziale Rahmenbedingungen noch offen

---

[69] Auch wenn § 21 SigG normiert, dass der Signator verpflichtet ist, die Signaturerstellungsdaten sorgfältig zu verwahren, soweit zumutbar Zugriffe auf Signaturerstellungsdaten zu verhindern und deren Weitergabe zu unterlassen, so ist wohl von der sozialen Realität auszugehen, dass im betrieblichen Umfeld die Signierung auch durch KollegInnen/Assistenzkräfte und/oder Vertraute erfolgen wird. Hier bedarf es besonderer Anstrengungen, den NutzerInnen die rechtlichen Wirkungen derartiger Verhaltensweisen deutlich zu machen.

5.4.2 Die ZMR-Zahl als Personenkennzahl

Gefahr der allgemeinen Verwendung der ZMR-Zahl als Personenkennzahl

Von den Grundfunktionen der Bürgerkarte ist aus Datenschutzüberlegungen insbesondere die direkte Personenbindung über die ZMR-Zahl (Zentrale Melderegister-Zahl) problematisch. Mit der ZMR-Zahl wurde in Österreich eine amtliche Personenkennzahl (PKZ)[70] eingeführt, die die bisher schon vorhandene Sozialversicherungsnummer an Genauigkeit übertrifft und vor allem aus der Verwaltung für die Verwaltung geschaffen wurde. Die Verwendung der Sozialversicherungsnummer unterliegt wie alle personenbezogenen Daten dem Zweckbestimmungsprinzip. Ihre Verwendung zur Kennung von Personen in anderen Bereichen als dem Sozialversicherungswesen (etwa der Finanzverwaltung) wurde relativ restriktiv gehandhabt und ist vor allem an gesetzliche Ermächtigungen gebunden. In anderen Bereichen wurden andere spezifische Ordnungskriterien (etwa die Matrikelnummer der jeweiligen Universität oder Fachhochschule) verwendet. Mit Einführung der ZMR-Zahl besteht nun die Gefahr, dass im Zuge der „Verwaltungsvereinfachung" diese Nummer auch in anderen Bereichen außerhalb des Meldewesens eingesetzt werden wird. Dass diese Gefahr durchaus besteht, kann auch aus der Tatsache abgeleitet werden, dass die ZMR-Zahl als Ausgangsbasis für die Aktualisierung der SV-Nummern herangezogen werden soll. Gesetzliche Vorkehrungen dazu wurden im Meldegesetz und im ASVG bereits getroffen: es besteht eine Gleichsetzungstabelle zwischen Sozialversicherungsnummer und ZMR-Zahl.[71] Auch die beabsichtigte Einführung einer Bildungsevidenz soll sich ja der SV-Nummer und über die Gleichsetzungstabelle auch der ZMR-Zahl bedienen. Damit können personalisierte „Bildungskarrieren" der BürgerInnen jahrzehntelang gespeichert werden (ARGE Daten 2002a).

---

[70] Auch wenn von offizieller Seite die ZMR-Zahl nicht als PKZ bezeichnet wird, so ist doch festzuhalten, dass sie ihrem Wesen nach das Potential zur flächendeckenden Verwendung und damit zur Funktion als PKZ in sich birgt.

[71] siehe § 16b (1) Meldegesetz und § 360 (6) Allgemeines Sozialversicherungsgesetz:

MeldeG: § 16b. (1) Zur Durchführung statistischer Erhebungen kann der Bundesminister für Inneres im Wege des ZMR Namen, Geburtsdatum und -ort, Wohnadressen, Staatsangehörigkeit, Familienname vor der ersten Eheschließung und die ZMR-Zahl für die Meldebehörden ermitteln, mit den von den Sozialversicherungsträgern Versicherten zugeordneten Versicherungsnummern in einem Verzeichnis (Gleichsetzungstabelle) verarbeiten und die Auswählbarkeit der dadurch geschaffenen Personendatensätze nach der ZMR-Zahl und der Sozialversicherungsnummer vorsehen.

(2) Zur Führung der Gleichsetzungstabelle hat der Hauptverband der österreichischen Sozialversicherungsträger dem Bundesminister für Inneres die von Sozialversicherungsträgern bestimmten Menschen zugeordneten Versicherungsnummern zu übermitteln und – sofern zu einem Menschen bereits ein Personendatensatz im Verzeichnis gemäß Abs. 1 verarbeitet wird – diesem zuzuordnen.

ASVG: § 360. (6) Die Sozialversicherungsträger und der Hauptverband haben zur Sicherung der Unverwechselbarkeit und Richtigkeit der von ihnen verwendeten Daten sowie zur Durchführung ihrer Verfahren das Recht, das Verfahren der Meldebehörden nach § 14 Abs. 2 des Meldegesetzes 1991 in Anspruch zu nehmen. Sie sind verpflichtet, bei Änderungen (Feststellung, Richtigstellung usw.) von Familiennamen, Vornamen, Geschlechtsangabe, Staatsbürgerschaft und Geburtsdaten sowie der ZMR-Zahl (§ 16 Meldegesetz 1991) mit dem Zentralen Melderegister beim Bundesminister für Inneres zum Zwecke der Führung der Gleichsetzungstabelle (§ 16b Meldegesetz 1991 in der Fassung des Artikels II des Bundesgesetzes BGBl. I Nr. 28/2001) zusammenzuarbeiten und dort geänderte Daten zu verwenden, soweit dies zur eindeutigen Identifizierung einer Person notwendig ist. Leistungsansprüche, Anwartschaften oder deren Veränderungen können aus solchen Änderungen nicht abgeleitet werden.

ZMR-Zahl wichtiges Merkmal für die Identifikation von BürgerInnen

Auch die Formulierung des § 16 (1) MeldeG weist in Richtung generelle Verwendung der ZMR-Zahl: „Das zentrale Melderegister ist insofern ein öffentliches Register, als der Hauptwohnsitz eines Menschen oder jener Wohnsitz, an dem dieser Mensch zuletzt mit Hauptwohnsitz gemeldet war, abgefragt werden kann, wenn der Anfragende den Menschen durch Vor- und Familiennamen, das Geburtsdatum und ein zusätzliches Merkmal, wie etwa Geburtsort, ZMR-Zahl oder einen bisherigen Wohnsitz, bestimmt. Über andere gemeldete Wohnsitze dieses Menschen darf einem Abfragenden nur bei Nachweis eines berechtigten Interesses Auskunft erteilt werden." Damit wird deutlich, dass die Kenntnis der ZMR-Zahl einer BürgerIn ein wichtiges Merkmal für deren Identifikation wird. Sie also das Potential zur universellen Verwendung – und damit ein deutlich gestiegenes Missbrauchspotential – hat.

wenig Schutz vor genereller Verwendung

Offen ist derzeit noch, wie stark der Druck für die BürgerInnen werden wird, die ZMR-Zahl universell einsetzen zu müssen. Beim Einsatz der Bürgerkarte ist zwar lt. AVG die Verwendung und Speicherung der ZMR-Zahl verboten, § 13 Abs. 4a AVG normiert aber nur: „Die ZMR-Zahl darf von der Behörde anlässlich der elektronischen Identifikation nicht aufgezeichnet werden." Ein globales Verbot der Verwendung der ZMR-Zahl zur Identifikation wäre im Sinne des Schutzes der Privatsphäre der BürgerInnen wesentlich deutlicher und deshalb vorzuziehen.

Zusammenführung von Daten wird vereinfacht

Die stärksten Befürworter einer Personenkennzahl kommen aus der Statistik, die ein über mehrere öffentliche Register hinweg gleiches Identifikationsmerkmal fordern, um die Zusammenführung von Daten zu erleichtern. Die Identifikation wird aber durch eine Personenkennzahl über die Statistik hinaus in verschiedenen Behörden und v. a. auch im kommerziellen Bereich erheblich erleichtert:

- Unternehmen könnten gewillt sein ihr Risiko zu minimieren und auch bei Bagatellgeschäften die Identifizierung verlangen (in einer Videothek könnte etwa statt eines Mitgliedsausweises oder Lichtbildausweises die ZMR-Zahl abverlangt werden. Die Folge daraus: Sie kann leicht elektronisch gespeichert werden und ist somit wieder verwendbar und auswertbar, statt wie beim Ausweis, der einmal gesehen und kontrolliert wird, was für diese Anwendung auch ausreichend ist.)
- Arbeitgeber könnten zukünftig Kosten für den Aufbau und das Design einer eigenen Datenbank sparen, wenn die ZMR-Zahl auch für das firmeninterne Zutrittssystem herangezogen wird.
- Etc.

Personenkennzahl in Deutschland als verfassungswidrig eingestuft

Das grundsätzliche Gefährdungspotential liegt darin, dass die Verarbeitung personenbezogener Daten sich verselbständigen könnte, Verknüpfungen werden sehr leicht machbar und präzise (damit noch wertvoller), sie könnten sich jedoch leicht jeglicher Steuerung entziehen. In Deutschland wurde deshalb vom Rechtsausschuss des Bundestages (5. Mai 1976) für die BRD eine PKZ als verfassungswidrig abgelehnt. Auch das schon zitierte Volkszählungsurteil von 1983 sieht in der Einführung einer PKZ (für alle Register und Dateien) einen wesentlichen Schritt dazu, die Bürger in ihrer ganzen Persönlichkeit zu registrieren und zu katalogisieren, und damit gegen das Persönlichkeitsrecht zu verstoßen.

die Möglichkeit schafft Gefahren des Missbrauchs

Diese Beispiele zeigen wie notwendig entsprechend strenge legistische Vorkehrungen – etwa das explizite Verbot der Verwendung der ZMR-Zahl für andere als gesetzlich angeordnete Anwendungen – sind. Kotschy (2001, 101) bringt die gesamte Problematik auf den Punkt: „Der Umstand, dass die Statistik an personenbezogenen Daten im Endeffekt nicht interessiert ist, kann nicht darüber hinwegtäuschen, dass mit dem Vorhandensein eines geschärften Suchinstrumentariums auch die Gefahr seiner Verwendung verknüpft ist, und zwar

nicht nur illegalerweise: Es ist ein bekanntes Phänomen, dass neue Möglichkeiten der Informationssuche neue Begehrlichkeiten wecken, die vom Gesetzgeber nur allzu oft bereitwillig durch entsprechende Ermächtigungsnormen erfüllt werden."

5.4.3 Die ZMR-Zahl auf der e-Card

Anhaltspunkte der e-Card Gestaltung im ASVG

Die Konzepte zur Bürgerkarte sind in weiten Abschnitten eher vage. Gleichzeitig hängt das Projekt Bürgerkarte ganz wesentlich mit der Einführung der e-Card zusammen. Deshalb ergibt die Diskussion der konkreten Änderungen des ASVG und anderer Gesetze im Zusammenhang mit der Vorbereitung der e-Card für die Bürgerkarte erste konkrete Anhaltspunkte für die Analyse des Konzepts Bürgerkarte. Die wesentlichen Änderungen am ursprünglichen Konzept der SV-Karte wurden im Rahmen der 59. ASVG Novelle durchgeführt. Dabei wurde u. a. der § 31a des ASVG geändert. Die damit einhergehenden Probleme und offenen Fragen sind mannigfaltig:

> *§ 31a (2) Das ELSY hat Datenschutz und Datensicherheit zu gewährleisten. Auf die im ELSY verwendeten Daten sind die Bestimmungen des Datenschutzgesetzes 2000 anzuwenden. Die innerhalb des ELSY zu verwendenden Chipkarten sind bundesweit einheitlich und als Schlüsselkarten zu gestalten, die auch die Authentifizierung des Karteninhabers (der Karteninhaberin) im elektronischen Verkehr ermöglichen und dem (der) berechtigten Verwender(in) nach Zustimmung des (der) Betroffenen den Zugriff auf persönliche Daten, die bei anderen Stellen gespeichert sind, möglich machen.*

Freiwilligkeit offen

Diese Passage im Gesetzestext lässt offen, ob die SV-Karte nun eine Schlüsselkarte zu sein hat oder ob diese Anwendung für die BürgerInnen tatsächlich freiwillig sein wird, wie es bisher immer kommuniziert wurde. Hier wäre eine sprachlich klarere Formulierung des Gesetzestextes wünschenswert. Unklar ist vor allem der Begriff der Schlüsselkarte, der für unterschiedliche Bedeutungsinhalte stehen kann. Einerseits die Karte als Schlüssel: nur wer sie besitzt hat Zugang zu Daten, oder andererseits die Karte als Speichermedium für Schlüssel (wie sie etwa in der Generierung von elektronischen Signaturen bzw. zur Verschlüsselung von Daten eingesetzt werden). Die Funktion als Schlüsselkarte für das Gesundheitswesen kann in ihrer einfachsten Ausfertigung der elektronische Krankenschein sein, denn er stellt sicher, dass eine PatientIn versichert ist und demgemäss Zugang zum österreichischen Gesundheitswesen haben soll. Die Schlüsselkarte in ihrer entwickelteren Version verweist viel eher auf die Verwendung von kryptographischen Schlüsseln, wie eben bei der Anwendung der elektronischen Signatur (Bürgerkarte) verwendet werden. Dass diese Formulierung eher so gemeint sein dürfte ist auch daraus abzulesen, dass von „berechtigten Verwendern" und „Zugriff auf persönlichen Daten" gesprochen wird. Bemerkenswert ist auch, dass das ASVG von Authentifizierung und nicht von Identifizierung spricht. Das bedeutet, dass das Weißbuch Bürgerkarte nicht im Einklang mit dem Gesetz formuliert ist, da dort die Identifizierung über die Personenbindung vorgesehen ist.[72]

[72] Details dazu im Abschnitt: 5.4.4.

