ISSN 0938-3476

Z 7625 F

Chipkarten

März 1996

1/96

Die Freiheit nehm' ich mir...

F.I.F.F.Kommunikation

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. 13. Jahrgang 1995 • Einzelpreis: 6 DM

Inhalt

EDITORIAL

AKTUELL

CHIPKARTEN

FIFF e.V.

RUBRIKEN

Inge Allinger, Roland Käser, Michael Müller, Claus Stark

Chipkarten

Nehmen sie die Gesellschaft in ihre Fänge?

Gestern noch waren die Einsätze bei der Informatik begrenzt: Sie waren kommerzieller, industrieller oder militärischer Natur. Von nun an nimmt die Informatik, da sie sich in eine unendliche Vielzahl kleiner Maschinen auflöst und hinter einem Netz unbegrenzter Verästelungen verschwindet, die ganze Gesellschaft in ihre Fänge.

Simon Nora und Alain Minc, „Die Informatisierung der Gesellschaft", Frankfurt/New York, 1979

Chipkarten, diese kleinen Informatik-Maschinen, erobern die Welt im leisen Sturm, durch sie wird Informationsgesellschaft erst möglich! Eine gewagte These? Sicherlich - aber das BMFT wies bereits 1994 darauf hin, daß Chipkarten einen hohen Stellenwert für die Informationsgesellschaft besäßen, dessen Marktpotential heute deutlich unterschätzt werde. Das Geschäft mit den vielfältigen Anwendungen stehe vor einer „Explosion" - wahrscheinlich ist diese Einschätzung nicht übertrieben. Ulrich Lange von der Forschungsgruppe Telekommunikation der FU Berlin 1994 auf der MultiCard-Tagung: „Kein technisches System wird uns in Zukunft so nahe sein wie die Chipkarte, die ich schon heute als Telefonkarte in meiner Brieftasche (am Herzen) trage, und keine Datentechnik verkörpert die Forderung nach 'selbstbestimmter Technikverwendung' so wie dieser Minicomputer im Scheckkartenformat."

Mini-PCs im Scheckkartenformat - diese Charakterisierung macht deutlich, worin der Unterschied der Chipkarte zu den vielen anderen maschinenlesbaren Karten - von der Prägekarte bis zur Magnetstreifenkarte - liegt: Sie besitzt eine eigene „Intelligenz" und macht somit Anwendungen denkbar, die sonst unmöglich zu realisieren wären. Die ersten Vorläufer dieser neuen Technologie wirkten dabei noch relativ primitiv und harmlos: Die Krankenversichertenkarte hat fast jeder von uns, ebenfalls die Telefonkarte - was ist eine Chipkarte mehr als „ein Stück Plastik mit etwas Elektronik"? Die deutschen Sparkassen wollen Ende 1996 die multifunktionale Karte einführen. Die Volks- und Raiffeisenbanken wollen 1997 mit einer „elektronischen Geldbörse" nachziehen, mit der man im Bus oder am Zigarettenautomat ohne Bargeld bezahlen kann. Krankenkassen, Ärzte- und Apothekerverbände wetteifern seit 1993 darum, die „echte" Patientenchipkarte (die endlich (!) auch medizinische Diagnosen, Medikationen und Risikofaktoren enthalten soll) unter das Volk zu bringen. Sehr viele Anwendungsfelder in den unterschiedlichsten gesellschaftlichen Bereichen sind denkbar und einige werden in diesem Heft diskutiert.

Was interessant ist an der aktuellen Diskussion: Chipkarten würden endlich das leidige „Datenschutzproblem" ein für alle mal lösen - sie verkörperten regelrecht in idealer Weise den Grundsatz der informationellen Selbstbestimmung. Wie das gemeint sein kann, wird im Beitrag von Klaus Pommerening deutlich: Sie sollen das quasi-anonyme, aber dennoch rechtsverbindliche Agieren unter Pseudonym ermöglichen. Diese neuen Möglichkeiten von Chipkarten - Pseudonyme sind dabei nur eine unter vielen - bedürfen dringend der offenen und breiten gesellschaftlichen Bewertung! Sind sie wirklich so sozialverträglich und datenschutzfreundlich, wie sie scheinen? Deshalb sei dieser Beitrag besonders hervorgehoben und zur (Pflicht-)Lektüre empfohlen - mit solchen Fragen sieht sich das FIFF in Zukunft konfrontiert.

Die weiteren Beiträge in diesem Heft beweisen, wie weit die Entwicklung in Sachen Chipkarten bereits gediehen ist: Mit Bürgerkarten sollen die Bürger wieder Souverän ihrer eigenen Daten werden (Steffen Stripp). Elektronisches Geld wird durch Chipkarten erst denkbar (Matthias Schunter und Arnd Weber). Und Kranken könne dank Patientenchipkarte optimal geholfen werden (Tien Nguyen N.). Aber: Wird die Einführung eines elektronischen Gesundheitspasses zur Prävention von Krankheiten und in der Gesundheitserziehung ganz automatisch ein gesundes Volk hevorbringen (Thomas Elkeles und Rolf Rosenbrock)? Gibt es Alternativen zur elektronischen Krankenakte (Hans-Jürgen Jonas)? Wie ist die Patientenkarte politisch zu bewerten (Steindor)? Ist vielleicht sogar die aktive Mitwirkung von Patienten- und Bürgergruppen an Karten-Modellprojekten denkbar (Michael Möhring)? Das könnte ein wichtiger Beitrag zur Gestaltung der „Informationsgesellschaft von unten" sein.

Aber nicht nur im Gesundheitswesen werden kritische Stimmen laut: Führt die Anwendung von Chipkarten bei der Abwicklung des Asylverfahrens nicht zum Gläsernen Flüchtling (Thilo Weichert)? Wer wird von den sogenannten StudiCards an den Hochschulen profitieren (Jens Woinowski)? Und wird nicht die gerade stattfindene Umstellung der Karten im österreichischen Bankenwesen von Magnetstreifen auf Chip geradewegs in den Überwachungsstaat führen (Karl Kollmann und Christian Reiser)? Hier wird wieder deutlich, daß auch bei der Einführung von kleinen, unscheinbaren Plastikkärtchen ernstzunehmende Probleme auftauchen. Chipkarten sind auf breiter Front, aber eben unauffällig, im Kommen. Die Verbreitung verschiedenster Prozessor- und Kryptochipkarten kann als die bisher größte (Voll-)Computerisierung der Gesellschaft begriffen werden! Und was von einigen lediglich als Übergangsphänomen auf dem Weg in die vernetzte Gesellschaft beurteilt wird, wird von anderen als nichts Geringeres als der Generalschlüssel dazu begriffen: Ohne Chipkarten keine rechtsverbindlichen Telekommunikationsakte - und damit auch keine Informationsgesellschaft. Falls es dazu kommen sollte, ist eines klar: Die dafür benötige Sicherheitsinfrastruktur wird gewaltig sein.

Die breite und offene gesellschaftliche Diskussion über den Sinn und Unsinn von Chipkartenanwendungen findet in Deutschland (noch) nicht statt. Kritiker und Protagonisten schlagen zwar mit Worten aufeinander ein, der Erkenntnisgewinn aus diesem Streit ist aber gering. Sind gesellschaftlich wünschenswerte Anwendungen denkbar, die außerhalb aller Kritik stehen? Und ist es ebenfalls denkbar, daß mit dem gleichen gesellschaftlichen Konsens gewisse Chipkartenanwendungen eben *nicht* realisiert werden? Wir sollten uns die Zeit nehmen, intensiver darüber nachzudenken. Sönke Jahn hat im SchlußpFIFF die chipkartengestützte Zukunft für uns etwas vorgedacht! ■

FIFF... Presseerklärung vom 2.3.1996

zum Entwurf eines Telekommunikationsgesetzes (TKG), Bundestagsdrucksache 13/3609 vom 30.01.1996

DER VOM BUNDESKABINETT beschlossene Entwurf des Telekommunikationsgesetzes (TKG-E) wurde als Gesetzesentwurf der Fraktionen der CDU/CSU, SPD und F.D.P. in den Deutschen Bundestag eingebracht. Hierdurch wird das Gesetzgebungsverfahren beschleunigt, so daß die Zeit für Stellungnahmen verkürzt wird.

Es ist zwar begrüßenswert, daß „die Wahrung der Interessen der Nutzer auf dem Gebiet der Telekommunikation und des Funkwesens sowie die Wahrung des Fernmeldegeheimnisses" (TKG-E § 2 Abs. 2 Nr. 1) als erstes von fünf Zielen der Regulierung der Telekommunikation genannt wird. Gleichwohl wird der Entwurf diesem Ziel nicht gerecht.

Weiterhin ist zwar positiv hervorzuheben, daß in § 3 TKG-E klare Begrifflichkeiten für den geregelten Bereich geschaffen werden und somit viele der Diskussionen, wie sie z.B. bei der Anwendbarkeit des Fernemeldeanlagengesetzes auf private, nicht gewerblich betriebene Mailboxen, vermieden werden. Leider wird diese klare Begrifflichkeit nicht konsequent durchgehalten.

Wie schon bei der Kritik am Entwurf einer Telekommunikationsdienstunternehmen-Datenschutzverordnung (siehe rechts) gilt auch beim TKG-E, daß die datenschutzrechtlichen Regelungen grundsätzlich in das Gestz selbst aufgenommen werden und nicht einer Verordnung vorbehalten werden sollten. Die gegenüber dem Entwurf der TDSV angebrachte Kritik gilt auch dem TKG-Entwurf.

Beim vorliegendem Gesetzentwurf sind noch eine Reihe - nicht nur datenschutzrechtlicher - Verbesserungen erforderlich:

A) informationspolitische Aspekte

Im Gesetzentwurf wurde es versäumt die Weichen für den Weg in eine sozialverträgliche Informationsgesellschaft zu stellen.

Statt den Gemeinden, ähnlich wie in des USA erfolgreich praktiziert, das Recht zu geben, die TK-Dienstleister verpflichten zu können, als Gegenleistung für die Nutzung der Straßen und Wege für deren Netze Schulen und andere öffentliche Einrichtungen kostenlos oder zumindest zu besonders günstigen Konditionen an die jeweiligen Netze anzuschließen, wird den TK-Dienstleistern die kostenfreie Nutzung der Straßen und Wege zum Verlegen ihrer Netze eingeräumt. Ein Möglichkeit der sozialen Verpflichtung wurde damit aus der Hand gegeben.

Die Regelungen für die Universaldienstleistungen, zu denen alle NutzerInnen „unabhängig von ihrem Wohn- und Geschäftsort zu einem erschwinglichen Preis Zugang haben müssen" (aus TKG-E § 16 Abs. 1), sind völlig unzureichend. So sollte bereits jetzt der ISDN-Standardanschluß als Universaldienstleistung festgelegt werden. Breitbandige Anschlüsse sind dann als Universaldienstletisung zu definieren, sobald die Nutzung dieser Dienste für eine gleichberechtigte Teilhabe an der Gesellschaft erforderlich ist. Nur so kann vermieden werden, daß bereits über die Finanzierbarkeit der Zugänge die Informationsgesellschaft in „information rich" und „information poor" aufgeteilt wird.

Aufgrund der im Entwurf enthaltenen Regelungen kann es passieren, daß z.B. ein auschließlich in einer Region tätiges Unternehmen dort zwar eine Monopolstellung hat, aber nicht zum Anbieten von den Universaldienstleistungen verpflichtet werden kann, da es bundesweit nicht über einen Marktanteil von 5% verfügt. Umgekehrt kann ein bundesweit marktbeherrschendes Unternehmen nur in den Regionen zum Anbieten von Universaldienstleistungen verpflichtet werden, in denen es selbst eine marktbeherrschene Stellung hat.

B) datenschutzrechtliche Aspekte

1) Die Wahrung des Rechts auf informationelle Selbstbestimmung sollte in den Katalog der Regulierungsziele (§ 2 TKG-E) aufgenommen werden.

2) In § 82 wird das Fernmeldegeheimnis geregelt. Abs. 2 besagt, daß zur Wahrung des Fernmeldegehimnisses verpflichtet ist

   „wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt".

   Die hier verwendeten Begriffe stehen außerhalb der Systematik des restlichen Gesetezentwurfes und sind nur unter Hinzuziehung der Begründung des Gesetzesentwurfes zu verstehen. Daher sollte Abs. 2 Satz 1 wie im Refentenentwurf vom 06. Oktober und auch noch von 22. November 1995 gefaßt werden:

   „zur Wahrung des Fernmeldegeheimnisses ist verpflichtet, wer eine nicht ausschließlich für eigene Telekommunikationszwecke bestimmte Telekommunikationsanlage betreibt, beaufsichtigt, bedient oder sonst bei Ihrem Betrieb tätig ist, sowie wer Telekommunikationsdienstleistungen erbringt oder daran mitwirkt."

3) § 12 Abs. 1 und 2 verpflichten Lizenznehmer, die Sprachkommunikationsdienstleistungen für die Öffentlichkeit anbieten, ihre Teilnehmerdaten anderen Lizenznehmern und sonstigen Dritten weiterzugeben zur Aufnahme eines Auskunftsdienstes oder der Herausgabe von „Verzeichnissen der Rufnummern der Teilnehmer in kundengerechter Form". Hier ist der Hinweis auf die anzuwendenen datenschutzrechtlichen Regelungen unzureichend (vgl. auch Nr. 4).

4) Grundsätzlich ist zu bemängeln, daß die datenschutzrechtlichen Bestimmungen im TKG-E nicht abschließend geregelt sind, sondern durch § 86 TKG-E einer Rechtsverordnung der Bundesregierung vorbehalten sind. Eingriffe

in das Recht auf informationelle Selbstbestimmung und die Beschränkung dieser Eingriffsmöglichkeiten sollten grundsätzlich in einer dem gesetzgebungsverfahren unterliegenden Rechtsquelle enthalten sein. Der in § 86 TKG-E enthaltene Rahmen für eine solche Rechtsverordnung ist zu vage. Der Inhalt der ebenfalls von der Bundesregierung im Entwurf vorgelegten Telekommunikationsdienstunternehmen-Datenschutzverordnung (TDSV) sollte unter Berücksichtigung der Änderungsvorschläge der Datenschutzbeauftragten direkt in das Gesetz aufgenommen werden. In der jetzigen Regelung ist noch nicht einmal sichergestellt, daß der Bundesbeauftragte und die Landesbeauftragten für den Datenschutz an der Erstellung dieser Rechtsverordnung beteiligt werden.

§ 86 Abs. 7 verweist auf einen Abs. 2 Satz 2, den es in der vorliegenden Fassung in diesem § nicht gibt.

5) Einer selbstständigen und unabhängigen Datenschutzkontrolle im liberalisierten Telekommunikationsmarkt ist eine große Bedeutung beizumessen. Anders als in § 87 TKG-E vorgesehen sollte diese Aufgabe dem Bundesbeauftragten für den Datenschutz nur dann übertragen werden, wenn lizenzpflichtige Dienstleistungen in mehr als einem Bundesland angeboten werden. Im übrigen sollte es bei den gegenwärtigen Zuständigenkeiten der Landesbeauftragten für den Datenschutz (z.B. im Bereich kommunaler TK-Netze) und der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich bleiben.

6) Eine weitere Verschlechterung des Datenschutzstandards könnte sich durch den § 87 TKG-E ergeben, der die Auskunftsersuchen der Sicherheitsbehörden betrifft. Die Vorschrift regelt den Zugriff der Regulierungsbehörde auf die Kundendateien aller Unternehmen, die Telekommunikationsdienstleistungen anbieten. Im Bezug auf die Daten der Kunden ist das Verfahren bedenklich, da es einen jederzeitigen Zugriff der Regulierungsbehörde auf die Datensätze ohne Zweckbindung ermöglich. Zudem soll der Zugriff den betroffenen Unternehmen verborgen bleiben. Damit besteht die Möglichkeit, daß die Regulierungsbehörde jederzeit über die vollständigen Kundendateien aller Telekommunikationsunternehmen verfügt, ohne daß diese davon Kenntnis haben.

7) Nach §§ 84 und 86 gelten die Anforderungen an technische Vorkehrungen, die u.a. dem Schutz des Fernmeldegeheimnisses und personenbezogener Daten dienen, sowie die zu erlassende Rechtsverordnung zum Datenschutz nur für Anbieter von Telekommunikationsdienstleistungen. Enstprechend der Definition aus § 3 Nr. 15 „sind Telekommunikationsdienstleistungen das gewerbliche Angebot von Telekommunikation einschließlich des Angebot von Übertragungswegen für Dritte". Somit gelten die Regelungen nur für gewerbliche Anbieter

   Die Regelungen für die technische Umsetzung von Überwachungsmaßnahmen durch die Sicherheitsbehörden gelten im Gegensatz dazu nach § 85 Abs. 4 für jeden „Betreiber einer Telekommunikationsanlage, der anderen den Zugang zu seiner Telekommunikationsanlage geschäftsmäßig überläßt". Entsprechend der Begründung § 82 Abs.2 TKG-E ist geschäftsmäßig nicht mit gewerblich gleich zu setzen. So erbringt „geschäftsmäßig Telekommunikationsdienste" „auch (wer) ein ohne Gewinnerzielungsabsicht erfolgendes, auf Dauer angelegtes Angebot von Telekommunikationsdiensten" anbietet. D.h. z.B., daß fast alle privaten, nichtgewerblichen MailboxbetreiberInnen unter diese Regelung fallen.

Weitere Möglichkeiten der datenschutzgerechten Gestaltung wurden im TKG-E nicht berücksichtigt. Dazu gehört die von den Datenschutzbeauftragten angeregte Möglichkeit, die Dienstleistungsanbieter zum Angebot von Zahlungssystemen zu verpflichten. ■

Presseerklärung

zum Entwurf einer Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (Telekommunikationsdienstunternehmen-Datenschutzverordnung, TDSV),

Stand: 05. Januar 1996

DIE BUNDESREGIERUNG erarbeit z. Zt. die Telekommunikationsdienstleistungsunternehmen-Datenschutzverordnung, die die bisherigen TDSV und UDSV ersetzen sollen.

Neben der grundsätzlichen Kritik, daß die datenschutzrechtlichen Regelungen der Telekommunikation per Gesetz und nicht nur per Verordnung geregelt werden sollten, um den Schutz des Rechts auf informationelle Selbstbestimmung gerecht zu werden, gibt es weitere wesentliche Kritikpunkte an dem Verordnungsentwurf:

- Der Entwurf der TDSV (TDSV-E) sieht vor, daß künftig ein Einzelverbindungsnachweis mit vollständiger Rufnummernerfassung angeboten werden kann. Dies ist ein schwerwiegender Eingriff in das Recht auf informationelle Selbstbestimmung der angerufenen TeilnehmerInnen (B-TeilnehmerInnen). Ein solcher Eingriff bedürfe zumindest eines Gesetzes. Zudem widerspricht diese Regelung dem rechtskräftigen Urteil des Oberverwaltungsgerichts Bremen, das eine Speicherung der vollständigen Rufnummer nur für maximal vier Tage ab Gesprächsdatum für gerechtfertig hält.
- Die Stellen, die beantragen können, daß bei ihnen die Anzeige der Rufnummer der Anrufenden nicht erfolgt und bei denen dies auch im Telefonbuch eingetragen wird, wurde drastisch eingeschränkt. Insbesondere viele freie Beratungsstellen und Einrichtungen werden nicht mehr hierunter fallen.
- Es ist zwar zu begrüßen, daß künftig den KundInnen das Recht eingeräumt wird, zu wählen, ob sie in keinem Verzeichnis, nur in gedruckten Verzeichnissen oder auch in elektronischen Verzeichnissen aufgeführt werden wollen. Allerdings ist die hier vorgesehene Widerspruchsregelung nicht ausreichend, nur bei ausdrücklicher Zustimmung sollten KundInnen in das elektronische Verzeichnis aufgenommen werden. ■

Stefan Walz

EU-Datenschutzrichtlinie jetzt in Kraft

Die Konsequenzen

1. Anpassung erfordert Novellierung des BDSG

Die Datenschutzrichtlinie der Europäischen Union ist fünf Jahre nach Vorlage des Erstentwurfs im Oktober 1995 - endlich - in Kraft getreten und im Amtsblatt der EG veröffentlicht worden (Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, Abl. der EG, L 281, S. 31 ff.). Zwischen der Verabschiedung des sogenannten „Gemeinsamen Standpunkts" am 20.02.1995 bis zur endgültigen Annahme des Textes im EU-Ministerrat am 24.07. 1995 gab es noch einzelne kleinere Korrekturen im Wortlaut und in den Erwägungsgründen aufgrund von Änderungswünschen aus der 2. Lesung im Europäischen Parlament am 15.06.1995. Von Bedeutung ist allerdings die in der Schlußversion enthaltene Abschwächung der Durchführungsbefugnisse der EU-Kommission.

Die Frist für die Mitgliedstaaten zur Anpassung ihres einzelstaatlichen Datenschutzrechts an die Richtlinie beträgt drei Jahre. Diese Zeit bis zum Herbst 1998 muß intensiv genutzt und mit den Vorarbeiten muß umgehend begonnen werden, wenn man bedenkt, daß die letzte Reform des Bundesdatenschutzgesetzes mehr als vier Jahre gedauert hat. Hinzu kommt, daß ja nicht nur das Bundesrecht, sondern auch die Landesdatenschutzgesetze mit den Vorgaben der EG in Einklang zu bringen sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat aus diesem Zeitdruck die Konsequenzen gezogen und beschlossen, Eckpunkte für die Änderung des BDSG schon auf ihrer 51. Konferenz im März 1996 vorzulegen. Zu den vorrangigen Forderungen gehört dabei vor allem, die Anknüpfung an den überholten Begriff der „Datei" aufzugeben und die Restriktionen für die Datenschutz-Kontrolle im nicht-öffentlichen Bereich wegfallen zu lassen. Auch der sogenannte Düsseldorfer Kreis, das Gremium der obersten Aufsichtsbehörden für die Datenschutz in der Privatwirtschaft, will bereits frühzeitig über den Anpassungsbedarf diskutieren.

2. Chance für die Modernisierung des Datenschutzrechts

Für die Datenschutzbeauftragten geht es dabei um mehr als nur um durch das neue Gemeinschaftsrecht erzwungene Minimalkorrekturen, um mehr als den buchhalterischen Abgleich zwischen den deutschen Gesetzestexten und den europäischen Formulierungen. Eine BDSG-Novellierung, die in zwei oder drei Jahren in Kraft tritt, kann die rapide Veränderung der Informations- und Kommunikationstechnik und die seit Inkrafttreten des zweiten BDSG vor fünf Jahren deutlich gewordenen Regelungsdefizite nicht außer acht lassen.