Auch hinsichtlich des Umfanges der zu speichernden Daten erweitert der geänderte § 31a das Spektrum nicht unwesentlich:

§ 31a (3) Auf den innerhalb des ELSY zu verwendenden Chipkarten dürfen nur folgende Daten gespeichert werden:

1. Angaben zur Person, für die die Chipkarte ausgestellt wurde:
a) Namen, Geburtsdatum, Geschlecht;
b) Versicherungsnummer (§ 31 Abs. 4 Z 1);

2. Bezeichnung des Chipkartenausstellers, Datum der Ausstellung und Chipkartennummer samt Gültigkeitskennzeichnung;

3. sonstige Daten, deren Speicherung bundesgesetzlich vorgesehen ist.

(4) Bestandteile des ELSY dürfen für andere als Sozialversicherungszwecke nur mit bundesgesetzlicher Ermächtigung und nur so weit verwendet werden, als dies mit dem Zweck des ELSY nicht unvereinbar (§ 6 Abs. 1 Z 2 DSG 2000) ist. Zu Fragen der Unvereinbarkeit neuer Verwendungszwecke sowie zu Fragen der Speicherung von Daten auf den innerhalb des ELSY zu verwendenden Chipkarten ist der Datenschutzrat unter Setzung einer angemessenen Frist anzuhören.

unklare Formulierung lässt vielfältige Interpretationen zu

In Abs. 3/3 wurde eine sehr offene Formulierung gewählt, die den weiteren Ausbau der e-Card, weit über die Digitale Signatur und die Info-Boxen hinaus ermöglicht. Die erste Ausweitung der Daten jenseits der o. a. wurde bereits mit der Speicherung der ZMR-Zahl realisiert (§ 13 Abs. 4a AVG). Auch Abs. 4 gibt Raum für Spekulationen. Wann ist eine Anwendung „nicht unvereinbar"? Wie groß hier die Unsicherheiten sind, zeigt die Einschätzung von Souhrada-Kirchmayer (2001, 221f): „Dieser Begriff stammt aus Art. 6 RL 95/46/EG und ist extrem interpretationsbedürftig. Nicht einmal die einschlägigen Gruppen, die auf der Basis der RL 95/46/EG in Brüssel tagen, haben sich bisher zu einer eindeutigen Interpretation dieser Formulierung durchringen können. Bei der Gesetzwerdung des § 31a ASVG dachte man noch an Verwendungszwekke, die zumindest dem Sozialversicherungswesen angelagert sind."

Schlüsselkarte beinhaltet positive Potentiale

Grundsätzlich ist die Idee der Schlüsselkarte – im Sinne des Ermächtigens – positiv zu beurteilen, da sie der NutzerIn die Möglichkeit in die Hand gibt, aktiv in den sie betreffenden Datenaustausch einzugreifen (bzw. diesen überhaupt erst zu ermöglichen). Eine wirkliche PET (privacy enhancing technology) wäre dies allerdings nur, wenn die strikte Freiwilligkeit realisiert würde. Der Realisierung der unbedingten Freiwilligkeit stehen im konkreten Projekt die große Verbreitung und das damit zusammenhängende Wissen um den Besitz dieser Karte entgegen. Da jede(r) ÖsterrreicherIn die e-Card haben wird, kann – anders als bei freiwilligem Bezug der Karte – leicht sozialer Druck in Richtung bestimmter Anwendungen entstehen.

Speicherung der ZMR-Zahl auf der Chipkarte

Eine weitere in Hinblick auf die Freiwilligkeit der Verwendung problematische Systemvariante ist die Absicht, die ZMR-Zahl auf der Chipkarte zu speichern. Dies wurde im AVG festgeschrieben:

§ 13 (4a): Zum Zweck der eindeutigen Identifikation von Verfahrensbeteiligten im elektronischen Verkehr mit der Behörde darf diese die ZMR-Zahl (§ 16 Abs. 4 des Meldegesetzes 1991, BGBl. Nr. 9/1992) als Ausgangsbasis für eine verwaltungsbereichsspezifisch unterschiedliche, abgeleitete und verschlüsselte Personenkennzeichnung verwenden. Die ZMR-Zahl darf auch auf den im elektronischen Verwaltungssystem für die Sozialversicherung (ELSY, § 31a Abs. 1 des Allgemeinen Sozialversicherungsgesetzes, BGBl. Nr. 189/1955) verwendeten Chipkarten als Ausgangszahl für die eindeutige Identifikation des Karteninhabers bei der Anwendung der elektronischen Signatur und der Verschlüsselung gespeichert werden. Die ZMR-Zahl darf von der Behörde anlässlich der elektronischen Identifikation nicht aufgezeichnet werden.

Freiwilligkeit noch ungeklärt

Es konnte bisher nicht zweifelsfrei geklärt werden, ob die ZMR-Zahl automatisch auf der e-Card gespeichert werden wird, oder ob dies nur mit dem Einverständnis der Betroffenen geschehen darf. Dadurch wären dann aber auf der SV-Card in ihrer Ausformung als Bürgerkarte neben den notwendigen Stammdaten (ASVG § 31a Abs. 3 Ziffer 1–2 Name, Geburtsdatum, Geschlecht, Versicherungsnummer, Chipkartenaussteller, Datum der Ausstellung, Chipkartennummer) auch die ZMR-Zahl, die digitale Signatur, die Datenhandtaschen, Info-Boxen, möglicherweise andere zusätzliche Anwendungen, Notfalldaten etc. gespeichert. Für Techniker ist vielleicht noch nachvollziehbar, dass es sich dabei um zwei oder in Zukunft vielleicht mehrere sogenannte „logisch getrennte" Karten handelt, für die durchschnittliche BürgerIn ist das *eine* Plastikkarte mit *einem* Chip. Die völlig unterschiedlichen Inhalte und Funktionalitäten verschwimmen dabei und dies ist aus Sicht der NutzerInnen abzulehnen.

Auskünfte nur mehr bei Identifikation?

Ein weiteres Problem ergibt sich durch den möglichen Druck auf auskunftswillige BürgerInnen bei allen Anfragen eine Authentifizierung vorzusehen, die aber durch die Verwendung von ZMR-gestützten Zertifikaten immer auch eine Identifizierung darstellt. Damit wären dzt. zu Recht anonym in Anspruch zu nehmende öffentliche Dienstleistungen nicht mehr anonym, ja sogar personenbezogen. Wenn jetzt hinter dem zur Authentifizierung eingesetzten Zertifikat die ZMR-Zahl steht, ist auch die Pseudonymisierung verbaut. Bei Zusammenführung entsteht tatsächlich der „gläserne Bürger".

fehlender Hinweis auf unumkehrbare Identifikationsnummern

Ein weiteres Problem, welches sich aus § 13 Abs. 4a AVG ergibt ist die sogenannte verfahrensspezifische Personenkennung: „Zum Zweck der eindeutigen Identifikation von Verfahrensbeteiligten im elektronischen Verkehr mit der Behörde darf diese die ZMR-Zahl ... als Ausgangsbasis für eine verwaltungsbereichsspezifisch unterschiedliche, abgeleitete und verschlüsselte Personenkennzeichnung verwenden." Wer stellt sicher, dass jede Behörde ein eigenes Verfahren verwendet und eigenen Identifikationsnummern generiert? Vor allem fehlt aber im AVG der Hinweis, dass die Ableitung der Identifikationsnummer durch eine *unumkehrbare Funktion* zu erfolgen hat. Dies war jedoch Inhalt eines entsprechenden Beschlusses des Datenschutzrates im Zusammenhang mit der Verwendung der ZMR. Dieser Hinweis wurde nicht umgesetzt und macht ein – an sich akzeptables – System angreifbar und datenschutzrechtlich bedenklich.

Sicherstellung der Spezifität wäre wünschenswert

Wichtig erscheint auch der Hinweis, dass eine stärkere Absicherung der „Verwaltungsbereichsspezifität" wünschenswert wäre (etwa im Sinne der Formulierung: „jede Verwaltungseinheit hat eine eigene Identifikationsnummer zu generieren"). Gleiches gilt auch für die „Verfahrensspezifität" – die Identifikation darf sich nur auf ein Verfahren beziehen und keine Verknüpfung mit anderen Verfahren derselben Person bei derselben oder anderen Behörden zulassen. Andernfalls könnte aus Effizienzüberlegungen der Fall eintreten, dass in einem Bundesland oder sogar österreichweit immer dasselbe System zum Einsatz kommt und so eine Differenzierung nach unterschiedlichen Behörden oder Aktenläufen nur mehr theoretisch gegeben wäre. Wenn dann noch umkehrbare Funktionen verwendet werden, wäre eine Rückführung von der Identifikationsnummer auf die ZMR und damit auf eine Person und mehrere Verfahren möglich.

ZMR-Zahl auf e-Card eröffnet Missbrauchsmöglichkeiten

Zu bedenken ist auch die Gefahr der sukzessiven Einschränkung öffentlicher Leistungen im nicht elektronischen Weg. Das heißt der mehr oder weniger starke Zwang zur Nutzung der Karte. Besonders problematisch erscheint die Variante, dass nicht die teure, aber sichere digitale Signatur, sondern nur die ZMR-Zahl direkt zur Identifizierung verwendet wird. Dem steht zwar AVG § 13 Abs. 4a entgegen: „... Die ZMR-Zahl darf von der Behörde anlässlich der elektronischen Identifikation nicht aufgezeichnet werden." Doch allein die zu-

sätzliche Speicherung der ZMR-Zahl außerhalb des Regelkreises der Verwendung im Rahmen der meldebehördlichen Notwendigkeiten stellt ein zusätzliches Bedrohungspotential Richtung „Profiling“ dar. Besonders problematisch ist dies, da die ZMR-Zahl auf der e-Card gespeichert werden soll und damit für alle verfügbar wird.

Dies alles zusammengenommen ermöglicht die Speicherung der ZMR-Zahl auf der e-Card eine zusätzliche Datengenerierung und leichtere Auswertung und ist im Sinne der Datensparsamkeit abzulehnen.

5.4.4 Identifikation versus Authentifikation: Das Problem der Personenbindung

Personenbindung über ZMR-Zahl

Neben der oben dargestellten Problematik der Speicherung der ZMR-Zahl auf der e-Card stellt sich im aktuellen Konzept noch ein weiterer Problemkreis: die sogenannte Personenbindung. Laut Weißbuch Bürgerkarte (Posch et al. 2002, 5) soll die Personenbindung (d. h. die Verknüpfung des Zertifikats der sicheren elektronischen Signatur mit der ZMR-Zahl) bei der Registrierung der digitalen Signatur erfolgen. Gleichzeitig wird die ZMR-Zahl aber auch als „Ausgangszahl“ für die behördenspezifischen Vorgangszahlen verwendet werden. Wie oben gezeigt, sind sowohl die Sozialversicherungen verpflichtet, als auch der Innenminister ermächtigt, einen Abgleich der Daten in der Gleichsetzungstabelle durchzuführen. Damit ist es ein leichtes die ZMR-Zahl sofort auf alle e-Cards zu speichern, unabhängig davon, ob eine Nutzung im elektronischen Behördenverkehr jemals geplant ist. Hiezu fehlt eine konkrete, explizit formulierte rechtliche Schranke.

eindeutige (Personen-)Kennzahlen ermöglichen umfassende Überwachung

Dass das Problem der Personenkennzahl nicht nur im Bereich staatlicher Verwaltung auftritt zeigt die Diskussion um feststehende IP-Adressen bei der Internetnutzung und wird sich noch viel drastischer stellen, wenn die Bestrebungen zur Einführung einer UPN (Universal Personal Telecommunications Number) realisiert werden. Die Absicht hinter einer UPN ist es, eine Nummer für alle Netze/Dienste weltweit anzubieten. Die hohe Erreichbarkeit und die Bequemlichkeit, alle unterschiedlichen Dienste unter einer Nummer nutzen zu können, würde allerdings mit einer äußerst engmaschigen und individualisierten Überwachung erkauft.

negative Vorbildwirkung der öffentlichen Verwaltung

Das Grundrecht auf Schutz der Privatsphäre ist in der österreichischen Rechtsordnung festgeschrieben, daraus sollte sich zwingend ergeben, dass die öffentliche Verwaltung in ihren Verfahren jedenfalls Vorbildwirkung entfalten und dem Grundsatz von Datensparsamkeit verpflichtet sein sollte. Da jede Verwendung von personenbezogenen Daten – so sie nicht allgemein verfügbar oder auf keinen bestimmten Betroffenen rückführbar sind – einen Eingriff in das Grundrecht auf Datenschutz darstellt, ist es nur folgerichtig, dass in § 1 Abs. 2 DSG 2000 normiert wird, dass jeder Eingriff in das Grundrecht „jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden“ darf. Vor diesem Hintergrund ist zu untersuchen, ob die Personenbindung via ZMR-Zahl tatsächlich datenschutzkonform ist. Hierbei sind zwei unterschiedliche Dimensionen zu analysieren:

- Funktionaler Unterschied von Identifikation und Authentifikation
- Rechtlicher Rahmen für Digitale Signaturen.

abgestufte Authentifizierungs- und Identifizierungsstufen wären erstrebenswert

Ein Hauptargument für die Personenbindung mittels ZMR-Zahl ist die Identifikation der BürgerInnen beim Online-Kontakt mit den Behörden. Dieses Argument mag für einige Verfahren und Prozeduren richtig sein, sicherlich aber nicht für alle. Im Sinne der Datensparsamkeit müsste Vorsorge getroffen wer-

den, dass es für Prozesse des e-Government abgestufte Authentifizierungs- und Identifizierungsstufen gibt. Dies berührt die grundlegende Funktion der elektronischen Unterschrift als Unterschriftersatz. Sie ist eben nicht als Ausweis konzipiert. Während die Unterschrift (Authentifizierung) sicherstellt, dass immer dieselbe Person in einem Verfahren aktiv wird, versucht der Ausweis (Identifizierung) sicherzustellen, dass nur eine ganz bestimmte Person im Verfahren involviert ist. Dazu sind weitere Identifikationsmerkmale über Name und Vorname hinaus notwendig. Dies sind in der Regel Geburtsdatum und -ort oder auch die Wohnadresse. Wie Roßnagel (2002) anschaulich beschreibt, sind in der überwiegenden Anzahl der Fälle jedoch Name und Vorname ausreichend, um eine hinreichend sichere Zuordnung einer Person zu einem Verfahrensverlauf zu ermöglichen. Der Grundsatz „was off-line gilt, soll auch online gelten" sollte auch in diesem Zusammenhang nicht durchbrochen werden. In den klassischen Anbringen bestätigen die BürgerInnen durch ihre Unterschrift den Wahrheitsgehalt der Angaben in den Formularen, etwa Geburtsdatum, Anschrift etc. Dies könnte in e-Government Applikationen ebenfalls so erfolgen. Die eindeutige unverwechselbare Zuordnung zu einer Person ist nur dann wirklich notwendig, wenn es sich um vollautomatische Abwicklungen handelt bzw. bei automatischer Verarbeitung personenbezogener Daten. In allen anderen Verfahren können die SachbearbeiterInnen durch Nachfrage oder durch Kontextinformationen aus dem Vorgang feststellen, ob die anfragende Person mit der berechtigten identisch ist. Daraus lässt sich ableiten, dass der Unterschriftersatz sich für alle Verfahren eignet, in denen der Bürger ohnehin irgendwann in der Behörde erscheinen muss, weil er etwas vorlegen oder etwas abholen muss (vgl. Roßnagel 2002, 282).

Personenbindung unterläuft Strategien zum Schutz der Privatsphäre

Die im österreichischen Konzept vorgesehene Personenbindung, die die Zertifikate an die ZMR-Zahl bindet, verhindert, dass die BürgerInnen unterschiedliche Zertifikate nutzen und bindet eine viel größere – nicht angemessene – Anzahl von Daten in den Verarbeitungsprozess ein. Damit unterläuft das Konzept Bürgerkarte eine wesentliche Privacy-Strategie: die Pseudonymisierung – die Trennung von true-identity und online-identity. Dies ist besonders problematisch, da für alle Anwendungen dieselbe Identität Verwendung findet. Angestrebterweise soll die elektronischen Signatur der Bürgerkarte ja auch im e-Commerce verwendet werden. Gerade in diesem Bereich ist aber Identifizierung nur sehr selten notwendig – hier reicht Authentizität meist aus. Wie in Abschnitt 3 dargelegt, ist aus Datenschutzüberlegungen ja sogar Anonymität beim Einkauf zu fordern und auch realisierbar. Zu fragen bleibt darüber hinaus für welche Geschäftsfälle im e-Commerce tatsächlich eine sichere elektronische Signatur eingesetzt werden soll.[73]

Alternative: freiwilliger „elektronischer Ausweis"

Für jene Fälle im e-Government, in denen eine eindeutige Identifizierung notwendig ist, könnte ein „elektronischer Ausweis" geschaffen werden. Dieser könnte eine von einer authorisierten Behörde signierte Datei sein, die die BürgerInnen freiwillig auf ihrer Chipcard gespeichert haben und jederzeit zu ihrer eindeutigen Identifizierung selbstbestimmt in ihre aktuell signierte Willenserklärung (etwa einen Antrag) einbinden können (vgl. Roßnagel 2002, 284).

[73] Die rechtwirksame Online-Unterschrift wird wohl vor allem im Business-to-Business (B2B) Bereich eine Rolle spielen. Die Einsatznotwendigkeiten im Business-to-Consumer (B2C) Bereich werden sich auf ein sehr enges Hochpreissegment beschränken.

Abschließend ist festzuhalten, dass der rechtliche Rahmen für gültige Willenserklärungen im Online-Bereich im SigG festgesetzt wurde. Im § 8 Abs. 4 SigG. ist normiert, dass eine sichere elektronische Signatur auch dann gültig ist, wenn sie auf einem Pseudonym basiert (Brenn 1999, 89). Dies wird durch die Personenbindung eindeutig unterlaufen und somit eine wesentlicher Aspekt modernen Datenschutzpolitik den BürgerInnen vorenthalten. Das Konzept Bürgerkarte unterläuft mit diesen Vorgaben ganz bewusst diese vom SigG eingeräumten Möglichkeiten – warum?

lt. Signaturgesetz können elektronische Unterschriften auch auf Pseudonymen basieren

5.4.5 Zweckbestimmung und Datensparsamkeit: Zur Fragwürdigkeit von Info-Boxen und Multifunktionskarten

Zum Konzept Bürgerkarte gehören neben der Digitalen Signatur auch die Datenhandtaschen oder Infoboxen. Hier stellt sich die Frage wozu diese dienen sollen und welchen Effekt sie auf das Gesamtsystem haben. Als Hauptargument wird ins Treffen geführt, dass es für die BürgerInnen von Vorteil sein kann, Dokumente (Bescheide, Vollmachten etc.), die bereits elektronisch vorliegen, auf der Karte gespeichert zu haben und bei Bedarf darauf zurückgreifen zu können. Diese Entwicklung widerspricht aber den ursprünglichen Intentionen – zumindest der e-Card. Denn diese ist „in erster Linie als keycard definiert und erst in zweiter Linie Träger von spezifischen Daten“ (Mandl 2001, 211). Die Systemvariante „Schlüsselkarte“ ist auch aus Sicht des Datenschutzes vorzuziehen. Wenn es gelingt ein System aufzubauen, das es den BürgerInnen ermöglicht, bewusst den Zugriff auf Daten freizugeben, wäre dies ein wesentlicher Schritt zur Verbesserung der informationellen Selbstbestimmung.

systemfremde Funktion Datenhandtasche …

Bei der Speicherung anderer – nicht näher definierter – Daten auf der Bürgerkarte stellen sich eine Unzahl von Fragen und Problemen: Werden die KarteneignerInnen durch das Laden von Daten zu Auftraggebern im Sinne des DSG, haben sie dadurch die Verantwortung für die Zustimmung zu jeder Verarbeitung – so es sich um Daten anderer Personen handelt – und vor allem: Wie werden sie der Verantwortung gerecht werden, die sie bezüglich Datensicherheit, Datenintegrität, Verfügbarkeit und Aktualität damit übernehmen. Wie sollen die BürgerInnen dieser neuen Situation gegenübertreten? Wer lädt die Daten, wo auf die Bürgerkarte? Wie können die Betroffenen die Daten überprüfen, korrigieren und löschen. Und wie können die KarteninhaberInnen die geeigneten Datensicherheitsmaßnahmen gewährleisten? Diese Fragen sind derzeit völlig offen und doch wären sie „dringend zu klären, zumal sich daran auch allfällige Haftungsansprüche knüpfen können.“ (Souhrada-Kirchmayer 2001, 225)

… wirft Vielzahl von Problemen auf

Auch ist nicht abschließend geklärt, was in diesen Info-Boxen gespeichert werden darf. Während die Projektverantwortlichen für die Bürgerkarte eine sehr vage Vorstellung von unterschiedlichen Speichermöglichkeiten haben, verweisen DatenschutzexpertInnen darauf, dass auf der SV-Karte jedenfalls nur Daten gespeichert werden dürfen, deren Speicherung bundesgesetzlich vorgesehen ist und nicht mit dem Zweck des ELSY unvereinbar sind. Was für die Diskussion der Zulässigkeit der ZMR-Zahl auf auf der e-Card gilt, gilt umso mehr für die Dateninhalte der Info-Boxen: „Bei der Gesetzwerdung des § 31aASVG dachte man noch an Verwendungszwecke, die zumindest dem Sozialversicherungswesen angelagert sind. Nach dem Wortlaut des ASVG darf die Chipkarte daher auch auf der Basis der Freiwilligkeit nur in diesem Rahmen für weitere Zwecke herangezogen werden.“ (Souhrada-Kirchmayer 2001, 222)

Über diese rechtlichen Fragen hinaus sind aber noch andere sozio-kulturelle Fragen von großer Wichtigkeit. Insbesondere die steigende Intransparenz des Systems ist problematisch. Multifunktionskarten sind grundsätzlich bedenklich, da sie durch ihre Komplexität für die BürgerInnen undurchschaubar und kaum verstehbar sind. Deutlich wird dies etwa durch die unterschiedliche Sprache: Wenn TechnikerInnen von „logisch getrennten" Karten sprechen, meinen sie unterschiedliche Anwendungen auf ein und demselben physischen Artefakt. Technisch getrennt kann trotzdem auf derselben physischen Karte sein. In der Wahrnehmung der durchschnittlichen KarteninhaberInnen wird aber nicht zwischen den „logisch" getrennten Karten unterschieden. Eine weitere Überfrachtung zur universellen Multifunktionskarte sollte jedenfalls vermieden werden, denn ein Überfrachten mit unterschiedlichsten Funktionalitäten kann die Akzeptanz des Gesamtsystems in Frage stellen.

Zusammenfassend meint Souhrada-Kirchmayer (2001, 242): „Um nicht einen falschen Eindruck zu vermitteln, möchte ich betonen, dass der Hauptansatzpunkt bei dieser Bürgerkarte – und dieser liegt in der digitalen Signatur – keine besonderen datenschutzrechtlichen Probleme aufwerfen wird, sondern eher die weitere Verwendung der „Daten-Handtasche", insbesondere hinsichtlich der Frage was auf dieser Karte gespeichert werden darf."