Anders ausgedrückt: Das Gebot der Anpassung der deutschen Rechtslage an die EU-Richtlinie muß als Chance wahrgenommen werden, das Datenschutzrecht in unserem Land von veralteten Konzepten zu entrümpeln und Regelungserfordernissen der von „Multimedia" geprägten Zukunft gerecht zu werden. Nur mit dieser doppelten Zielsetzung, d. h. Anpassung „an Europa" und Modernisierung in Richtung auf die Informationsgesellschaft, kann das Datenschutzrecht auch am Ende dieses Jahrzehnts seine Schutzrolle für das informationelle Selbstbestimmungsrecht der Bürger erfüllen.

Meine Vorstellungen von den neuen Herausforderungen von "Multimedia" und weltweiter Vernetzung für den Datenschutz und den sich daraus ergebenden Ansätzen für ein neues Datenschutzkonzept kann ich an dieser Stelle aus Raumgründen nicht wiedergeben. Ich habe sie in meinem Beitrag zum Schwerpunktheft Multimedia der Zeitschrift WECHSELWIRKUNG zusammengefaßt (Ausgabe Febr./ März 1996, S. 26 ff.).

3. Weiterentwicklung des Datenschutzes auf Gemeinschaftsebene

Die verabschiedete Richtlinie stellt jedoch nur einen Zwischenschritt dar. Für eine konsequente Weiterentwicklung des Schutzes von Individualität und Privatsphäre in der europäischen Union bedarf es weiterer Maßnahmen:

- Das Recht auf Achtung der Privatsphäre, im deutschen Verständnis das Recht auf informationelle Selbstbestimmung, gehört in einem Europa, das grenzüberschreitende Datenflüsse multipliziert und transeuropäische Datennetze aufbaut, in den Grundrechtskatalog einer geschriebenen EU-Verfassung.
- Die Institutionen und Organe der EG, die zunehmend in ihren eigenen Computern persönliche Daten der Gemeinschaftsbürger sammeln und auswerten (z. B. in den Bereichen Statistik, Fond-Verwaltung und Bekämpfung des Subventionsbetrugs), müssen sich selbst dem Datenschutz-Regime unterwerfen, das die Richtlinie für die Behörden und Unternehmen in den Mitgliedstaaten vorschreibt.
- Gleiches gilt für die Kontrolle: Die dann geltenden Regelungen für die Brüsseler und Luxemburger Behörden müssen von einem in den Gemeinschaftsverträgen abgesicherten, unabhängigen Datenschutzbeauftragten kontrolliert werden.

Diese drei Kernforderungen hat die Europäische Datenschutzkonferenz im September 1995 auf Vorschlag der deutschen Delegation beschlossen. Die deutsche Datenschutzkonferenz hat diese Petita in ihrer Entschließung im November 1995 in Bremerhaven bekräftigt (vgl. den Text im 18. Jahresbericht des Bremischen Landesbeauftragten für den Datenschutz; erscheint 4/96).

Die Reaktionen aus Brüssel zu diesen letzteren beiden, seit langem bekannten Forderungen waren jedoch bisher mehr als zögerlich - weder beim behördeninternen Datenschutz noch bei der Bestellung eines Beauftragten sind bisher nennenswerte Fortschritte erzielt worden. Die EU-Organe müssen sich allerdings darüber klar sein, daß „hausinterne" Organisationsregelungen zum Datenschutz, wie sie in Form eines Rundschreibens des Generalsekretärs für die Kommission seit 1995 existieren, nicht mehr ausreichen. Vielmehr kann die Übermittlung personenbezogener Daten von nationalen Behörden an die Dienststellen der Gemeinschaft für den Fall, daß keine speziellen Rechtsgrundlagen die Weitergabe vorschreibt, gefährdet sein, wenn letztere nicht über eine den Mitgliedstaaten äquivalenten Datenschutz-Standard verfügen. Nur ein solcher einzelstaatlicher Druck auf Brüssel war es auch, der seinerzeit zur Verabschiedung der EG-Statistik-Verordnung geführt hat, die das Statistikgeheimnis beim Europäischen Amt in Luxemburg sicherstellen soll.

4. Konzertation durch Datenschutzgruppe

Die Richtlinie setzt in Art. 29 eine Arbeitsgruppe ein. Sie wird u. a. die Umsetzung in das einzelstaatliche Recht überwachen und sich bei Zweifelsfragen der Interpretation einschalten. Darüber hinaus hat die Kommission alle Regelungsprojekte der EU mit Datenschutzbezug dieser Gruppe zur Stellungnahme vorzulegen. Diesem Gremium wird es auch obliegen, in Zweifelsfällen oder bei Beurteilungsdivergenzen das Datenschutzniveau in Staaten außerhalb der Gemeinschaft, in die personenbezogene Angaben „exportiert" werden sollen, auf seine Vergleichbarkeit mit dem nach der Richtlinie verbindlichen gemeinschaftsweiten Standard zu überprüfen.

Die Gruppe nach Art. 29 hat sich am 17.01.1996 vorläufig konstituiert; die Verabschiedung der Geschäftsordnung und die Wahl des Vorsitzenden werden erst auf der nächsten Sitzung im Mai stattfinden. In diesem Organ sind alle Mitgliedstaaten mit ihren unabhängigen Datenschutzbehörden vertreten. Deutschland wird voraussichtlich zumindest vertreten werden durch den Bundesbeauftragten und einen Landesbeauftragten für den Datenschutz.

Wie die föderale Struktur und Kompetenzverteilung der deutschen Datenschutzkontrolle im öffentlichen bzw. im nicht-öffentlichen Bereich bei der Vertretung und der konkreten Arbeit in dieser Gruppe abgebildet werden kann, steht noch nicht endgültig fest. Die Datenschutzbeauftragten werden darüber für ihren Bereich im Frühjahr entscheiden.

Stefan Walz, Landesbeauftragter für den Datenschutz, Bremen. ■

Schwerpunkt: Chipkarten

Die Autorinnen und Autoren:

Thomas Elkeles
ist Projektgruppenleiter bei Epidemiologische Forschung Berlin (EFB).

Sönke Jahn
ist Redakteur beim Mac Magazin, Hamburg.

Hans-Jürgen Jonas
ist Sonderpädagoge und freier Mitarbeiter im Gesundheitsladen Köln.

Karl Kollmann
ist Dozent am Institut für Technologie und Warenwirtschaftslehre der Wirtschaftsuniversität Wien und stv. Abteilungsleiter Konsumentenpolitik in der Kammer für Arbeiter und Angestellte in Wien.

Michael Möhring
ist wissenschaftlicher Mitarbeiter am Institut für Sozialwissenschaftliche Informatik der Universität Koblenz-Landau.

Tien Nguyen N.
ist Health Research Coordinator am CITA Forschungsinstitut der Universität Namur/Belgien.

Klaus Pommerening
ist Professor für Mathematik und arbeitet am Institut für Medizinische Statistik und Dokumentation der Johannes-Gutenberg-Universität Mainz. Er leitet die GMDS-Arbeitsgruppe „Datenschutz in Krankenhausinformationssystemen".

Christian Reiser
ist Diplomingenieur der Informatik und Doktor technicae der Technischen Universität Wien.

Rolf Rosenbrock
ist Leiter der Arbeitsgruppe Public Health des Wissenschaftszentrums Berlin für Sozialforschung (WZB).

Matthias Schunter
ist wissenschaftlicher Mitarbeiter am Institut für Informatik der Universität Hildesheim.

Marina Steindor
(MdB) ist gesundheitspolitische Sprecherin der Bundestagsfraktion von Bündnis 90/Die Grünen.

Steffen Stripp
ist Mitarbeiter am Danish Board of Technology in Kopenhagen und hat 1994 die Konsensuskonferenz zur Bürgerchipkarte durchgeführt. Er ist unabhängiger Berater im Bereich Computer-Ethik und Mitglied des Danish Governments IT-Security Advisory Board.

Arnd Weber
ist wissenschaftlicher Mitarbeiter am Institut für Sozialforschung der Universität Frankfurt/Main. Er beschäftigt sich mit der Genese der Public-Key-Kryptographie und den Auswirkungen elektronischer Zahlungsverfahren im Rahmen von DfG- und EU-Projekten.

Thilo Weichert
ist Referent beim Niedersächsischen Landesbeauftragten für den Datenschutz und Vorsitzender der Deutschen Vereinigung für Datenschutz (DVD).

Jens Woinowski
studiert Informatik und Philosophie an der TH Darmstadt und hat den Arbeitskreis „Chipkarten" auf der KIF 95 in Hamburg mitorganisiert.

Klaus Pommerening

Chipkarten und Pseudonyme

Ich sage dir: Verwisch die Spuren!
B. Brecht, Aus dem Lesebuch für Städtebewohner

Chipkarten erzeugen Datenspuren

Stellen Sie sich vor, Sie gehen ins Kaufhaus einkaufen. Für die Bezahlung legen Sie ihre Kundenkarte ins Lesegerät, der Computer liest die Kundennummer ab und verknüpft sie mit Name und Kontonummer. Das Kaufhaus rechnet die Kaufsumme mit der Bank ab. Diese Transaktion hinterläßt Spuren. Das Kaufhaus kann ein „Kundenprofil" erstellen, die Bank erfährt, wo und wann Sie wieviel einkaufen.

Stellen Sie sich vor, sie fahren auf der Autobahn der Zukunft, natürlich gebührenpflichtig. An den Kontrollpunkten wird Ihre Chipkarte per Funk automatisch ausgewertet, damit die Gebühren von Ihrem Konto abgebucht werden können. (Dieses Verfahren wurde ernsthaft diskutiert; im Moment scheint es nicht durchsetzbar zu sein.) Wer die Daten hat, kann feststellen, wo Sie überall waren und wann. „Bewegungsprofil" nennt man das.

Stellen Sie sich vor, Sie gehen mit Ihrer Krankenversichertenkarte zum Arzt. Mit deren Hilfe wird eine Datenspur erzeugt, denn Diagnose- und Therapiedaten werden maschinenlesbar an die Krankenkasse übermittelt - im Widerspruch zum Datenschutzgedanken, aber mit ausdrücklicher Billigung des Gesetzgebers. Die Krankenkasse sammelt auf diese Weise ein „Patientenprofil" von jedem ihrer Mitglieder. Das ist im übrigen nicht Zukunft, sondern Gegenwart.

In vielen Bereichen wird die Einführung von elektronischen Ausweisen angedacht oder geplant - als Sicherheitsausweise für den Zugang zu Informationssystemen, als Berechtigungsausweise für die Ausübung eines Berufs ('Professional Card'), als elektronische Geldbörsen, Elektronische Ausweise sind so praktisch und effizient, auch für den Besitzer. Aber sie hinterlassen Datenspuren. Die Datenspuren werden dabei nicht speziell durch die Chipkarten verursacht - jede Art von maschinenlesbaren Karten wirkt genauso. Chipkarten zeichnen sich aber durch besondere Fälschungssicherheit aus; die auf Chipkarten mögliche Sicherheitstechnik scheint die Verbreitung elektronischer Ausweise wesentlich zu fördern.

Pseudonyme verwischen Datenspuren

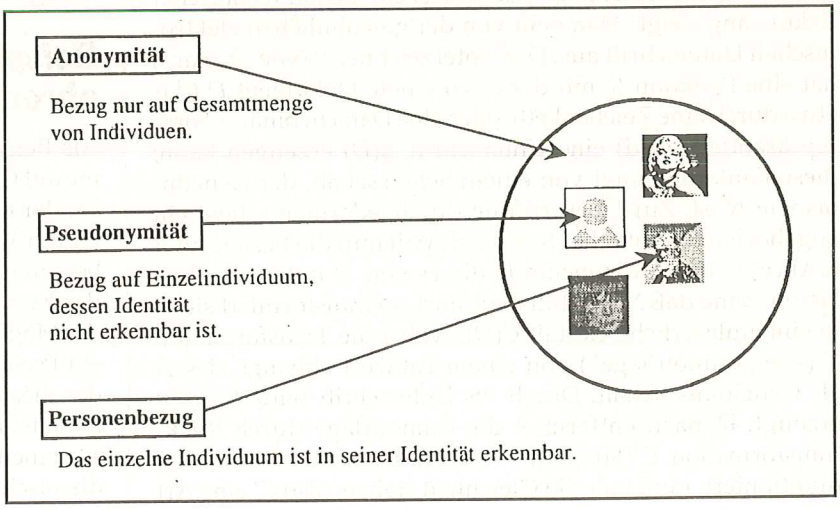
Aber müssen die unbestrittenen Vorteile der Chipkarte wirklich mit einem Totalangriff auf das Grundrecht der informationellen Selbstbestimmung erkauft werden? Es wird z. B. argumentiert, daß die Krankenkassen, um die Kosten des Gesundheitssystems in den Griff zu bekommen, personenbezogene Auswertungen vornehmen müssen - im Interesse der Patienten! Aber brauchen sie dazu wirklich den vollen Personenbezug mit Namen und Adresse und und und ...? Bei der statistischen Auswertung irgendwelcher Daten ist der Personenbezug meistens nicht eigentlich nötig. Er wird trotzdem oft mitgeführt, um verschiedene Daten eines Falls zusammenführen oder bei Forschungsprojekten Daten nacherheben zu können. Dazu reichen aber *Pseudonyme* aus. Sie reichen auch aus im Zahlungsverkehr und für Berechtigungsausweise.

Durch die Einführung von Pseudonymen kann der Personenbezug so verschleiert werden, daß faktische Anonymität entsteht. Bei

- *Anonymität* besteht ein Bezug nur auf eine Gesamtmenge von Individuen,
- *Pseudonymität* besteht ein Bezug zu einem einzelnen Individuum, dessen Identität allerdings nicht erkennbar ist,
- *Personenbezug* ist das einzelne Individuum in seiner Identität erkennbar (siehe Abbildung).

Bekannt ist die Verwendung von Pseudonymen durch Buchautoren. Was diesen zugestanden wird, sollte auch Bürgern, etwa in ihrer Eigenschaft als Patienten, gewährt werden: sich ein Pseudonym zu wählen, um ihre persönlichen Daten zu schützen. Aber im Gegensatz zum Autorenpseudonym müssen Pseudonyme auf Chipkarten auch etwas *beweisen*, etwa eine Berechtigung, und das heißt, sie müssen *rechtssicher* sein [PWP].

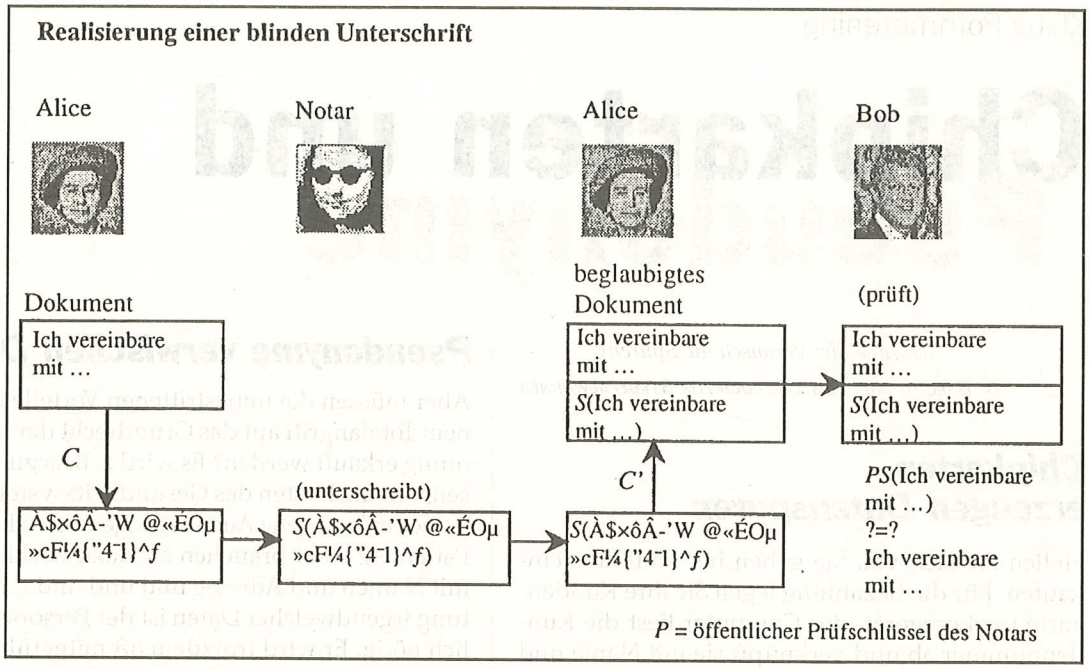
Für manche Anwendungsbereiche von Chipkarten ist komplette Anonymität möglich, wie das Beispiel der Telefonkarten zeigt. Aber diese repräsentieren geringe Werte, sind übertragbar, und ein Verlust schmerzt nicht sehr. Daher sind sie nicht besonders sicher, insbesondere nicht



fälschungssicher. Bei den meisten Anwendungen ist größere Sicherheit nötig.

Elektronische Pseudonyme

Die Rechtssicherheit von elektronischen Dokumenten wird durch elektronische Unterschrift (oder digitale Signatur, wie sie auch genannt wird) erreicht. Damit mein Pseudonym etwa meine Mitgliedschaft bei einer Krankenkasse beweist, müßte es also von eben dieser Krankenkasse unterschrieben werden, aber die soll es ja gerade nicht kennen. Ein Ausweg wäre die Unterschrift durch eine unabhängige Institution („Trusted Third Party"), der beide Partner trauen, im Beispiel also die Krankenkasse und ich. Es geht aber auch ohne eine solche Institution, denn die Kryptographen haben sich eine bessere Lösung ausgedacht [Ch1]: die *blinde Unterschrift*. Ein (elektronisches) Dokument wird dabei unterschrieben, ohne daß der Unterschreibende dessen Inhalt erkennen kann. Die Unterschrift bestätigt also nicht den Inhalt des Dokuments, sondern nur die Tatsache der Vorlage durch eine bestimmte Person zu einem bestimmten Zeitpunkt. Ein Analogon wäre die Unterschrift auf der Rückseite eines Papierdokuments. Zur Prüfung werden Dokument und Unterschrift vorgelegt. Der Prüfende kann erkennen, ob die Unterschrift zum Dokument gehört und rechtmäßig erlangt wurde. Niemand, auch nicht der Unterzeichner, kann, wenn er Dokument und Unterschrift vorgelegt bekommt, diese dem Besitzer zuordnen oder den Unterschriftsvorgang rekonstruieren.



Setzt man „Pseudonym" statt „Dokument" ein, so ist dies genau das Verfahren, mit dem eine Institution Pseudonyme beglaubigen kann ohne die Möglichkeit, sie wiederzuerkennen oder ihrem Besitzer zuzuordnen.

Um die Realisierbarkeit dieser scheinbar paradoxen Anforderungen plausibel zu machen, ist ein kleiner technischer Exkurs angezeigt. Man geht von der gewöhnlichen elektronischen Unterschrift aus. Der Unterzeichner N (wie „Notar") hat eine Funktion S, mit der er zu einem Dokument D (das etwa durch eine Zeichenkette oder eine Datei in binärer Form repräsentiert wird) eine Unterschrift $S(D)$ erzeugen kann; diese Funktion hängt von einem Schlüssel ab, der Geheimnis von N ist. Zur Überprüfung durch jedermann dient ein zugehöriger öffentlicher Schlüssel. Will nun die Besitzerin A („Alice") eines Dokuments D dieses von N unterschreiben lassen, ohne daß N den Inhalt erfährt, so transformiert sie es in eine unleserliche Gestalt $C(D)$, wobei die Transformation C (wie „Camouflage") von einem Paßwort abhängt, das A als Geheimnis behält. Durch Ns Unterschrift wird $S(C(D))$ erzeugt. Danach entfernt A die Camouflage durch Rücktransformation $C'(S(C(D)))$?=? $S(D)$. Damit das Verfahren funktioniert, muß hier die Gleichheit stehen, also C' eine Art Umkehrtransformation von C sein; C' muß aus C und bekannten Parametern leicht bestimmbar sein. Solche Transformationen lassen sich mit den bekannten Schemata zur elektronischen Unterschrift, etwa nach dem RSA-Verfahren, tatsächlich finden; für die mathematischen Einzelheiten sei auf [Ch1], [Ch2] verwiesen. Veranschaulicht wird der Vorgang durch Abbildung 2. Wichtig zu wissen ist dabei, daß die notwendigen mathematischen Operationen von existierenden Chipkarten vorgenommen werden können. *Chipkarten sind somit die idealen Träger von elektronischen Pseudonymen.* Die Technik ist vorhanden. Sie muß aber so gestaltet werden, daß diejenigen, die mit ihr umgehen sollen, dazu auch in der Lage sind.

Personenpseudonyme oder *Rollenpseudonyme* sind an die Person oder Rolle gebunden, mehrfach verwendbar und erzeugen somit zusammenführbare Daten; sie entsprechen Berechtigungsausweisen. Daneben gibt es *Transaktionspseudonyme*, die ähnlich wie ein Gutschein nur einmal verwendet werden und nicht miteinander in Bezug gebracht werden können. Personenpseudonyme sind auch die bei der Krebsregistrierung [P1] verwendeten Kontrollnummern, die dazu dienen, für Forschungszwecke anonymisierte personenbezogene Daten zusammenzuführen.

Beispiel: Pseudonyme Krankenkassenabrechnung

Als Beispiel für die Anwendung elektronischer Pseudonyme auf Chipkarten wird gezeigt, wie sich der Personenbezug bei der Krankenkassenabrechnung vermeiden läßt. Das Verfahren wurde bereits in [P2] vorgestellt; es wird hier zum besseren Verständnis vereinfacht wiedergegeben - die Rolle der kassenärztlichen Vereinigung bleibt außer Acht, ebenso die Möglichkeit, auch den Arzt vor der Krankenkasse durch ein Pseudonym zu schützen. Ein umfassenderer Vorschlag, der dies alles berücksichtigt, wird zur Zeit von der GMDS-Arbeitsgruppe „Datenschutz in Krankenhausinformationssystemen" [AG] erarbeitet. Die GMDS, Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie [GMDS],

ist die wissenschaftliche Fachgesellschaft für diese Fächer.