5.4.6 Behörden übergreifende Vernetzung und Datenaustausch: One-Stop-Shop

mögliches Spannungsverhältnis zwischen Effizienz und Schutz der Privatsphäre

Ziel der Umgestaltungen im Rahmen der e-Government Initiativen ist einerseits eine schlankere, effizientere Verwaltung, andererseits auch eine kundenfreundlichere. Diese Orientierung wird vor allem mit dem Stichwort „One-Stop-Shop" umschrieben. Dieses Konzept bezeichnet die Möglichkeit, an einer Stelle bzw. einem Portal alle behördenrelevanten Erledigungen durchführen zu können. Je nach Ausformung des One-Stop-Shop (First-Stop, Convenience Store oder True one-stop (Kubicek und Hagen 2000, 8f)) ist eine mehr oder weniger starke Vernetzung unterschiedlicher Behörden notwendig. Auch die Zugriffsrechte der BeamtInnen sind in unterschiedlicher Weise auszugestalten. Jedenfalls tritt hier die Spannung zwischen Verwaltungsvereinfachung bzw. Effizienzsteigerung der Verwaltung einerseits und dem Grundrecht auf Schutz der Privatsphäre andererseits besonders deutlich hervor. Als Orientierung könnte etwa der Grundsatz gelten, dass Datenschutz ein Ziel demokratischer Regierungen ist, Effizienz jedoch nur eine Maßzahl wie gut eine Regierung ihre Ziele erreicht.

unterschiedliche Zugriffsrechte für Front- und Back-Office

Die Trennung von Front-Office (Annahme, Weiterleitung) und Back-Office (Bearbeitung) kann hier einen wichtigen Beitrag zu datenschutzfreundlichen Lösungen bringen. Bei der Bearbeitung im Back-Office Bereich bleibt den BeamtInnen weiterhin der (eingeschränkte) Zugriff auf jene Daten, die sie zur Erledigung ihrer Verfahren brauchen. Je stärker die Integration der Bearbeitung im Front-Office Bereich ist, umso umfassendere und damit missbrauchsanfälligere Zugriffsrechte müssen vergeben werden. Je mehr Bearbeitungen unterschiedlicher Natur in das Front-Office verlagert werden, umso wichtiger wird es, dass die BürgerInnen selbst bestimmen können, wann eine BeamtIn auf ihre Daten zugreift. Auch muss sichergestellt werden, dass der Zugriff grundsätzlich als singuläres Ereignis definiert und protokolliert wird. Eine einmalige Zustimmung zur Datenverarbeitung im Rahmen eines konkreten Verfahrens kann nicht zum Freibrief für schrankenloses Datensammeln und Verarbeiten über Behördengrenzen hinweg werden.

Zu vermeiden sind jedenfalls behördenübergreifende Vernetzungen und unkontrollierter Datenaustausch – insbesondere unter Bezugnahme auf ein eindeutiges Identifikationsmerkmal (die ZMR-Zahl). Wie eine effiziente öffentliche Verwaltung unter Nutzung neuer Informations- und Kommunikationstechnologien und der Gewährleistung des Grundrechts auf Datenschutz aussehen könnte, bedarf zusätzlicher Studien, die allerdings nicht an Effizienzüberlegungen allein ausgerichtet sein dürfen. Festzuhalten bleibt jedoch, „dass *ausgewogene* Lösungen notwendig sind: Die Vorteile neuer technisch-organisatorischer Methoden dürfen nicht mit dem Verlust an grundrechtlichem Schutz bezahlt werden." (Kotschy 2001, 102)

Effizienz nicht auf Kosten von Grundrechten

5.4.7 Sonstige sozio-ökonomische Problemfelder

Kosten für die BürgerInnen

Neben den datenschutzrechtlichen Aspekten gibt es im Zusammenhang mit der Bürgerkarte auch noch eine Reihe anderer ungelöster Fragen. Dazu gehören einerseits ökonomische Aspekte aus mikro- und makro-ökonomischer Perspektive, wie auch sozio-kulturelle Fragen der Anwendung und Akzeptanz.

Kosten für Zertifikate und …

Mit Stand April 2002 waren in Österreich fünf Zertifizierungsdiensteanbieter (Arge Daten – Österreichische Gesellschaft für Datenschutz (Verein), A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH, Datakom Austria GmbH, Generali Office-Service und Consulting AG und das Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie) aktiv (vgl. RTR GmbH 2002), von denen allerdings nur zwei auch qualifizierte Zertifikate und sichere elektronische Signaturen anbieten. Nur diese sind laut Signaturgesetz der eigenhändigen Unterschrift gleichgestellt und auch für die Verwendung auf der Bürgerkarte vorgesehen. Die nicht unerheblichen Kosten, die auf die potentiellen VerwenderInnen zukommen, reichen von € 7,20 p. a. für sogenannte Light Zertifikate zum Versenden von sicheren und vertraulichen e-Mails bis zu € 62.– p. a. für qualifizierte Zertifikate zur Erstellung sicherer elektronischer Signaturen.

… für Lesegeräte

Die Kosten für Lesegeräte sind dabei noch nicht berücksichtigt. Auch ist derzeit vollkommen offen, ob es auch Zugang über öffentliche Kioske geben wird, bzw. wie dieser gestaltet sein wird. D. h. der Einzelnen obliegt es nicht nur die Kosten für die digitale Signatur zu tragen, sondern auch die Anschaffung eines sicheren Endgerätes (Chipkartenleser) zu finanzieren. Diesen Kosten steht der derzeit unklare und nicht quantifizierbare Nutzen der online Abwicklung entgegen.

Kosten Makroebene: lange Parallelstruktur notwendig

exakte Kostenschätzungen nicht verfügbar

Wie auf der Mikro-Ebene der individuellen AnwenderInnen ist auch auf der Gesamtsystemebene die Kostenfrage weitgehend unklar. Es sind derzeit keine exakten Kostenabschätzungen verfügbar, welche Mehrkosten die Vorbereitung der e-Card für die Bürgerkarte tatsächlich verursacht. Als Kostenkategorien fallen jedenfalls die Kosten für den Chip mit größerem Speicherbedarf, die Kosten für die Systemumgestaltung sowie die nicht unwesentlichen Kosten, die dem Gesamtsystem durch die mehrmalige Verschiebung des Einsatzes der e-Card entstehen, an. Da es in der Verwaltung noch kaum wirkliche Anwendungen für e-Government unter Nutzung der elektronischen Signatur gibt, die elektronischen Formulare noch nicht einsatzfähig, die workflows in den Be-

hörden erst umzustellen sind und ohne konkrete Anwendungen kein erkennbarer Nutzen für die KonsumentInnen besteht, ist eine geringe Akzeptanz voraussagbar.

Selbst bei weiteren Verzögerungen beim flächendeckenden „Roll-out" der Karten wird sich die Situation nicht grundlegend ändern. Die Definition von workflows und die Re-Organisation des gesamten Back-Office Bereichs nehmen wesentlich mehr Zeit in Anspruch.

langsamere Einführung kann Mehrkosten verhindern

Aus dieser Situation ergibt sich die Frage, warum man nicht eine Einführungsstrategie gewählt hat, die sich zielgruppenorientiert und Schritt für Schritt den NutzerInnen nähert? Damit hätte man zumindest die durch die Bürgerkarte entstandenen Mehrkosten vermeiden können, ohne einen merklichen Nutzenverlust in Kauf nehmen zu müssen.

überschätzte Einsparungspotentiale

Weiters sind auf der Makro-Ebene die erhofften Einsparungspotentiale kurz- und mittelfristig höchst fraglich, da sich aus der geringen Verbreitung der Anwendungen und der möglicherweise nur sehr schleppenden Akzeptanz des Tokens die notwendige Doppelstruktur für elektronische und herkömmliche Anbringen und Erledigungen sehr lange aufrecht erhalten werden muss. Auch hier wird von einem Step-by-Step Approach mehr zu erwarten sein, der bei internen Workflow-Re-engineerings die online Schnittstelle zwar mitdenkt, aber nicht im Vordergrund der Entwicklung sieht.

Digital Divide

Tendenzen zur Benachteiligung von Nicht-NutzerInnen

Eines der wesentlichen sozialen Probleme rund um die Einführung der Bürgerkarte ist der sogenannte Digital Divide. Damit ist der Umstand angesprochen, dass es aus Effizienzüberlegungen zu einer Bevorzugung elektronischer Anbringen kommen wird und dass so Druck in Richtung Verwendung der Karte entstehen kann. Doch nicht nur die Bevorzugung der „Online-User" gegenüber herkömmlichen BürgerInnen steht als Problem im Raum. Kritiker meinen auch, dass es durch die Bürgerkarte zu einer Veränderung der Informationspolitik der Verwaltung kommen könnte. „Zeger hegt allerdings die Befürchtung, die Auskunftspflicht könnte durch die Einführung einer Chipcard empfindlich eingeschränkt werden. Dann nämlich, wenn die Chipcard zur Voraussetzung für die Erteilung von Auskünften avanciere." (ORF 2000)

Die Gefahr des Digital Divide wird durch die Kosten für die NutzerInnen (Gebühr für die digitale Signatur, Lesegerät, PC etc.) noch verstärkt. Fraglich ist, wie viele BürgerInnen sich diese Kosten leisten können oder wollen. Schon aus grundsätzlichen demokratiepolitischen Überlegungen ist deshalb eine aktive Strategie zur Vermeidung des Digital Divide notwendig.

5.5 Exkurs: Die „e-Card"

Aufgrund der speziellen Situation, dass in Österreich mit der Einführung der e-Card der Sozialversicherung erstmals die Chance besteht, nahezu alle BürgerInnen mit einem Trägermedium auszustatten, kann bei der Diskussion der Bürgerkarte von diesem Trägermedium nicht abstrahiert werden. Dies umso mehr, als sich aus den Erfahrungen anderer Länder zeigte, dass – wohl aufgrund fehlender Anwendungen seitens der Verwaltung – die Diffusion anderer Varianten noch längere Zeit auf sich warten lassen wird.

elektronischer Krankenschein als Ausgangspunkt

Was ist nun der Kern der e-Card? Die SV-Karte oder neu auch e-Card stellt das Produkt einer jahrelangen Diskussion um die Einführung der Chipkarte im österreichischen Gesundheitswesen dar. Ziel war die Effizienzsteigerung im Abrechnungssystem und die Umstellung auf den „elektronischen Krankenschein“. Als Nebeneffekte wurden unter anderem die Verwaltungsvereinfachung und ein Computerisierungsschub im Bereich der niedergelassenen Ärzte erwartet. Vorteile aus dem System sollten sowohl die Sozialversicherungen, die Arbeitgeber (sie ersparen sich die Verwaltung der Krankenscheinausgabe), als auch die Ärzte und die PatientInnen haben.

ursprüngliches Konzept mit wenigen gespeicherten Daten

Die grundsätzlichen Probleme beim Einsatz von Chipkarten im Gesundheitsbereich wurden bereits im Jahre 1991 dargestellt (Peissl et al. 1991). Mit der 56. ASVG Novelle wurde dann die Einführung der Chipkarte (samt notwendiger Infrastruktur – ELSY) als Krankenscheinersatz gesetzlich normiert. Zu diesem Zeitpunkt sollten folgende Daten auf der Chipkarte gespeichert werden: der Name und der akademische Grad, das Geburtsdatum, das Geschlecht, die Versicherungsnummer, die Nummer der Karte, der Nachweis eines bestehenden Versicherungsverhältnisses (Versicherungsträger, Anspruchszeit), eine eventuelle Rezeptgebührenbefreiung wegen sozialer Schutzbedürftigkeit und das Datum und die Fachgruppe des Arztes beim Erstbesuch im Quartal in verschlüsselter Form.

Administrationskarte datenschutzrechtlich unbedenklich

Mit dieser „Administrationskarte“, die sich in der Datenintegrationsdichte wesentlich von sogenannten „Gesundheitskarten“ – auf denen auch klinische Daten gespeichert werden – unterscheidet, wurde ein Kompromiss zwischen dem Wunsch nach elektronischer Abrechnung einerseits und Datenschutzüberlegungen andererseits gefunden. Schon in den Anfängen der Diskussion um die Einführung einer elektronischen Variante des Krankenscheines war es klar, dass aus technischer Sicht die Chipkartentechnologie nicht die einzig mögliche Realisierung war. Die zur Abrechnung notwendigen Daten ließen sich ebenso gut auf Magnetstreifenkarten speichern und elektronisch verarbeiten. Da das Missbrauchsrisiko der reinen Administrationsdaten als eher gering eingestuft werden kann, wäre auch aus dieser Sicht die Magnetstreifenkarte möglich gewesen. Da nun aber die Entscheidung eine Chipkarte zu wählen gefallen ist, ist es nur logisch – und war auch vorauszusehen – dass die „Möglichkeiten der Technologie genutzt werden sollten“.[74] Immerhin sind auch die Anschaffungskosten des Systems auf Chipkartenbasis wesentlich höher als in der Alternativvariante. Vor diesem Hintergrund ist die Diskussion um die „Aufwertung der e-Card zur Bürgerkarte“ zu sehen.

Die e-Card in der Form der 56.ASVG Novelle war eine klassische one-purpose-card und als solche übersichtlich, verstehbar und aus NutzerInnensicht weitgehend unproblematisch.

Erweiterung der Funktionen mit der 59. Novelle zum ASVG

Wie weiter oben dargestellt, wurde mit der 59. Novelle zum ASVG allerdings von den o.a. Prinzipien abgegangen und der Verwendungszweck der SV-Karte erweitert. Bezugnehmend auf die SV-Karte behandelt die 59. Novelle zum ASVG zwei unterschiedliche Problemkreise:

a. SV-Card als Schlüsselkarte

b. Zusätzliche Speicherung von Notfalldaten.