Sollen die Patienten gegenüber den Krankenkassen hinter Pseudonymen versteckt werden, sind folgende Anforderungen zu erfüllen:

1. Die Krankenkassen müssen bei der Abrechnung der Behandlung zweifelsfrei erkennen, daß die Leistungen für eines ihrer Mitglieder erbracht wurden.
2. Die Krankenkassen sollen keine personenbezogenen Krankheitsgeschichten sammeln können.
3. Die Krankenkassen sollen aber zur Kalkulation ihrer Risiken einzelfallbezogene Auswertungen über Krankheitsverläufe und Kosten für bestimmte Krankheitsbilder erstellen können.

Ein mögliches Verfahren zur Realisierung sieht so aus: Die Patientin erhält von der Krankenkasse eine Versichertenkarte, wie bisher auch. Sie wählt zu Hause oder an vertrauenswürdiger Stelle, etwa bei ihrem Hausarzt, eine Kontrollzahl als Pseudonym, camoufliert sie und überträgt sie auf die Karte; alles dies wird durch „benutzerfreundliche" Software auf einen Maus-Klick und die Eingabe eines Paßworts reduziert. Dann läßt sie diese Kontrollzahl von der Krankenkasse (blind) unterschreiben; danach entfernt sie die Camouflage wieder, ebenfalls per Maus-Klick und Paßwort. Das Pseudonym wird auf der Versichertenkarte durch ein Paßwort (oder eine PIN) geschützt, das in Wirklichkeit der Schlüssel für ein kryptographisches Verschlüsselungsverfahren ist; solche Verfahren sind beim heutigen Stand der Chipkartentechnik ohne weiteres zu realisieren.

Bei ärztlicher Behandlung legt die Patientin die Versichertenkarte vor und schaltet das Pseudonym durch Eingabe ihres Paßworts frei; der Arzt übernimmt das Pseudonym, prüft es auf Gültigkeit und verwendet es zur Abrechnung. Es ersetzt also die Versichertennummer. Die Krankenkasse erkennt durch Prüfung der Unterschrift, daß die behandelte Patientin bei ihr versichert ist, kann mit dem Arzt abrechnen und die Daten der Patientin zusammenführen. Sie kann die Daten aber nicht der konkreten Patientin zuordnen. Da der behandelnde Arzt die Zuordnung zwischen Pseudonym und Identität sowieso erkennt und der Schweigepflicht unterliegt, schadet es nicht, wenn für die Erzeugung des Pseudonyms sein Praxiscomputer eingesetzt wird. Es schadet auch nicht, wenn die Versichertenkarte zur Vermeidung von Mißbrauch „personalisiert", also etwa mit Paßbild und Unterschrift versehen wird, solange in der elektronischen Datenspur nur das Pseudonym erscheint.

Ein entsprechendes Verfahren zur Abrechnung von Rezepten wurde bereits von B. Struif [Str] vorgestellt, zusammen mit einer funktionierenden Musterimplementation. Nach ähnlichem Muster würden pseudonymbasierte Berechtigungsausweise auch in anderen Anwendungsbereichen funktionieren. Bemerkenswert ist, daß ein solches Ausweissystem ohne online-Verbindung, also ohne Datennetz, funktioniert.

Technik für den Menschen?

Haben wir mit dem elektronischen Pseudonym die Patentlösung gefunden, bei deren Anwendung wir konsequent Chipkarten für alle Zwecke einführen können, ohne den Datenschutz zu durchlöchern? Die Idee wurde bisher nur in Fachkreisen, unter Kryptographen, diskutiert. Viele Fragen sind offen. Einige davon will ich stellen.

Wieviele Chipkarten verträgt ein Mensch? Damit die Daten darauf geschützt sind, braucht man ein Paßwort (oder eine PIN). Wieviele Paßwörter kann sich ein Mensch merken? Sollten wir lieber *eine* Chipkarte für alle Anwendungen anstreben, eine Art universellen Personalausweis, der alle Berechtigungen und Pseudonyme, Schlüssel für die elektronische Unterschrift, medizinische Daten und was nicht noch alles enthält? Dann bräuchten wir nur ein einziges Paßwort. Aber dann muß auch die Möglichkeit bestehen, die Daten der Chipkarte nur in Teilen freizugeben. Ist ein Durchschnittsbürger, der nicht einmal seinen Videorecorder programmieren kann, mit solcher Komplexität überfordert? Oder ist umgekehrt die Technik von Chipkarten und Lesegeräten sogar geeignet, die Komplexität des Lebens zu verringern? Welchem Hersteller, welcher Technik, welchem Gerät kann der Mensch trauen? Sehr konkrete Gedanken und Vorschläge dazu findet man in [PPSW] und [Ch3]. Werden wir durch pseudonyme Berechtigungsausweise verletzlicher? Welche Möglichkeiten eröffnen sich Kriminellen, die nicht davor zurückschrecken, sich durch „social engineering" (Erpressung o. ä.) in den Besitz eines Paßworts zu bringen? Was passiert, wenn ein Pseudonym aufgedeckt wird? Wenn eine Chipkarte verloren geht oder beschädigt wird? Wo und wie fertigt man Sicherheitskopien der Daten und Pseudonyme an? Soll im Falle eines Rechtsstreits ein Pseudonym aufdeckbar sein? Auf welche Weise? Wird durch ein ständig verwendetes Personenpseudonym so viel Datenmaterial verknüpfbar, daß die Anonymität nicht mehr aufrecht zu erhalten ist? Was muß der Mensch über seine Chipkarte und seine Pseudonyme wissen, um verantwortungsvoll damit umgehen zu können und seine informationelle Selbstbestimmung wirkungsvoll auszuüben?

Zusammenfassung

Nachdem die Idee der elektronischen Unterschrift in einer doch schon recht breiten Öffentlichkeit angekommen ist, ist es jetzt an der Zeit, die Idee des elektronischen Pseudonyms auf ebenso breiter Grundlage zu diskutieren. Diese Pseudonyme auf kryptographischer Basis stellen eine Grundtechnik des praktischen Datenschutzes dar. Sie sollten, wo immer möglich, eingesetzt werden, um Datenspuren zu vermeiden.

Die Sicherheitsfunktionen, die auf Chipkarten technisch vorgesehen sind, sind konsequent für die Verwendung von Pseudonymen einzusetzen. Dann bringen Chipkarten nicht nur Sicherheitsvorteile für die Banken, die Krankenkassen, den Staat, sondern auch für die Kunden, die Patienten, die Bürger. Pseudonymbasierte Chipkarten statt identitätsbasierter Chipkarten retten das Grundrecht auf informationelle Selbstbestimmung.

Elektronische Pseudonyme sind aber keine Patentlösung. Ihre Verwendung muß in jedem Anwendungsfall sorgfältig auf Risiken und Nebenwirkungen geprüft werden, vor allem auch unter dem Gesichtspunkt, wie die Beteiligten damit umgehen ■

Literatur: siehe folgende Seite

Literatur zum Beitrag »Chipkarten und Pseudonyme«

[Ch1] Chaum, D.: Security without identification: Transaction systems to make Big Brother obsolete. *Communications of the ACM* 28, 1985, 1030 - 1045.

[Ch2] Chaum, D.: Security without identification: Card computers to make Big Brother obsolete.
http://www.digicash.com/publish/bigbro.html

[Ch3] Chaum, D.: Achieving electronic privacy. *Scientific American*, August 1992, 96 - 101.
http://www.digicash.com/publish/sciam.html

[PWP] Pfitzmann, B.; Waidner, M.; Pfitzmann, A.: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen. *Datenschutz und Datensicherung* 14, 1990, 243 - 253 & 305 - 315.
http://www.informatik.uni-hildesheim.de/FB4/Institute/Informatik/issi/sirene/publ/PWP_90anonyZsys.ps.gz

[PPSW] Pfitzmann, A., Pfitzmann, B., Schunter, M., Waidner, M.: Vertrauenswürdiger Entwurf portabler Benutzerendgeräte und Sicherheitsmodule. In: Brüggemann, H. H.; Gerhardt-Häckl, W. (Hrsg.): *Verläßliche IT-Systeme, Proceedings der GI-Fachtagung VIS 95*. Braunschweig, Vieweg 1995, 329 - 350.

[P1] Pommerening, K.: Krebsregister - Ein Konzept für die sozialverträgliche Gestaltung; *FIFF-Kommunikation* 4/93, 64 - 66.

[P2] Pommerening, K.: Pseudonyme - ein Kompromiß zwischen Anonymisierung und Personenbezug. In: H. J. Trampisch, S. Lange (Hrsg.): *Medizinische Forschung - Ärztliches Handeln, 40. Jahrestagung der GMDS*. München, MMV Medizin Verlag 1995, (im Druck).

[Str] Struif, B.: Datenschutz bei elektronischen Rezepten und elektronischem Notfallausweis. In: *Vertrauenswürdige Informationstechnik für Medizin und Gesundheitsverwaltung*. Erfurt; TeleTrusT Deutschland 1994.

[AG] http://www.uni-mainz.de/FB/Medizin/IMSD/AGDatenschutz/AGDS.html

[GMDS] http://www.med.uni-muenchen.de/gmds/gmds.html

Steffen Stripp

Die Bürgerkarte

Ein kleiner Helfer zum Schutz der Privatsphäre?

Chipkarten (IC-"integrated circuits-"cards) wurden einst von ihrem Erfinder Roland Moreno folgendermaßen charakterisiert: "Sie haben das Potential, Big Brothers kleine Helfer zu werden". Bei Diskussionen über die Chipkarte in Australien, Großbritannien und anderswo liegt das Hauptaugenmerk auf diesem Aspekt.

Haben IC-Karten jedoch vielleicht auch das Potential, ein kleiner Helfer zum Schutz der Privatsphäre des Bürgers zu sein? Die dänische Technologiekommission (The Danish Board of Technology - DBT) hat mit einer Studie zur Technikfolgenabschätzung eine öffentliche Debatte über die Bürgerkarte ausgelöst. In einem Papier vom September '95 bezeichnete der Innenminister die Bürgerkarte als "den Schlüssel zu sicherer Kommunikation".

Infrastruktur

Ein Hauptergebnis der DBT-Studie "Plastikkarten als Bürgerkarten" ("Plastic cards as citizen's cards") war, daß eine Bürgerkarte die Infrastruktur der Informationstechnik in Dänemark stärken kann.

- Die Bürgerkarte soll von den Bürgern zur Identifizierung beim Zugriff auf öffentliche Computersysteme eingesetzt werden.

Das Projekt

Das Projekt "Plastikkarten als Bürgerkarten" wurde 1993/94 gestartet. Das Projekt bestand aus einer Studie, deren Ergebnisse von einer Bürgerkommission und Interessengruppen bewertet wurden.

In der Studie wurden die Einsatzmöglichkeiten von Computerkarten analysiert. Als Teil der Analyse wurden Expertentreffen durchgeführt und die Zwischenergebnisse mit einer Gruppe von Vertretern von Interessengruppen, Beratern, Fachvertretern, Unternehmen und Organisationen diskutiert.

Bewertungen durch das Projektmanagement, Interessengruppen und den Bürgerrat wurden durchgeführt. Eine Beurteilung der sensiblen Funktionen, die eine solche Computerkarte enthalten könnte, wurde gemacht. Diese Funktionen wurden als Vorschlag zu einer "Privatkarte" ("Private Card") vorgestellt. Daraufhin beantworteten einige Interessengruppen auf Hearings Fragen zu dieser Studie. Schließlich bewertete eine Kommission aus zehn Bürgern („Bürgerrat") die "Privatkarte" auf einer Konsensuskonferenz. Die Projektleitung faßte diese Einzelbewertungen in einer Abschlußbewertung zusammen.

Informationen wurden während und nach der Projektlaufzeit Nachrichtenagenturen, Medien, Interessengruppen, staatlichen Stellen und Politikern zur Verfügung gestellt. Dadurch sollte öffentlicher Diskurs und Bewertung des Themas gewährleistet werden.

Der Projektbericht (Steffen Stripp: "Plastic cards as citizen's cards" - nur in dänischer Version) kann vom DBT bezogen werden. ■

- Die Bürgerkarte soll Verschlüsselungsfunktionen enthalten, um sie zur Erstellung einer digitalen Unterschrift und zur Gewährleistung von Sicherheit bei elektronischem Datenverkehr einsetzen zu können. Diese Funktionen könnten bei elektronischer Post, im elektronischen Warenbestellwesen, beim Homebanking und bei anderen elektronischen Servicediensten genutzt werden. Dadurch könnten sie Paßwörter ersetzen und Zugriffsschutz auf Disketten und Festplatten gewährleisten.
- Die Bürgerkarte soll Zugangsberechtigung zu den in öffentlichen Computern gespeicherten persönlichen Daten geben.
- Die Karte könnte auch die Stammdaten des einzelnen Bürgers und von Minderjährigen enthalten.
- Die Bürgerkarte soll freiwillig sein.
- Der Personalausweis als Karte wurde vom Bürgerrat der Technologiekommission abgelehnt, auf freiwilliger Basis sollte es nach seiner Ansicht jedoch möglich sein, die Bürgerkarte bei Personenkontrollen als Ausweis zu verwenden.

Der Bürgerrat unterstützte die Verwendung eines Biocode (eines biometrischen, d.h. körperbezogenen Merkmals) anstelle einer PIN-Nummer zur Authentifikation des Karteninhabers unter der Voraussetzung, daß dieser Biocode, zum Beispiel als Fingerabdruck, nur auf der Karte existiert (one-way). Der Einsatz eines Biocode anstelle einer PIN wurde auch vom Verbraucherschutzbund befürwortet.

Die Hauptforderung des Projekts ist, daß die Bürgerkarte Sicherheitsmechanismen enthalten muß, um dadurch Teil der künftigen Informationsinfrastruktur zu werden. Es besteht Konsens, daß die Lösung der Frage der Sicherheitsmechanismen Grundvoraussetzung für die Anwendung einer solchen Informationsinfrastruktur ist. So wie die Straßenverkehrssicherheit eine öffentliche Aufgabe ist, muß auch die auch die Gewährleistung von „Verkehrssicherheit" auf den Infobahnen und -landstraßen als öffentliche Aufgabe angesehen werden.

Regierungspolitik

Eine elektronische Bürgerkarte mit PIN-Code ist Teil eines "politischen Aktionsplanes Informationstechnik" ("IT political action plan") der dänischen Regierung. Darin heißt es: "Auf Grundlage eines kürzlich veranstalteten Hearings zum Bericht des Innenministers wird es zu einer politischen Entscheidung über die mögliche freiwillige Einführung einer elektronischen Bürgerkarte mit PIN-Code und Lichtbild" kommen. Dieser im Dezember '94 veröffentlichte Bericht, wurde in öffentlichen Anhörungen bis Mai '95 diskutiert. Der Innenminister veröffentlichte im September '95 einen neuen Vorschlag und forderte zu öffentlicher Debatte auf. Die Bürgerkarte wird dort als "der Schlüssel zu sicherer Kommunikation" bezeichnet und setzt dabei Schwerpunkte auf drei Funktionen:

- Autorisierung für Selbstbedienungssysteme
- Vertraulichkeit bei e-mail und anderer elektronischer Kommunikation
- Digitale Unterschrift

Die Bürgerkarte kann dort aber neben anderen Funktionen auch als Ausweiskarte eingesetzt werden und dadurch verschiedene andere Ausweise ersetzen. Die öffentliche Debatte soll bis März nächsten Jahres abgeschlossen sein. Danach wird es vielleicht zu einer politischen Entscheidung kommen.

Eine Technologie zum Schutz der Privatsphäre?

Ich denke, daß eine "Kommunikationskarte", die Schutzfunktionen wie Sicherheit elektronischer Post und digitaler Signatur gewährleistet, eine Technologie zum Schutz der Privatsphäre sein kann. Es ist möglich, einige generelle Forderungen aus der in Dänemark durchgeführten Analyse und öffentlichen Debatte abzuleiten.

Erstens sollte die Bürgerkarte *keine* Ausweiskarte sein. Es darf unter keinen Umständen zu einer Pflicht werden, daß der Bürger sie als Ausweiskarte zur Kontrolle durch Polizei und andere Stellen mit sich führen muß. Diese Forderung genießt breite Zustimmung. In verschiedenen Studien kann die Bürgerkarte zur persönlichen Identifikation auf freiwilliger Basis eingesetzt werden. In der Diskussion wurde diese Möglichkeit als erste Stufe zur Überwachung gesehen.

Zweitens: Die Bürgerkarte sollte freiwillig sein. Diejenigen Bürger, die sich gegen eine Karte entscheiden, dürfen in keiner Weise diskriminiert werden. Diese Forderung unterstreicht auch die erste Forderung, weil dann jederzeit auf die Freiwilligkeit der Karte verwiesen werden kann. Diese Forderung ist Teil des offiziellen Regierungsprogramms.

Drittens sollte eine Bürgerkarte gesetzlich geregelt sein. Dieses Gesetz muß den Einsatz der Bürgerkarte definieren. Diese Forderung ist im Vorschlag des Innenministers enthalten.

Aus dem Englischen übersetzt von Michael Müller. ■

Die dänische Technologiekommission

Der DBT startet Projekte, um die Folgen von Möglichkeiten und Auswirkungen technischer Entwicklung zu bewerten. Er liefert Anstöße zum öffentlichen Technologiediskurs. Der DBT setzt typischerweise interdisziplinäre Kommissionen aus Experten und Bürgern ein, um Technologie zu analysieren und Folgen abzuschätzen. Die Ergebnisse der Kommissionsprojekte und Debatten spiegeln die Bewertungen der beteiligten Fachexperten und Bürger wieder.

The Danish Board of Technology
Antonigade 4
DK-1106 Copenhagen
Denmark
Phone: +45 3332 0503
Fax: +45 3391 0509
E-mail: tekno@init.uni-c.dk
WWW: http://www.ingenioren.dk

Jens Woinowski

Chipkartensysteme an Hochschulen

Auf der 23,5ten Konferenz der Informatik-Fachschaften (KIF) in Hamburg, die eine Woche nach der FifF-Jahrestagung 1995 stattfand, gab es einen Arbeitskreis zum Thema Chipkarten. Neben einer Übersicht über verschiedene bereits eingeführte oder geplante Kartensysteme war der Schwerpunkt auf Chipkarten an Hochschulen gelegt. Dies liegt vor allem nahe, weil hier ganz offensichtlich versucht wird, über eine große und im allgemeinen technikfreundliche Gruppierung Chipkarten als positive Imagevermittler einzuführen. Ein Ergebnis des Arbeitskreises ist, daß es einen Reader geben wird, der zur politischen Diskussion beitragen soll. Zum Adressatenkreis gehören neben den Asten in Deutschland alle anderen, die sich mit der Chipkartenproblematik beschäftigen.

Der Arbeitskreis hatte eine längere Vorgeschichte. Einer der Anlässe war die Einführung eines

„Chip-Schlüssel"-Systems zur bargeldlosen Bezahlung an der Mensa der TH Darmstadt im Herbst 1995. Das System erfaßt die Schlüssel-ID und ein wiederaufladbares Guthaben. Jeder Kaufposten wird mit Art, Preis und Datum zentral für vier Wochen gespeichert. Erst zu Beginn des Wintersemesters gelang es, an der TH Darmstadt das politische Interesse außerhalb der Fachschaft Informatik zu wecken. Parallel hierzu lief bei der GMD in Darmstadt eine Tagung über eine allgemeine StudentInnenkarte mit Mehrzweckfunktionen - unter anderem, weil die GMD ein eigenes System zu verkaufen hat. Wir erfuhren außerdem, daß in Chemnitz bereits seit längerem ein zur Mensa Darmstadt ähnliches System läuft, mit der Besonderheit, daß dort zu der Schlüssel-ID im System auch die Namen der KartenbesitzerInnen gespeichert werden. Aus diesem Anlaß haben wir eine Woche vor der KIF, eine Materialsammlung via Mail gestartet, dem auch nachgekommen wurde.

Auf der FIFF-Jahrestagung wurde dann bereits ein Teil der Papiere gesichtet.Außerdem wurde bei der Gelegenheit auch der bremische Datenschutzbeauftragte Stefan Walz zur rechtlichen Einordnung des Darmstädter Systems befragt. Von einigen Leuten, die auch zur KIF am fogenden Wochenende fahren wollten, wurde darüber diskutiert, ob auf der KIF ein Arbeitskreis eingerichtet werden sollte, oder eher ein eigenes Treffen nur vorbereitet werden sollte. Die Fülle des Materials und die gute Gelegenheit, auf der KIF viele Leute für das Thema interessieren zu können, machten die Entscheidung leicht, den Arbeitskreis stattfinden zu lassen.

Am ersten Tag wurde das eingegangene und mitgebrachte Material (ca. 250 Seiten) gesichtet, thematisch geordnet und in Kleingruppen aufgearbeitet. Das Material umfaßte neben Studi-Karten auch Krankenkassenkarten, Telefonkarten, Sozialversicherungsausweis, technische Informationen und vieles mehr. Durch Referate der Kleingruppen wurde der gesamte AK auf einen gemeinsamen Wissensstand gebracht. Währenddessen und anschließend fand eine heftige Diskussion über die Informationen statt. Wir waren schwer erschüttert, wie umfassend und skrupellos die Verdatung vor allem im Unibereich geplant und bereits durchgeführt wird:

Diverse Uni-Chipkarten-Systeme existieren bereits in Chemnitz, Darmstadt, München (FH, TU und LMU), Karlsruhe und (wie sich inzwischen herausgestellt hat) auch in Bremen, Aachen (FH-Abteilung Jülich, mit einem System, das dem der GMD ähnlich ist), sowie mehreren ausländischen Unis.

In Holland läuft ein Mega-Pilotprojekt (ca. 4,5 Mio. DM) zur Einführung einer „General Studi-Card", die gleichzeitig Studiausweis, Semesterticket, Bibliotheksausweis, Zugangsberechtigung zu Uniräumen, Mensakarte, Copycard, Telefonkarte, electronic cash für Campus-Einkäufe sowie Rechnerzugang zu einem Uni-Verwaltungssystem für Prüfungsanmeldung, Adreßänderung, Rückmeldung etc. (alle Verwaltungsaufgaben!) in sich vereint. Das Projekt wird von IBM Holland/Deutschland, der PTT (Telekom und Postbank Holland) und der IBG (einer zentralisierten, privatisierten holländischen Schule-Kultur-Forschungs-Verwaltungs-Gesellschaft für alle Hochschulen) in Kooperation durchgeführt. Seit September 1995 läuft dieses Pilotprojekt an zwei holländischen Hochschulen in Groningen (Uni und School of Ecomomics) und in Twente, wo als Vorläufer ein weniger leistungsfähiges System mit Magnetstreifentechnik eingeführt wurde.