---

[74] Zuletzt Pumberger (freiheitlicher Gesundheitssprecher) (APA-OTS 19.4.2002): „Die Möglichkeit der freiwilligen Speicherung von Notfalldaten ist Kern der Chipkarte. Nur für den reinen Versicherungsnachweis bräuchte man kein so aufwendiges Projekt“.

zusätzliches Risiko Notfalldaten

Während die Schlüsselkarte grundsätzlich einen positiven Ansatz Richtung PET (privacy enhancing technologies) darstellt, der in der vorliegenden Version allerdings mit bedeutenden Schwachpunkten versehen ist,[75] sind die Notfalldaten nicht notwendig bzw. unklar und stellen ein zusätzliches Missbrauchsrisiko dar.

Aus Datenschutzüberlegungen sollte vom Grundsatz der Datenvermeidung ausgegangen werden. Die beiden o. a. Problemkreise erfüllen diese Grundvoraussetzungen nicht, da sie einerseits keinen erkennbaren Zusatznutzen erzeugen bzw. mehr oder spezifischere personenbezogene Daten speichern, als unbedingt notwendig.

5.5.1 Problemkreis Notfalldaten

vom Krankenscheinersatz zur Bürgerkarte

Mit der 59. ASVG Novelle und mit der Änderung des Allgemeinen Verwaltungsverfahrensgesetzes 1991 wurden die rechtlichen Möglichkeiten geschaffen, die bisher als „Krankenscheinersatz" gedachte SV-Karte zur Bürgerkarte auszubauen. Weiters wurde durch die 59. ASVG Novelle nun die Möglichkeit geschaffen auf der e-Card auch Notfalldaten zu speichern. Damit wurde ein Tor in Richtung höherer Datenintegration auf der Karte geöffnet, ohne einen wesentlichen Vorteil zu erzielen.

> *§ 31a (5): Für Zwecke der medizinischen Versorgung des Karteninhabers (der Karteninhaberin) können auf ausdrückliches Verlangen des (der) Betroffenen jene medizinischen Daten auf den innerhalb des ELSY zu verwendenden Chipkarten gespeichert werden, die für den (die) Betroffene(n) im medizinischen Notfall von entscheidender Bedeutung sind (Notfallsdaten). Zur Eintragung, Änderung und Löschung von Notfallsdaten auf den Chipkarten sind nur entsprechend geschulte Personen auf der Grundlage gesicherter medizinischer Daten berechtigt; das Auslesen der auf den Chipkarten gespeicherten Notfallsdaten ist nur unter denselben Sicherheitsbedingungen möglich, die für ELSY-Anwendungen vorgesehen sind. Das Nähere ist durch Verordnung des Bundesministers für soziale Sicherheit und Generationen zu regeln.*
>
> *(6) Das Erheben, Verlangen, Annehmen oder sonstige Verwerten von den auf den Chipkarten gespeicherten Notfallsdaten für andere Zwecke als jene der medizinischen Versorgung des Karteninhabers (der Karteninhaberin) ist verboten. Wer gegen dieses Verbot verstößt, begeht – sofern die Tat weder den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet noch nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist – eine Verwaltungsübertretung und ist von der Bezirksverwaltungsbehörde mit Geldstrafe bis zu 18 890 € zu bestrafen.*

Die Speicherung von Notfalldaten auf der e-Card ist ein besonderes Problem aus Sicht des Datenschutzes. Sie entspricht nicht den Grundsätzen von Datensparsamkeit bzw. Datenvermeidung. Sensible Gesundheitsdaten können gespeichert werden, ohne dass deren konkreter Nutzen nachvollziehbar wäre.

wenig Klarheit über Umfang von „Notfalldaten" und rechtliche Folgen

Unseres Wissens gibt es derzeit keinen in der Medizin hinreichend definierten Katalog von „Notfalldaten" (deren Fehlen in Notfällen tatsächlich Schaden oder zumindest suboptimale Behandlung begründet). Hinzu kommen hier noch die nicht geklärten technisch-organisatorischen Rahmenbedingungen und die schadenersatzrechtlichen Regelungen über Haftung bei Verwendung

[75] Details dazu im Abschnitt Identifikation versus Authentifikation: Das Problem der Personenbindung.

der auf der Karte gespeicherten Daten. Diese ist übrigens ein offener Punkt bei den „Notfalldaten“ (Im Gesetz sind zwar die „gesicherten medizinischen Daten“ vorgesehen. Befreit das den behandelnden Arzt wirklich von der Verantwortung selbst zu überprüfen (was die Speicherung der Daten unsinnig macht) bzw. von der Haftung bei Fehlern der Daten (wer haftet? Der Chiphersteller, die SV-Karten ausgebende Stelle, die schreibenden ÄrztInnen, oder die PatientIn, weil sie nicht für Aktualisierung sorgte?).

geringe Praktikabilität

Weitere grundsätzliche Bedenken betreffen den realen Einsatz der e-Card im Notfall und den Zugang zu Notfalldaten. Zum Einen besteht die Problematik der Trennung von PatientIn und Karte. Bei Unfällen kann oft nicht zweifelsfrei und schnell genug sichergestellt werden, welche Karte tatsächlich zu welchem Unfallopfer gehört. Das macht die e-Card als Notfallausweis unbrauchbar. Auch der Hinweis, für das „Auslesen der auf den Chipkarten gespeicherten Notfallsdaten ist nur unter denselben Sicherheitsbedingungen möglich, die für ELSY-Anwendungen vorgesehen sind“ deutet auf eine geringe Praktikabilität hin. Dieselben Sicherheitsbedingungen heißen „4-Augen-Prinzip und Arztkarte“. Das Einverständnis muss im Notfall vorausgesetzt werden, sobald jemand freiwillig Notfalldaten auf seiner e-Card speichern läßt. Da aber nicht davon ausgegangen werden kann, dass jede ÖsterreicherIn Notfalldaten speichern lässt, eine ÄrztIn aber in Argumentationsnotstand käme, wenn sie sich nicht vergewissert hätte, ob Notfalldaten verfügbar sind, werden wohl alle Unfallopfer, so ihnen eine e-Card zugeordnet werden kann überprüft werden – ein unnotwendiger Zeitverlust im Notfall. Das Prinzip der Arztkarte bedeutet eine eingeschränkte Verfügbarkeit der Notfalldaten nur für jene Helfer, die auch mit entsprechenden Gegenkarten, die die Leseberechtigung enthalten, ausgestattet sind. Eine weitere reale Einschränkung der Verfügbarkeit und Praktikabilität.

Neben diesen grundlegenden Bedenken gegen die Praktikabilität der Notfalldaten auf der e-Card gibt es auch noch rechtlich-soziale Bedenken: „Zur Eintragung, Änderung und Löschung von Notfallsdaten auf den Chipkarten sind nur entsprechend geschulte Personen auf der Grundlage gesicherter medizinischer Daten berechtigt“ dieser Satz schließt die Patientinnen eindeutig von der Bearbeitung ihrer höchst persönlichen Daten aus. Sie haben zwar nach § 26 DSG 2000 ein Auskunftsrecht und nach § 27 DSG 2000 ein Recht auf Richtigstellung oder Löschung, müssen sich aber jedenfalls einer „entsprechend geschulten Person“ bedienen. Dies mag aus medizinischer Sicht sinnvoll sein, weist aber den PatientInnen eine nur mittelbare Gewalt über ihre Daten zu, was wohl auch zur Folge haben wird, dass sie keine bzw. nur eine mittelbare Verantwortung für etwaige Fehleinträge bzw. fehlende Aktualisierung treffen kann.

bedenklicher aktueller Verordnungsentwurf

Abschließend sei noch auf den aktuellen Verordnungsentwurf des Gesundheitsministers verwiesen. Der nun bekannt gewordene Verordnungsentwurf zur Speicherung medizinischer Daten auf der Sozialversicherungskarte (e-card) ist aus medizinischer wie auch aus der Sicht des Schutzes der Privatsphäre äußerst bedenklich.

„Alles-oder-Nichts“ Strategie entmündigt BürgerInnen

Neben einer Fülle von Gesundheitsangaben, zu Epilepsie, Hämophilie, Hepatitis, Allergien, Asthma, Diabetes, Herzerkrankungen, Prothesen, Schrittmachern, Transplantaten und Medikamenten soll auch die Tatsache, dass jemand HIV-positiv ist, vermerkt werden. Insbesondere die „Alles-oder-Nichts“ Strategie, die es den Patientinnen verwehren soll, bestimmte Daten nicht auf der Karte zu speichern wird kritisiert (ARGE Daten 2002b). Dies wird mit der „Vollständigkeit“ argumentiert. Dies kann jedoch niemals sichergestellt werden, da ja wie oben dargestellt die grundsätzlichen Rechte auf Richtigstellung und Löschung bestehen. Zudem ist auch der Zeitpunkt der Speicherung relevant, da ja „notfallrelevante“ Umstände erst eintreten können, nachdem die Notfalldaten auf der Karte gespeichert werden.

5.6 Schlussfolgerungen

Ausgehend von den Forschungsfragen der Studie stellen sich folgende zentrale Fragen:

a. Was kann die Einzelne selbst was tun?

b. Wie steht es um freiwillige Selbstbeschränkung?

c. Wie schaut die staatliche Regulierung aus?

Alternativen nutzen

ad a) Die Antwort hier lautet eindeutig: die e-card nicht als Bürgerkarte verwenden. Obwohl elektronische Signaturen im Geschäftsverkehr für zusätzliche Sicherheit der Abwicklung sorgen werden, werden sie wohl eher im Bereich des B2B und nicht so sehr im B2C relevant sein. Für Abwicklungen die elektronische Signaturen vorsehen, sind für KonsumentInnen über weite Strecken auch einfachere und damit billigere Zertifikate ausreichend. Wo sichere Signaturen und qualifizierte Zertifikate notwendig sein werden, können diese auf Basis von Pseudonymen genutzt werden. Wie im Bereich über die Internetnutzung ausgeführt, gibt es Ansätze auch im Internethandel Anonymität sicherzustellen. Diese sind zu stärken und zu nutzen. Was die Anwendungen im e-Government betrifft, so ist von einer langen Übergangszeit und einer nur geringen Anzahl von realen Einsatzmöglichkeiten auszugehen, sodass die Kosten für eine sichere Signatur mittelfristig die zu erwartenden Nutzen weit übersteigen werden. Erste Anwendungen werden für Unternehmen und bestimmte eng umgrenzte Gruppen von BürgerInnen (zB. StudentInnen) zur Verfügung stehen. Für diese stellt sich die Frage, ob nicht eine eigene „Signaturkarte" (die dasselbe kostet wie die Signatur auf der e-Card) der bessere Weg ist. Darüber hinaus sind die Info-Boxen in ihrer rechtlichen Einordnung nicht hinreichend geklärt, was zu haftungsrelevante Fragestellungen für die BürgerInnen führen kann. Auch hier ist für die Einzelnen Skepsis angebracht.

viel ungenütztes Potential zur Selbstbeschränkung

ad b) Die Selbstbeschränkung der „Branche e-Government" könnte aus Sicht des Datenschutzes effizienter ausfallen – das Konzept Bürgerkarte könnte datenschutzfreundlicher gestaltet werden: Keine Speicherung der ZMR-Zahl auf der Karte, da diese ein sehr großes Potential zur universellen Verwendung in sich trägt (Problematik Personenkennzahl) aber auch Weglassen der verpflichtenden Personenbindung. Man sollte Möglichkeiten schaffen, die Anbringen auch mit elektronischen Signaturen lt. SigG (Pseudonyme) zuzulassen. Die zusätzliche Schaffung eines wirklich freiwilligen „elektronischen Ausweises" den die BürgerInnen bei Bedarf einsetzen oder eben auch nicht, stünde dem nicht im Wege. Ein nicht zu unterschätzendes Problem stellen auch intransparente, komplexe Multifunktionskarten dar, weshalb auch hier Beschränkung wünschenswert erscheint. Insbesondere die Private-Public-Partnership, die die Bürgerkarte gemeinsam mit der Bankomatkarte realisieren will, erscheint problematisch. Die zu enge Verbindung von hoheitlichen und privaten Aktivitäten birgt ein zusätzliches Potential zum Profiling, dem entgegenzuwirken ist.

fehlende Vorbildfunktion des Staates

ad c) Die staatliche Regulierung ist derzeit eher zersplittert, da unterschiedliche Bereiche betroffen werden. Zu überlegen wäre, ob es nicht im Sinne eines klaren, die BürgerInnen transparent informierenden Ansatzes sinnvoll wäre, einen gesetzlichen Rahmen (e-Government-Gesetz) zu formulieren, der den Staat als Vorbild heraushebt, die Prinzipien modernen Datenschutzes ernst nimmt und in den Mittelpunkt der Überlegungen stellt.

mehr Bürgerbeteiligung bei der Einführung der Bürgerkarte

Zusammenfassend ist festzuhalten, dass die Freiwilligkeit der Bürgerkarte eine notwendige aber nicht hinreichende Bedingung darstellt. Bei voller Diffusion der e-Card (99 % SV-Versicherte) kann ein hohes Maß an Druck zur Verwendung entstehen. Was den Bestrebungen insgesamt fehlt, ist eine öffentliche

Diskussion der Vor- und Nachteile des e-Government unter Einsatz der Bürgerkarte und ihrer unterschiedlichen Ausprägungen. Insbesondere die sozialen und wirtschaftlichen Folgen wären zu diskutieren. Die Bürgerkarte im Kontext e-Government ist ein techno-organisatorisches System mit einem großen Maß an Gestaltungsfreiheit und auch für den Einzelnen interessanten Aspekte, die zudem in der tagespolitischen Debatte noch nicht zu einzementierten Positionen geführt hat – ein ideales Thema für eine vorausschauende, die Wünsche und Sorgen der Betroffenen einbeziehende partizipative Technikfolgen-Abschätzung.

6 Integration der Ergebnisse – Empfehlungen

6.1 Internetnutzung

6.1.1 Aktive Datenschutzbehörde(n) und verbesserter Zugang zum Recht

Aufwertung der Datenschutzkommission

Eine der Ursachen für die faktisch geringe Wirkung der den Datenschutz betreffenden Gesetze ist in den mangelnden Kompetenzen, Verpflichtungen und Möglichkeiten der dafür sachlich zuständigen Behörden zu sehen. Für eine Aufwertung der Datenschutzkommission (DSK), die natürlich auch entsprechende personelle und materielle Ressourcen erfordert, werden folgende Maßnahmen vorgeschlagen. Erstens sollte die *Zuständigkeit der DSK auf den Privatsektor ausgedehnt werden*. Damit wird die Zuständigkeit der DSK bei Beschwerden auf Organisationen ausgeweitet, die nicht in Vollziehung der Gesetze tätig sind. Für Auskünfte ist diese Zuständigkeit bereits jetzt gegeben, eine sachlich nicht gerechtfertigte Unterscheidung zwischen Auskünften und Beschwerden, die dem Bürger den Gerichtsweg aufbürdet, um seine Rechte durchzusetzen, könnte somit überwunden werden. Diese Vorgangsweise wurde in Deutschland mit der Novellierung des Bundesdatenschutzgesetz (BDSG) gewählt, das amtliche Prüfungen der Privatwirtschaft vorsieht.

verpflichtende Prüfung im Verdachtsfall

Eine zweite vorgeschlagene Maßnahme betrifft die *Erweiterung der Prüfungspflichten*. Derzeit kann die die DSK im Fall eines begründeten Verdachtes Datenanwendungen überprüfen. Diese Kann-Bestimmung im Verdachtsfall sollte durch eine Muss-Bestimmung zu ersetzen, stichprobenartige Überprüfungen sollten auch ohne begründeten Verdacht erfolgen können.

jährliche Datenschutzberichte

Als dritter Punkt wird empfohlen, die mit dem DSG 2000 weggefallene *Berichtspflicht wiedereinzuführen*. Dem Gesetzgeber und der Öffentlichkeit ist ein Recht einzuräumen, über den Zustand des Datenschutzes in Österreich und in der Europäischen Union sowie die Tätigkeit der DSK regelmäßig informiert zu werden. Angesichts der raschen technischen und gesellschaftlichen Veränderungen ist eine jährliche Berichtslegung vorzusehen.

Weiters ist zu überprüfen, ob der Wegfall der Registrierungspflicht für Standarddatenverarbeitungen zu Verschlechterungen für den Bürger geführt hat und gegebenenfalls eine Wiedereinführung vorzusehen.

Datenschutz-Ombudsmann als zentrale Anlauf- und Informationsstelle

Für eine entscheidende Aufwertung des Datenschutzes und der DSK sollte diese einen *hauptamtlichen Datenschutz-Ombudsmann* stellen, der für individuelle Beschwerden und Anfragen zuständig ist. Ein Datenschutz-Ombudsmann kann mehrere Aufgaben erfüllen. Die Funktion selbst trägt zur öffentlichen Sichtbarkeit des Themas und damit zur Bewusstseinsschaffung bei, eine zentrale Anlauf- und Informationsstelle erleichtert den Zugang zum Recht, als Schlichtungsstelle kann sie unter Umständen zivilrechtlichen Klagen ersetzen und das damit verbundene finanzielle Risiko für die Streitparteien mindern, und sie kann mit weitergehenden Informations- und Beratungstätigkeiten über ein Internetportal verknüpft werden.

Verbesserung der rechtlichen Stellung der BürgerInnen

Um den BürgerInnen einen besseren Zugang zu ihrem Recht auf Privatsphäre zu ermöglichen, sind die *Verfahrensvorschriften* zu *ändern*. Nach geltendem Recht sind für Klagen bereits in erster Instanz die Landesgerichte zuständig. Die damit verbundene Anwaltspflicht stellt in den meisten Fällen wohl eine vollkommen unangemessene und unverständliche Hürde dar, wenn es etwa um die Löschung oder Korrektur eines Datensatzes geht.

Um das Grundrecht auf Privatsphäre in der Gesellschaft zu verankern und besser zu schützen, wird längerfristig eine *Erweiterung der Persönlichkeits- und Schadenersatzrechte notwendig* sein, die auch immaterielle Verluste durch Verletzungen der Privatsphäre zivilrechtlich einklagbar macht.

Verbesserungen sind auch *bei den Widerrufsrechten* der Konsumentinnen notwendig. Sind Daten in der Zwischenzeit weitergegeben worden, sollte das Unternehmen, welches die Weitergabe durchgeführt hat, auch zur Weiterleitung des Widerrufes verpflichtet sein; im Falle der widerrechtlichen Weitergabe sollte es für die Löschung der Daten bei den Parteien, die die Daten übernommen haben, haftbar gemacht werden können.

Grundrechte höher bewerten als kommerzielle Interessen

Rechtliche Vorkehrungen müssen getroffen werden, damit *nicht neue Unternehmensformen oder kommerzielle Interessen das Grundrecht auf Privatsphäre aushöhlen*. Viele Schutzrechte setzen bei der Weitergabe von Daten über Unternehmensgrenzen an. Im Telekommunikationsbereich gibt es eine Reihe von Unternehmen, deren Angebote von herkömmlichen Telefondiensten über Mobilkommunikation und Internetservices bis zu Pay-TV-Programmen reichen. Hier kann schon eine rein unternehmensinterne Auswertung der anfallenden Daten die Privatsphäre aushöhlen. Ähnliche Potentiale der umfassenden Profilbildung bieten Call-Centers, die für mehrere Unternehmen tätig sind. Um den Intentionen der Datenschutzgesetzgebung gerecht zu werden, ist in diesen Fällen eine Zweckbindung an das jeweilige Geschäftsfeld vorzusehen, und auch eine unternehmensinterne Datenweitergabe an eine ausdrückliche Zustimmung der betroffenen Person zu binden.

Für kommerzielle *Adressenverlage und Direktwerbeunternehmen* sieht die Gewerbeordnung Erleichterungen vor, die dem Zweck der Geschäftstätigkeit entsprechen. Diese dürfen aber nicht dazu führen, dass kommerzielle Interessen höhere Wertigkeit als Grundrechte erhalten. Die diskutierten Vorschläge, Adressverlagen den Zukauf von Mitgliederlisten von Vereinen und NGOs zu erlauben, ist strikt abzulehnen. Laut geltender Gewerbeordnung dürfen Daten, welche die rassische Herkunft, politische Anschauungen oder religiöse oder andere Überzeugungen erkennen lassen, nicht ohne ausdrückliche schriftliche Zustimmung ermittelt, verarbeitet und übermittelt werden. Die Mitgliedschaft in Vereinen oder bei NGOs lässt aber oft direkt auf solche personenbezogene Daten schließen.

6.1.2 Bewusstseinsschaffung und Selbstregulierung

klassische Formen der Aufklärung

Als klassische Formen der Aufklärung und Bewusstseinsschaffung ist eine verpflichtende Einbindung der Datenschutzproblematik in den (Informatik)-Unterricht einzuführen, weiters ist zielgruppenspezifisches Informationsmaterial in Form von Broschüren und multimedialen Datenträgern sowie durch ein thematisch konzentriertes Webportal bereitzustellen. Diesem Internetportal ist besondere Vertrauenswürdigkeit zu verleihen, indem die DSK bzw. der Datenschutzombudsmann als Betreiber fungiert. Die inhaltliche Gestaltung ist durch ein Gremium zu kontrollieren, das Interessensvertreter und NutzerInnenvereinigungen einschließt. Mit diesen Maßnahmen allein kann man aber nur einen Teil der Bevölkerung erreichen. Personen, die das Bildungssystem bereits durchlaufen haben oder nicht ein Mindestmaß an Grundsensibilisierung aufweisen, bleiben davon ausgeschlossen.

verpflichtende Warnhinweise mit Kontaktinformationen zum „Datenschutz-Ombudsmann“

Es ist daher eine zentrale Forderung, durch einen allgemeinen Gefahrenhinweis in der Art *„Die Nutzung neuer Informations- und Kommunikationsmedien kann Ihre Privatsphäre gefährden“* zur Sensibilisierung in der breiten Bevölkerung beizutragen. Diese Warnung hat Kontaktinformation zum Datenschutz-Ombudsmann zu beinhalten, bei der die Konsumentinnen weitere Informationen einholen können. Dieser Warnhinweis ist verpflichtend auf schriftlichen und elektronischen Informations- und Werbematerial von Telekommunikationsbetreibern und Internetprovidern, insbesondere auch auf deren Rechnungen anzubringen. Gemäß Telekommunikationsgesetz haben die Betreiber in jenen Fällen, in denen ein „besonderes Risiko der Verletzung der Vertraulichkeit besteht, die Teilnehmer über dieses Risiko und über mögliche Abhilfen einschließlich deren Kosten zu unterrichten.“[76]

Anreicherung des e-Commerce-Gütesiegels um datenschutzspezifische Elemente

Gütesiegel sind ein wichtiges Instrument der Selbstregulierung, indem sie eine freiwillige Selbstbeschränkung publik und überprüfbar machen. Grundsätzlich wäre ein Datenschutzgütesiegel wünschenswert, allerdings nur, wenn es gelingt, dieses auf EU-Ebene zu etablieren, um einen Wildwuchs konkurrierender Siegel zu vermeiden. Unmittelbar wird vorgeschlagen, das österreichische e-Commerce-Gütesiegel um weitere datenschutzspezifische Elemente anzureichern und die ebenfalls bereits laufenden Bemühungen, es auf EU-Ebene zu etablieren, zu forcieren. Eine zusätzliche Bestimmung zum Datenschutz, die die Träger dieses Gütesiegels zu erfüllen haben, ist die Verwendung von Cookies nur bei Einverständnis des Konsumenten und unter Aufklärung des Verwendungszweckes, diese Forderung ist in der zukünftigen Neufassung der der EU-Richtlinie 97/66 bereits integriert. Weitere Elemente sind ein grundsätzlicher Verzicht auf unbemerkte Datensammlung durch Webbugs und eine Publikationspflicht der Datenschutzpolitik in maschinenlesbarer Form gemäß dem P3P-Standard.

6.1.3 PETs – Datenschutz durch Technik

Angesichts des enormen Überwachungspotentials, das neue Informations- und Kommunikationstechnologien in sich bergen, und das mit mobilen Diensten um die Dimension von exakten Bewegungsprofilen erweitert wird, sind technische Vorkehrungen zum Schutz der Privatsphäre unvermeidlich.

Zertifizierung von PETs

Die technischen Konzepte sind entwickelt, und in den meisten Fällen sind Dienste und Tools auch vorhanden, die den Konsumentinnen eine anonyme Nutzung ermöglichen oder sie vor unbemerkten Datensammlungen bewahren können. Die angeboten Dienste und Programme sind aber von sehr unterschiedlicher Wirksamkeit und Benutzerfreundlichkeit. Um die Nutzung auch für NichtexpertInnen zu öffnen, sind glaubwürdige Institutionen notwendig, die Zertifikate nach der Vertrauenswürdigkeit, dem Grad der Anonymität sowie vor allem auch hinsichtlich Benutzerfreundlichkeit und Alltagstauglichkeit überprüfen. Diese Funktion soll der neu zu schaffende Datenschutzombudsmann bzw. das an ihn geknüpfte Internetportal übernehmen. Diese Informationen sind laufend zu aktualisieren und die Kriterien der Zertifizierung offen zu legen. Für die Durchführung der Tests ist eine Lösung im Verbund der europäischen Datenschutzbehörden anzustreben, um die notwendigen Ressourcen für eine umfassende und aktuelle Hilfestellung für die KonsumentInnen sicherzustellen. Diese Stelle sollte ihre Erfahrungen auch den EntwicklerInnen von PETs zur Verfügung stellen und Konzepte für größere Benutzerfreundlichkeit und deren Integration in Standardsoftware entwickeln.