Das bayrische Kultusministerium hat eine Studie zur „Optimierung von Universitätsprozessen" in Auftrag gegeben, die konzeptionell dem holländischen Modell sehr ähnelt.

Wir zogen währenddessen immer wieder Vergleiche zu anderen Kartensystemen (Telefonkarte, Krankenversicherungskarte, EC-Karte) sowie dem Sozialversicherungsausweis. Sehr kontrovers wurde die Diskussion, als es um die Bewertung der neuen Informationen und die daraus abgeleiteten Szenarien sowie eine gesellschaftspolitische Einordnung ging.

Am nächsten Tag faßten wir den Beschluß, uns im AK thematisch auf die Studi-Cards zu beschränken. Wir setzten uns zum Ziel, zu diesem Thema einen Info-Reader für Asten und andere Interessierte als politische Argumentationshilfe zu erstellen. Da uns klar wurde, daß die Zeit auf der KIF dafür nicht ausreichen würde, wurde ein Redaktionstreffen vereinbart und ein Verteiler für die Zwischenergebnisse organisiert. Die inhaltliche Diskussion vom Vortag setzte sich fort, was dazu führte, daß wir Themen für den Reader zusammenstellten.

Fortsetzung auf der folgenden Seite unten ▶

Thomas Elkeles, Rolf Rosenbrock

Chipkartenanwendung in der Prävention

Angesichts der rasanten Entwicklung der Chipkartentechnologie werden im Gesundheitswesen nicht nur Anwendungsfelder im Bereich der medizinischen Versorgung, sondern auch für den Bereich der Prävention und Gesundheitsförderung diskutiert. Medizin und Gesundheitswesen bilden - wie bei anderen Entwicklungen der Informations- und Kommunikationstechnologien - einen gigantischen potentiellen Markt für diese neuen Produkte. Der Dynamik entspricht ein teilweise unübersichtlicher Stand der Entwicklung, Implementation und Evaluation von Kartenprojekten. Deutlich ist, daß einerseits die technische Machbarkeit, andererseits ökonomische Interessen von Hard- und Softwareherstellern und -vertreibern zu Ausweitungstendenzen führen.

Gefordert wird daher auch, die technische Entwicklung bewußt zu steuern, indem der Nachweis eines Nutzenüberschusses gegenüber den zu erwartenden Risiken zu führen, Technikfolgenabschätzungen vorzunehmen und ethische Implikationen vorab zu bedenken seien. Sicher ist, daß die Sensibilität potentiell auf einer Chipkarte zu speichernder Variablen im Bereich von Prävention und Gesundheitsförderung noch erheblich größer ist als im Bereich medizinischer Patientendaten. Bei bestehenden politischen Tendenzen dazu, daß die Solidargemeinschaft der Versicherten nicht mehr im bisherigen Umfang für Krankheit aufzukommen hat, könnte zum Beispiel die Speicherung als selbstverschuldet denunzierbarer Risiken (wie Rauchen, Übergewicht etc.) für die betroffenen Individuen unter Umständen gravierende Folgen haben.

Dieses Beispiel zeigt, daß eine Speicherung individuenbezogener präventiver Daten prinzipiell für Kontroll- und Sanktionsstrategien nutzbar wäre. Es muß daher ethisch sehr genau geprüft werden, welche Daten überhaupt zu einer potentiellen Speicherung in Frage kommen und wer Verfügungsmöglichkeiten über sie erhalten soll. Die historische Erfahrung nationalsozialistischer Vernichtungsaktionen an sogenannten oder vermeintlich Erbkranken gebietet es, hier besonders strenge Maßstäbe anzulegen. In der sich gegenwärtig entwickelnden Diskussion um Nutzungsmöglichkeiten von Chipkarten im Gesundheitswesen sind u.E. zwar keine Tendenzen ersichtlich, gesundheitliche Kontrolle oder Sanktion bewußt zu intendieren. Sie sollen daher hier auch nicht unterstellt werden. Ein Spannungsfeld von Autonomie und Kontrolle ist jedoch beim Thema der Prävention grundsätzlich angelegt. Als aktuelles Beispiel sei hier lediglich auf die Aidspolitik verwiesen.

Den Risiken einer Verfügbarkeit von Daten stehen deren Nutzen gegenüber. Daten über den Bedarf und die Bedarfsdeckung sind im Bereich von Prävention und Gesundheitsförderung aus einer gesundheitswissenschaftlichen Perspektive von hohem Nutzen. In der Regel wird eher beklagt, daß Daten ungenügend zur Verfügung stehen bzw. zur Verfügung stehende Daten ungenügend genutzt werden.

Sollte dies nicht bedeuten, daß Daten über den Bereich Prävention und Gesundheitsförderung geradezu ein ideales Anwendungsfeld für Chipkartenentwicklungen darstellen? In einem für die Senatsverwaltung für Gesundheit Berlin angefertigten Gutachten untersuchten wir die Nutzungsmöglichkeiten in diesem Gebiet.

Kriterien

Legt man ein umfassendes Verständnis von relevanten Einflußbereichen auf die Gesundheit und von den möglichen Risiken und Ressourcen zugrunde, sind eine Reihe von zum Teil ganz unterschiedlichen Bereichen zu berücksichtigen, aus denen Indikatoren zu erfassen und auf der Karte zu

---

▶ Am dritten Tag wurden die Themen in Kleingruppen stichwortartig mit Inhalt gefüllt und anschließend in der Großgruppe diskutiert. Schließlich wurde die Gesamtstruktur für den Reader erstellt und die konkrete Ausarbeitung als Einzelarbeitsaufträge verteilt.

Bezugsadresse für den Reader:

Technische Hochschule Darmstadt
Fachschaft Informatik
Alexanderstraße 6
64283 Darmstadt

Zur Literatur des Arbeitskreises gehörte unter anderem:

1. Tagungsband des „GMD-SmartCard-Tag 'Studentenkarte' „ vom 5.10.1995, Hrsg.: Bruno Struif, GMD
2. Der Reader „Die Krankenversichertenkarte gefährdet Ihre Gesundheit" (1992), Hrsg.: Deutsche Vereinigung für Datenschutz (DVD, Bonn) und Institut für Informations- und Kommunikationsökologie (IKÖ).

Jens Woinowski / AK Chipkarten der 23,5ten KIF. ■

speichern wären (hereditäre und erworbene Risiken, Risiken der Arbeitswelt, Risiken der technischen und natürlichen Umwelt etc.). Ob dies einerseits als machbar, andererseits als erwünscht gelten kann, kann mit folgenden Kriterien überprüft werden:

1) Verfügbarkeit von Indikatoren,
2) Konsensfähigkeit von Indikatoren,
3) Individuelle Zuschreibbarkeit von Indikatoren,
4) Individuelle Erhebbarkeit von Indikatoren,
5) Organisatorischer, politischer, finanzieller und rechtlicher Regelungsbedarf,
6) Abschätzung von Nutzenpotentialen für die individuelle Prävention,
7) Abschätzung von Nutzenpotentialen für die bevölkerungsbezogene Prävention sowie
8) Ethische Aspekte.

Die Auswahl dieser Kriterien entspricht den Anforderungen, jeweils schrittweise die Machbarkeit und Erwünschtheit einer Erweiterung des Dateninhalts einer Patientenchipkarte zu prüfen. Voraussetzung einer Machbarkeit ist zunächst, daß zu einem jeweiligen Bereich der Prävention und Gesundheitsförderung - sei es in der Praxis oder in der wissenschaftlichen Literatur - erstens Indikatoren verfügbar sind und zweitens über ihren Indikatorgehalt wissenschaftlicher Konsens besteht. Drittens ist Voraussetzung, daß solche Indikatoren einzelnen Individuen zuschreibbar sind und daß die individuelle Erhebung praktikabel ist - insbesondere wenn die Vorstellung besteht, das einzelne Individuum solle sich aufgrund der Informationen auf der Chipkarte selber vermehrt um die Erhaltung und Förderung seiner Gesundheit kümmern. Ist dieses alles der Fall, ist als weitere Voraussetzung der Machbarkeit abzuschätzen, ob der Umfang des organisatorisch-politischen Regelungsbedarfs in absehbarer Zeit bewältigbar erscheint. Bei gegebener Machbarkeit ist dann zu prüfen, welcher präventive Nutzen einerseits für das einzelne Individuum anzunehmen ist, das eine derartige Chipkarte nutzt, und welcher präventive Nutzen darüber hinaus für die bevölkerungsbezogene Prävention eines jeweiligen gesundheitlichen Risikos besteht. Das Überwiegen eines Nutzens muß sich ferner dadurch erweisen, daß Risiken der Anwendung unter ethischen Gesichtspunkten als vertretbar klein angenommen werden können.

Bewertung

Praktisch in allen Bereichen mangelt es an Indikatoren. Zwar gibt es eine Reihe von Forschungsinstrumenten zur Messung von Risiken. Oft besteht jedoch noch kein wissenschaftlicher Konsens über deren Aussagefähigkeit und Qualität. Noch weniger kann von einer Standardisierung von Instrumenten gesprochen werden. Hierzu sind selbst im wissenschaftlichen Bereich noch erhebliche Entwicklungsarbeiten zu leisten, ganz abgesehen von dem organisatorischen Aufwand, außerhalb des Wissenschaftsbetriebs derartige Indikatoren zu erfassen und auf eine Chipkarte zu bringen. In relevanten Präventionsbereichen wie Arbeitswelt, technische sowie soziale Umwelt sind die bekannten Risiken zumal meist nicht einzelnen Individuen als Merkmal zuschreibbar.

Der Präventionsbereich, in dem Risikomerkmale einzelnen Personen zugeschrieben werden können, ist der Bereich der Lebensstile. Über die Bedeutung und präventive Anwendung der hier zur Verfügung stehenden Risikofaktoren (z.B. Übergewicht, Cholesterin) besteht jedoch wissenschaftlich und politisch kein Konsens. Mit anderen Worten: Eine individuelle Zuschreib- und Erhebbarkeit dieser Merkmale ist gegeben. Umstritten sind jedoch die Indikatorfunktion und der präventive Nutzen, also die Aussagefähigkeit und Belastbarkeit der Indikatoren sowie die Relation von erwünschten und unerwünschten Wirkungen hieraus abgeleiteter Präventionsstrategien. Entsprechend finden sich einzelne kommerzielle Anbieter entsprechender Kartenversionen. Es ist jedoch fraglich (und vor allem von der gewählten präventionspolitischen Strategie abhängig), ob derartigen Anwendungen eine Zukunft beschieden ist.

In keinem Präventionsbereich konnte die Bedingung erfüllt werden, daß sämtliche acht zur Prüfung benutzten Kriterien ein positives Urteil nahelegen. Für die Mehrzahl der Bereiche gilt, daß es bereits an einer Machbarkeit zu mangeln scheint.