---

[76] Telekommunikationsgesetz – TKG 97, § 90 (2).

Unterstützung von Anonymisierungsdiensten

Anonymisierungsdienste sind oft durch mangelnde Kontinuität gekennzeichnet. Der Datenschutz-Ombudsmann sollte Konzepte entwickeln, bei denen Interessensvertretungen und andere vertrauenswürdigen Organisation gemeinsam solche Dienste anbieten. Der Ombudsmann sollte auch dafür bürgen, dass Konzepte realisiert werden, die bei normaler Nutzung die Anonymität garantieren, bei kriminellen Aktivitäten aber eine Aufdeckung im Einzelfall erlauben.

gesetzliche Verankerung der Datenvermeidung durch Technik

Datenvermeidung ist grundsätzlich effizienter als der Schutz vor missbräuchlicher Verwendung oder unbefugter Weitergabe. PETs können dazu eingesetzt werden, dass Dienste nur von befugten Personen in Anspruch genommen werden können, ohne dass dazu eine persönliche Identifizierung notwendig ist. Um die Datenvermeidung mittels PET-Unterstützung zu fördern, ist eine Ergänzung der Datenschutzgesetze um einen entsprechenden Passus vorzunehmen. Diese Ergänzung soll in Analogie zu den entsprechenden Vorschriften bei der Datensicherheit vorschreiben, dass „unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit“[77] entsprechende Vorkehrungen getroffen werden. Ein entsprechender Passus ist in das deutsche Teledienstedatenschutzgesetzes (TDDSG) integriert und ein zentrales Anliegen bei der Gleichbehandlung von Transaktionen in der Offline-Welt und bei der Nutzung elektronischer Kommunikationsformen. Neben gesetzlichen Verpflichtungen ist auf die Vorbildwirkung von öffentlichen Informations- und Transaktionswirkungen bei der Implementierung von datensparenden Technologien zu forcieren. Die Beachtung dieses Prinzips bei den laufenden e-Government-Aktivitäten würde zudem helfen, eine wichtige Diffusionsbarriere zu überwinden.

6.2 Data Mining

6.2.1 Staatliche Regulierung

effektivere Durchsetzung geltender Bestimmungen

Die wichtigsten Empfehlungen im Bereich Gesetzgebung und Gesetzesvollzug betreffen auch im Bereich „Data Mining“ Maßnahmen, die auf eine effektivere Durchsetzung geltenden Rechts abzielen. Viele der Vorschläge zum Thema Internetnutzung lassen sich daher unverändert auf diesen Bereich übertragen. Zu diesen Empfehlungen zählen die im Abschnitt 6.1.1 näher ausgeführten Punkte, insbesondere die Vorschläge *„Ausdehnung der Zuständigkeit der DSK auf den Privatsektor“*, die *„Erweiterung der Prüfungspflichten“* oder die Etablierung eines *„hauptamtlichen Datenschutz-Ombudsmannes“* als Ansprechpartner für betroffene KonsumentInnen scheinen auch für eine Verbesserung des Schutzes der Privatsphäre gegen unrechtmäßige Data Mining Anwendungen unverzichtbar zu sein.

rechtliche Klärung des „Data Mining“

Neue Techniken der Datenanalyse bringen aber natürlich auch einen Bedarf an Adaptionen und Präzisierungen von geltenden Regelungen mit sich. Eine notwendige Präzisierung betrifft den Vorgang des Data Minings selbst. Data Mining kann sowohl als Zweck einer Erhebung angesehen werden, wenn etwa Daten erhoben oder in Warehouses gespeichert werden, um sie dieser Art von Analyse zu unterziehen, aber auch als Verarbeitung, wenn der Zweck des Data Mining etwa in der Verbesserung der eigenen Marketing liegt. Im ersten Fall ist nach gängiger Rechtsauffassung mangels spezifizierten Zweckes die Verarbeitung personenbezogener Daten rechtswidrig, im zweiten Fall sehr

[77] DSG 2000, § 14 (1).

wohl zulässig. Objektiv besteht aber bei der Durchführung und bei den möglichen Resultaten zwischen beiden Fällen keinerlei Unterschied, und es obliegt einzig dem Unternehmen, zwischen den Alternativen zu wählen.

Gefahr der Aushöhlung von Schutzniveaus durch Konzentrations- oder Auslagerungsprozesse

Die Regulierung hat auch dafür zu sorgen, dass durch Konzentrations- oder Auslagerungsprozesse keine Aushöhlung der Rechte auf Privatsphäre auftreten kann. Zu diesem Zweck müssen getrennte Geschäftsfelder in einem Unternehmen, wie etwa Festnetz-, Mobil- und Internetdienste aus einer Hand, auch hinsichtlich der Datensammlung und Auswertung getrennt bleiben. Ebenso müssen Unternehmen, die datenschutzrelevante Leistungen für mehrere andere Unternehmen erbringen, dazu verpflichtet werden, keine übergreifenden Auswertungen vorzunehmen.

6.2.2 Selbstregulierung bzw. freiwillige Beschränkungen

Anreize zur Selbstregulierung schaffen

In Analogie zu den Empfehlungen zum Bereich Selbstregulierung bei Internetnutzung gilt auch hier, dass einerseits bewusste KonsumentInnen und andererseits ein Staat, der bereit ist, gesetzlichen Normen Nachdruck zu verleihen und bei einer Missachtung von Grundrechten entsprechende Schritte zu setzen, Grundvorrausetzungen für „freiwillige" Maßnahmen von Unternehmen sind. Als überwiegend unternehmensinterner Prozess mit wenig Sichtbarkeit nach außen und entsprechend eingeschränkter Kontrollierbarkeit ist ein faires Verhalten von Unternehmen notwendig, um die Privatsphäre der KonsumentInnen zu schützen.

Leitlinien fairen Verhaltens definieren

Eine wesentliche Aufgabe der Politik muss die Entwicklung von Leitlinien sein, an denen sich ein fairer und datenschutzkonformer Einsatz des Data Mining zu orientieren hat. Das DSG 2000 hat in § 6 Abs. 4[78] ein Verfahren zur Generierung von Verhaltensregeln für einzelne Bereiche des privaten Sektors. Die Empfehlung für die Politik lautet, für den Bereich Data Mining entsprechende Regeln zu entwickeln und zu veröffentlichen. Um die Anreize für Unternehmen zu erhöhen, sich an diese Leitlinien zu halten, sind sie in datenschutzgerechte Gütesiegel zu integrieren.

6.3 Bürgerkarte

6.3.1 Freiwilligkeit

tatsächliche Freiwilligkeit auf allen Ebenen

Die e-Card wird an alle sozialversicherten ÖsterreicherInnen ausgegeben. In der Grundform der Administrationskarte sind auf ihr keine sensiblen Daten gespeichert, weshalb auch die flächendeckende Verbreitung kaum datenschutzrechtliche Bedenken hervorruft. Wesentlich wird aber die Forderung nach tatsächlicher Freiwilligkeit, sobald mehr als die Verwaltungs- und Stammdaten gespeichert werden. Sowohl die Speicherung der Notfalldaten, wie auch die

[78] „Zur näheren Festlegung dessen, was in einzelnen Bereichen als Verwendung von Daten nach Treu und Glauben anzusehen ist, können für den privaten Bereich die gesetzlichen Interessenvertretungen, sonstige Berufsverbände und vergleichbare Einrichtungen Verhaltensregeln ausarbeiten. Solche Verhaltensregeln dürfen nur veröffentlicht werden, nachdem sie dem Bundeskanzler zur Begutachtung vorgelegt wurden und dieser ihre Übereinstimmung mit den Bestimmungen dieses Bundesgesetzes begutachtet und als gegeben erachtet hat."

zur Identifizierung herangezogene ZMR-Zahl und eine mögliche elektronische Signatur müssen absolut freiwillig erfolgen. Zu fragen bleibt, wie diese Freiwilligkeit durchsetzbar ist. Allein die mögliche Speicherung medizinischer Daten kann für die Versicherten eine zusätzliche Verantwortung bedeuten und so die Freiwilligkeit einschränken. Notwendig wäre hier eine gesetzliche Normierung, damit aus dem Fehlen von (Notfall-)Daten auf der e-Card den BesitzerInnen kein wie immer gearteter Schaden erwächst. Auch die gesetzliche Normierung des nicht-diskriminierenden Zugangs zu öffentlichen Leistungen erscheint notwendig, da sonst aufgrund des Effizienzgebotes die Gefahr besteht, dass BürgerInnen, die die Bürgerkarte nicht nutzen wollen oder können, nur mehr eingeschränkt Zugang zu Leistungen der öffentlichen Hand haben.

Zur Freiwilligkeit gehört auch die Wahlmöglichkeit für die KonsumentInnen zu entscheiden, welchen Signaturbetreiber und vor allem auch welchen Token (welche Karte) sie einsetzen wollen. All dies sollte verbindlicher als im Weißbuch Bürgerkarte festgeschrieben werden.

6.3.2 Restriktive Anwendung der Identifikation

strenge Prüfung der Notwendigkeit einer Identifikation

Besonderes Anliegen muss es sein, die Personenbindung nur sehr eingeschränkt einzusetzen. Dazu ist es notwendig, bei allen angebotenen Online-Transaktionen vorerst zu prüfen, ob eine Authentifikation ausreichend erscheint. In den meisten Fällen müsste eine elektronische Signatur nach dem SigG (auch möglich unter Benutzung von Pseudonymen) ausreichend sein. Zu fordern ist auch die Trennung von Zertifikat und Personenbindung. Wo unbedingt erforderlich, könnte ein elektronischer Ausweis auf freiwilliger Basis eingeführt werden.

Verzicht auf generelle Speicherung der ZMR-Zahl auf der Chipkarte

Besondere Vorsicht ist bei der Verwendung der ZMR-Zahl geboten, da sie ein hohes Potential zur allgemeinen Verwendung (Personenkennzahl) in sich birgt und damit auch ein hohes Missbrauchspotential darstellt. Deshalb sollte die ZMR-Zahl nicht auf der e-Card gespeichert werden.

unumkehrbare Funktionen bei der verfahrensspezifischen Kennung

Sicherzustellen ist weiters, dass nur unumkehrbare Algorithmen zur Ableitung der „verfahrensspezifischen“ Kennung herangezogen werden. Dies deshalb, damit ausgeschlossen werden kann, dass Profile und Querverbindungen über Aktivitäten Einzelner über Verfahrens- oder Behördengrenzen hinaus möglich werden.

Insgesamt erscheint die Einführung einer digitale Signatur für e-Government Anwendungen ein richtiger Schritt und diskussionswürdig. Diese digitale Signatur muss aber nicht notwendigerweise auf der e-Card realisiert werden.

6.3.3 Keine Vermischung mit anderen Funktionen/Karten

Beschränkung der Multifunktionalität

Multifunktionskarten sind aus Sicht der Nutzerinnen grundsätzlich bedenklich, da sie eine hohe Komplexität aufweisen, für die Nutzerinnen undurchschaubar und kaum verstehbar sind. Aufgrund dieser mangelnden Transparenz für die BürgerInnen können sehr leicht Akzeptanzprobleme des Gesamtsystems auftreten.

keine Datenhandtaschen

Die vorgesehenen Datenhandtaschen bzw. Info-Boxen sind abzulehnen. Sie widersprechen dem Prinzip der Datenvermeidung, ihre Sinnhaftigkeit ist bisher nicht geklärt (sie sind nicht klar genug definiert) und außerdem ist eine Reihe von Fragen bezüglich der Verantwortung für die darauf gespeicherten Daten weitgehend ungeklärt.

keine Notfalldaten

Auf der e-Card sind die Notfalldaten abzulehnen. Sie haben keinen bzw. nur unklaren klinischen Mehrwert bei bestehendem Risikopotential. Das widerspricht dem Grundsatz der Datensparsamkeit. Zudem sind bestens bewährte Alternativen vorhanden.

Nutzung unterschiedlicher Identitäten fördern

Insgesamt ist den one-purpose cards der Vorzug zu geben. Dabei kommt es nicht zur Vermischung der Anwendungsfelder. Insbesondere die einheitliche Signatur für e-Government und e-Commerce erscheint fragwürdig. In einer zunehmend vernetzten Welt macht es Sinn, für unterschiedliche Rollen der Einzelnen unterschiedliche Signaturen und elektronische Identitäten zu verwenden. Die sollte über die Verwendung von unterschiedlichen Attributen bei ein und demselben Zertifikat hinausgehen.

6.3.4 Bedarfsorientiertes Vorgehen

schrittweise Einführung nach konkretem Bedarf

Da derzeit noch die Anwendungen im e-Government fehlen, ist der Nutzen für die BürgerInnen unklar. Damit ist vorauszusehen, dass sie die Mehrkosten auf individueller Ebene nicht zu tragen bereit sein werden und dass der umfangreiche Mehraufwand für die e-Card keine Entsprechung in der Nutzung durch die Bürgerinnen finden wird. Sinnvoller erscheint hier ein bedarfsorientiertes Vorgehen indem man Nutzerinnen, die sehr bald von konkreten Anwendungen profitieren werden können, die digitale Signatur anbietet. Dadurch könnte man Mehrkosten einsparen.

keine Einschränkung bei Offline-Diensten

Besonders wichtig erscheinen in dieser Hinsicht auch Maßnahmen gegen den „digital divide“. Darunter versteht man die Gefahr, dass Dienste möglicherweise nur mehr elektronisch und nach „Ausweisleistung“ angeboten werden. Hier sollte unbedingt darauf geachtet werden, was offline anonym verfügbar ist, sollte dies auch online sein. Zudem besteht noch eine ökonomische Barriere, da die Kosten für die digitale Signatur und die Lesegeräte für viele ein Problem darstellen.

Einbindung der BügerInnen in die Systemgestaltung

Insgesamt bedürfte es einer breiten öffentliche Diskussion des Gesamtsystems e-Government unter Einbindung der Bürgerkarte. Eine frühe Einbindung aller Betroffenen könnte einen teuren Flop vermeiden helfen. Durch Einsatz von Methoden der partizipativen Technikfolgen-Abschätzung wäre es möglich, Gestaltungsvarianten auszuloten und zu einer sozialverträglicher Gestaltung des Gesamtsystems zu kommen.

7 Abkürzungen und Glossar[79]

ChipCard: ..... Eine Karte – meist in der Größe von Kreditkarten – mit einem eingebetteten Mikroprozessor (auch Smartcard genannt).

Data Mining:..... *"'Data Mining' or Knowledge Discovery in Databases (KDD) as it is also known, is the nontrivial extraction of implicit, previously unknown, and potentially useful information from data. This encompasses a number of different technical approaches, such as clustering, data summarization, learning classification rules, finding dependency net works, analysing changes, and detecting anomalies"*. (William J Frawley, Gregory Piatetsky-Shapiro and Christopher J Matheus)[80]

Digitale Signatur:..... siehe Elektronische Signatur

DSK..... Datenschutzkommission

Elektronische Signatur:.. Elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und zur Authentifizierung im Onlineverkehr verwendet werden. Geregelt im Signaturgesetz (SigG)

GnuPG..... GnuPG ist ein freier Ersatz für PGP

IP-Adressen ..... Die IP-Adresse identifiziert Rechner im Internet. IP ist die Abkürzung für Internet Protocol. Derzeit besteht eine IP-Adresse (noch) aus vier Bytes.

P3P ..... Abkürzung für „Platform for Privacy Preferences"

PETs ..... Abkürzung für Privacy Enhancing Technologies

PGP ..... Pretty Good Privacy, ein weit verbreitetes Verschlüsselungsprogramm

PKI: ..... Abkürzung für Public Key Infrastructure

PKZ: ..... Abkürzung für Personenkennzahl: Als Personenkennzahl wird eine Identifikationsnummer für Individuen üblicherweise dann bezeichnet, wenn diese (eindeutige) Identifikationsnummer unabhängig vom Sachbereich, flächendeckend in einer Gesellschaft zur Idenditfikation von Personen verwendet wird (Kotschy 2001, S 100 FN21)

Port..... Englische Bezeichnung für Schnittstelle, Verbindungsmöglichkeit des PCs mit Peripheriegeräten

Posting..... Abgeleitet vom Englischen to post (hinterlegen) beschreibt dieser Begriff das Absenden und Veröffentlichen eines Artikels/einer News in einer Newsgroup.

---

[79] Dieses Verzeichnis wurde teilweise mit Unterstützung des Internet-Glossars GLOSSAR.de erstellt. http://www.myglossar.de/glossar/index.htm.

[80] Quelle: Queen's University of Belfast, *What is Data Mining?*, http://www.pcc.qub.ac.uk/tec/courses/datamining/stu_notes/dm_book_2.html#HEADING2.

Proxy ..... ‚Proxy' bedeutet soviel wie ‚Stellvertreterdienst'. Proxies nehmen Anforderungen von einem Client (z. B. einem WWW-Browser) entgegen und geben sie, gegebenenfalls modifiziert, an das ursprüngliche Ziel (z. B. eine WWW-Site) weiter.

SSL ..... Abkürzung für „Secure Socket Layer". Technik, mittels der ein Web-Client den Server authentifizieren kann und der Datenverkehr zwischen beiden verschlüsselt wird.

8 Literatur

ARGE Daten, 2002a, *BM Gehrer plant Missbrauch der Volkszählungsdaten*; [Aufgerufen am: 02-07-14] <http://www.argedaten.at/news/20011001.html>.

ARGE Daten, 2002b, *e-card wird zum HIV-Ausweis*; [Aufgerufen am: 02-07-14] <http://www.ad.or.at/news/pw20020426.html#3>.

BKA, 2001, *Aktionsplan eEurope 2002 – Maßnahmenkatalog Umsetzung in Österreich*, Stand: 31.1.2001, Wien: BUNDESKANZLERAMT – Wirtschaftliche Koordination, <http://www.austria.gv.at/regierung/AP01.pdf>.

Brenn, C., 1999, *Signaturgesetz*; in Reihe: Manzsche Gesetzausgaben, Bd. Sondausgabe 101, Wien: Manzsche Verlags- und Universitätsbuchhandlung.

Čas, J., Peissl, W. (Institut für Technikfolgen-Abschätzung, Österreichische Akademie der Wissenschaften), 2000, Beeinträchtigung der Privatsphäre in Österreich, im Auftrag von: Bundeskammer für Arbeiter und Angestellte, Oktober 2000, Wien: Institut für Technikfolgen-Abschätzung, <http://www.oeaw.ac.at/ita/ebene5/d2-2a24a.pdf>.

Cavoukian, A., 1998, Data mining: Staking a Claim on Your Privacy; <http://www.ipc.on.ca/english/pubpres/papers/datamine.htm>.

Chaum, D. L., 1981, Untraceable Electronic Mail, Return addresses, and Digital Pseudonyms, *Communications of the ACM 24(2)* <http://www.eskimo.com/~weidai/mix-net.txt>.

Eckhardt, A., Fattebert, S., Keel, A., Meyer, P. (Basler & Hofmann, Z., Institut romand d'éthique, U. d. G.), 2000, *Der gläserne Kunde. Elektronische Erfassung und Auswertung von Kundendaten*, im Auftrag von: Technologiefolgen-Abschätzung, Z. f., Nr. TA 38/2000, November 2000, Bern: <http://www.ta-swiss.ch/www-remain/reports_archive/publications/2000/38_TA_Bericht_Glaeserne_Kunden.pdf>.

Entschließung der Konferenz der Datenschutzbeauftragten, 2000, Data Warehouse, Data Mining und Datenschutz, *59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder*, 14./15. März 2000, Hannover <http://www.datenschutz-berlin.de/doc/de/konf/59/datawa.htm>.

Europäisches Parlament und der Rat, 1995, Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, *Amtsblatt nr. L 281 23/11/1995*, 0031 – 0050 <http://europa.eu.int/eur-lex/de/lif/dat/1995/de_395L0046.html>.

Europäisches Parlament und der Rat, 1995, Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, *Amtsblatt nr. L 281 23/11/1995*, 0031 – 0050 <http://europa.eu.int/eur-lex/de/lif/dat/1995/de_395L0046.html>.

Europäisches Parlament und der Rat, 1997, 395L0046 *Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation* (24. Oktober 1995). Amtsblatt nr. L 24/1 (30. Januar 1998) <http://europa.eu.int/eur-lex/pri/de/oj/dat/1998/l_024/l_02419980130de00010008.pdf>.

Fox, D., 1995, Automatische Autogramme. Mit digitalen Signaturen von der Datei zur Urkunde, *c't – Magazin für Computer und Technik (10/95)* <http://www.ix.de/ct/Artikel/CT9510/Retorte.htm>.

Hassler, V., 2000, Europäische Aspekte – eEurope Smart Card Charta, *Zusammenfassender Bericht „Forum Bürgerkarte"*, 13.12.200, Wien <http://www.buergerkarte.at>.

Hes, R., Borking, J. J., Netherlands. Registratiekamer., Information and Privacy Commissioner/Ontario., 1998, *Privacy-enhancing technologies: the path to anonymity*; in Reihe: Achtergrondstudies en verkenningen; 11, Rev. Aufl., The Hague: Registratiekamer.

Ian Goldberg, D. W., Eric Brewer, 1997, *Privacy-enhancing technologies for the Internet*, Berkeley: University of California <http://www.cs.berkeley.edu/~daw/papers/privacy-compcon97-www/privacy-html.html>.

Kotschy, W., 2001, Grundrechte und staatliche EDV-Register, in: Österreichische Juristenkommisssion (ÖJK) (Hg.): *Grundrechte in der Informationsgesellschaft – 24.-26. Mai Weißenbach am Attersee*, Wien: Neuer wissenschaftlicher Verlag, 88–102.

Kubicek, H., Hagen, M., 2000, One-Stop-Government in Europe: An Overview, in: Kubicek, H., Hagen, M. (Hg.): *One-Stop-Government in Europe: Results from 11 national surveys*, Bremen: University of Bremen, 1–36.

Mandl, A., 2001, SV-Chipkarte, in: Österreichische Juristenkommisssion (ÖJK) (Hg.): *Grundrechte in der Informationsgesellschaft – 24.-26. Mai Weißenbach am Attersee*, Wien: Neuer wissenschaftlicher Verlag, 211–213.

OECD, 1980, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 23 September 1980 <http://www1.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM>.

ORF, 2000, *Protest gegen Pläne zur „Bürgerkarte"*; [Aufgerufen am: 21. November 2001] <http://futurezone.orf.at/futurezone.orf?read=detail&id= 48947&tmp=27252>.

Peissl, W., Tschakalov, O., Wild, C. (Forschungsstelle für Technikbewertung der Österreichischen Akademie der Wissenschaften (FTB)), 1991, *Die möglichen Folgen einer Einführung der Medcard in Österreich, Teil A, Endbericht*, im Auftrag von: BMGSK, Jänner 1991, Wien.

Petrak, J., 1997, *Data Mining – Methoden und Anwendungen*, Nr. TR-97-15, Wien: Österreichisches Forschungsinstitut für Artificial Intelligence, Christian Doppler Labor für Expertensysteme <http://www.ai.univie.ac.at/oefai/ml/kdd/tr-kdd.html>.

Posch, R., 2001a, *Bürgerkarte – elektronischer Ausweis im Netz*; [Aufgerufen am: 02-05-09] <http://www.buergerkarte.at/Buergerkarte.htm>.

Posch, R., 2001b, *Bürgerkarte – Wie geht es weiter?*; [Aufgerufen am: 02-05-09] <http://www.buergerkarte.at/wie_geht_es_weiter.htm>.

Posch, R., 2002, eGovernment und elektronische Signatur aus Bundessicht, *Österreichische Gemeindezeitung (2/2002)*, 27–33.

Posch, R., Karlinger, G., Konrad, D., Leiningen-Westerburg, A., Menzel, T., 2002, *Weißbuch Bürgerkarte*, im Auftrag von: BmöLS, Mai 2002, Wien: Zentrum für sichere Informationstechnologie Austria (A-SIT) <http://www.buergerkarte.at>.

Posch, R., Leitold, H., 2001, *Weißbuch Bürgerkarte*, im Auftrag von: BmöLS, Juni 2001, Wien: A-Sit Zentrum für sichere Informationstechnologie Austria <http://www.buergerkarte.at>.

Roßnagel, A., 2002, Der elektronische Ausweis – Notwendige und mögliche Identifizierung im E-Government, *DuD 26 (5)*, 281–285.

Roßnagel, A., Pfitzmann, A., Garstka, H., 2001, *Modernisierung des Datenschutzrechts* Bundesministerium des Innern.

RTR GmbH, 2002, *Liste der Zertifizierungsdiensteanbieter*; [Aufgerufen am: 02-05-09] <http://www.signatur.rtr.at/de/providers/providers.html>.

Souhrada-Kirchmayer, E., 2001, Die Bürgerkarte im Lichte der Informationsgrundrechte, in: Österreichische Juristenkommisssion (ÖJK) (Hg.): *Grundrechte in der Informationsgesellschaft – 24.-26. Mai Weißenbach am Attersee*, Wien: Neuer wissenschaftlicher Verlag, 218–225, 242.

Statistik Austria, 2001, *E-Commerce 2000/2001. Ergebnisse der Ersten Europäischen Piloterhebung*; Schnellbericht 11.1, im Auftrag von: Bundesministerium für Wirtschaft und Arbeit und EUROSTAT, Wien.