Lediglich für einen Typ von Daten stellt sich die Situation anders dar, und zwar für präventivmedizinische Daten, insbesondere über entsprechende Untersuchungen in entsprechenden gesundheitspolitischen Programmen dar (z.B. Schwangerenvorsorge, Krebsvorsorge). Für diese Art von Daten gilt wie für jene in der Krankenversorgung, daß sie zwar erhoben, jedoch oft nicht in systematischer Form dokumentiert werden. Ihre Speicherung auf einer Chipkarte könnte die Verfügbarkeit von präventivmedizinischen Informationen über den Patienten bzw. Versicherten bei Ärzten oder anderen therapeutischen Berufen verbessern. Eine solche Präventionskarte wäre im Grunde eine Patientenkarte.

Für letztere ist denkbar, daß sie um rehabilitative (= sog. Tertiärprävention, z.B. bei chronisch Kranken) und Aspekte medizinischer Vorsorge erweitert wird und daß dies positive Informationseffekte für die Experten hat.

Machbar wäre auch die Aufnahme von Informationen über toxische und andere bereits heute gemessene Belastungen am Arbeitsplatz (medizinische Vorsorgeuntersuchungen). Versuche mit einem solchen Paß in Papierform sind andernorts allerdings wiederholt an Bedenken der Gewerkschaften hinsichtlich des Datenmißbrauchs durch Unternehmen gescheitert. ■

Literatur:

Elkeles, T., Rosenbrock, R.: Chipkarten im Gesundheitswesen. für Prävention und Gesundheitsförderung? Veröffentlichungsreihe der Arbeitsgruppe Public Health, Wissenschaftszentrum Berlin für Sozialforschung, Nr. P95-203. Berlin.

Tien Nguyen N.

»HEMACARD«

Ein Hämatologie-Kartenprojekt in Belgien

HEMACARD ist ein gemeinsames Projekt der Forschungsgruppe CITA für Technikfolgenabschätzung an der Universität von Namur in Belgien und der Hämatologie-Abteilung eines großen Krankenhauses in der Nähe Namurs (Mont-Godinne). Das Projekt lief im Januar 1992 an, die Evaluation ist für den März 1996 geplant. Das Ziel des Projekts besteht darin, eine Gesundheitskarte für Patienten mit Blutkrankheiten zu entwickeln und zu bewerten. Als Technologie wird eine Mikroprozessor-Chipkarte verwendet.

Durch das HEMACARD-Projekt beteiligt sich die Forschungsgruppe CITA auch am EC-DGXIII-Eurocards-Programm (WG 5: „Users acceptance") - zusammen mit der Forschungsgruppe CRID an der Universität Namur (für rechtliche Fragen), dem Projekt Santal in Frankreich und der Commission d´Acces a l'Information du Quebec in Kanada, der dortigen Universität Laval sowie den Krankenversicherungsbehörden in Quebec (Rimouski-Projekt).

Die Nutzer von HEMACARD und ihre Anforderungen

Der erste von der Karte betroffene Nutzer ist der Patient. Er ist der Eigentümer und Besitzer der Karte. Damit er der Benutzung seiner Karte zustimmen kann, muß ihm die Vertraulichkeit der auf der Karte befindlichen Informationen zugesichert werden. Weitere Nutzer sind die Angehörigen des medizinischen Personals: Ärzte, Krankenpfleger und Rettungssanitäter. Sie müssen einfach und schnell auf die Karteninformationen zugreifen können. Sowohl die Integrität als auch die Verbindlichkeit der Daten müssen sichergestellt sein. Die zu erfüllenden Sicherheitsanforderungen sind daher Vertraulichkeit und Vollständigkeit der Daten sowie Schutz vor unberechtigtem Zugriff. Ärzte können die Informationen lesen, schreiben sowie aktualisieren, während Krankenpfleger die Daten lediglich lesen können.

Die gespeicherten Daten

- **Verwaltungsdaten:**

  Darunter fallen Daten zur Identifikation des Patienten, seine Kranken- und Sozialversicherungsdaten, Informationen über seinen Hausarzt sowie Informationen über eine im Notfall zu verständigende Person.

- **Medizinische Daten:**

  Klinische Daten: Diagnose, Therapien, Behandlungen, Allergien, Eingriffe (Chirurgie, Transplantation, Radiologie), Infektionen, Komplikationen sowie Informationen über weitere anzunehmende Krankheiten oder Behandlungen.

  Blutdaten: Phänotypus (Erscheinungsbild), Besonderheiten in bezug auf Transfusionen.

  Notfalldaten.

Methodische Betrachtungen: Ein konstruktiver Ansatz der Technikfolgenabschätzung

Einer Versuchsphase schließt sich eine konstruktive Methode der Technikfolgenabschätzung an, indem die Einführung der Karte vom Beginn bis zur abschließenden Bewertung begleitet wird, um die Sichtweise der Nutzer (medizinisches Personal sowie Patienten) einzubeziehen und die Technikgestaltung in ihrer Weiterentwicklung zu beeinflussen. Das macht es notwendig, die „black box" der speziellen Technik zu öffnen, um ihre speziellen Eigenschaften zu erkennen und besser bewerten zu können.

Diese konstruktive Methode wirft insbesondere Licht auf die Doppelrolle von TA-Forschern, in der sie gleichzeitig sowohl Beobachter als auch Akteure sind. TA-Forscher müssen daher ständig die Balance zwischen organisatorischen Gesichtspunkten sowie den kritischen erkenntnistheoretischen und ethischen Fragstellungen wahren: beispielsweise in der Frage, wie die für das Gelingen des Projekts notwendige Begeisterung erhalten werden kann, ohne jedoch dem zu verfallen, was Oppenheimer „die technische Faszination" nannte.

Im Verlauf des Projekts wurden weitere zentrale Schlüsselfragen bei der Anwendung einer konstruktiven TA-Methode deutlich:

* die Öffnung der technologischen „Black Box",
* die Meinungsverschiedenheiten, Verhandlungen und Kompromisse zwischen den unterschiedlichen am Projekt beteiligten Akteuren (Experten, Praktikern, Krankenpflegern, ...),
* der Umgang mit dem unterschiedlichen Einfluß der Akteure auf das Projekt,
* die Lösung von Kontroversen zwischen Akteuren und deren Rückwirkungen auf die Technik,
* die Beteiligung „passiver Akteure" wie Patienten, Verwaltungsangestellte, ...

Die Evaluation

Zur Durchführung der Evaluation erstellten die Forscher, gemeinsam mit den Hämatologen des Krankenhauses, ein Bewertungsraster, um die Vorteile und Risiken für jeden Akteur zu sammeln und systematisch zu diskutieren. In diesem Raster wurden einige zentrale Fragestellungen analysiert, was im folgenden dargestellt wird.

Die möglichen Vorteile für die Hämatologen des Krankenhauses bestehen beispielsweise in einer verbesserten Kommunikation des medizinischen Personals; der Verringerung medizinischer Fehler (was, unter den oben erwähnten Bedingungen, natürlich auch einen Nutzen für den Patienten darstellt); präziseren Diagnosen; effektiveren Therapien sowie einem gesteigerten Wert (u.a. im Prestige und in der Personal- und Rechnerausstattung) der Hämatologie-Abteilung. Auf der anderen Seite können einige Risiken vorkommen, wie Bedienungsfehler wegen unzureichender oder mangelhafter Ausbildung im Umgang mit Computern; höhere zugewiesene Verantwortung im Fall eines medizinischen Fehlers; vereinfachte Kontrolle der Verschreibungszahlen durch die Sozialversicherungsbehörden usw.

Für den Patienten und seine Angehörigen können sich durch die Einführung einer Karte beispielsweise folgende möglichen Vorteile ergeben:

- Vereinfachung von Verwaltungsabläufen,
- freie Wahl des Arztes durch den Patienten, wenn Ausstattung und Abläufe standardisiert sind und das Recht des Patienten auf informationelle Selbstbestimmung geachtet wird. Im Fall eines medizinischen Fehlers kann mit Hilfe der Karte die Verantwortlichkeit eines Arztes belegt werden.
- Zugriff auf korrekte und relevante Gesundheitsinformationen, wenn die Karte regelmäßig aktualisiert wird und der Patient der Speicherung der vollständigen Informationen zustimmt.

Im Gegensatz zu den Vorteilen kann ein Mißbrauch der Karte zu riskanten Situationen führen wie: Unethische Benutzung von Informationen (durch Versicherungen, Arbeitgeber usw.); Verletzung der Intimsphäre, Sicherheit und Zuverlässigkeit des Systems; Zerstörung oder Veränderung (beabsichtigt oder versehentlich) der medizinischen Information; Verlust der Karte; oder Diskriminierungen (beispielsweise durch die Einrichtung eines geschlossenen Gesundheitssystems, in dem nur diejenigen behandelt werden dürfen, die eine Karte besitzen). Darüberhinaus bestehen medizinische Risiken, wenn sämtliche Aufzeichnungen in einem vordefinierten und codierten (Anm. d. Ü.: und damit u. U. in ihrer Ausdruckskraft beschränkten) Format vorliegen.

Bezüglich organisatorischer Abläufe innerhalb der Hämatologie-Abteilung könnte die Verwendung einer Karte eine genauere Aufgabendefinition für jeden Beschäftigten im Gesundheitswesen, sowie mehr Verantwortung der Krankenpfleger bei der Handhabung von Karten bewirken, wenn Ärzte und Krankenpfleger vertrauensvoll zusammenarbeiten. Jedoch kann die Karte auch zu zusätzlicher Arbeit für Hilfspersonal wie Ärzte in der Ausbildung, Krankenpfleger oder Verwaltungspersonal führen, wenn die Ärzte die Daten nicht selbst eingeben wollen.

Betrachten wir das Krankenhaus als Ganzes, kann die Karte eine bessere medizinische Verständigung zwischen verschiedenen Abteilungen bewirken, wenn das gesamte Informationssystem angemessen ist und das Kartensystem zu diesem System im Einklang steht. Anderenfalls könnten größere Spannungen zwischen verschiedenen Abteilungen entstehen, wenn kein kompatibles System zur Verfügung steht („a two-speed-system").

Betrachtet man das Zusammenspiel der Hämatologie-Abteilungen verschiedener Krankenhäuser im größeren Zusammenhang, wird es eine Übereinstimmung in bezug auf die Pflege geben, wenn erst die Ausstattung und die Protokolle standardisiert sind. Somit könnten wir eine Verringerung überflüssiger Untersuchungen und Behandlungen erwarten - und damit eine Verringerung der Kosten im Gesundheitswesen.

Daneben müssen einige Betrachtungen im Umfeld der epidemologischen Forschung angestellt werden. Eine regelmäßige Aktualisierung der Karte könnte die Erstellung von Datenbanken und statistischen Analysen ermöglichen - sofern ein korrektes Sicherungssystem und die Garantie von Datenanonymität gegeben sind. Außerdem könnte die Karte zu einer Verbesserung der Gesundheitserziehung und Patienteninformation beitragen. Wenn die verschiedenen Berufsgruppen jedoch nicht kooperieren, werden die Statistiken unvollständig und unzuverlässig sein.

Übersetzt aus dem Englischen von Harald Selke und Inge Allinger. ■

Ausgewählte Literatur:

BERLEUR J., NGUYEN N. T. and DELHAYE R. (1995), Technology Assessment for Decision Making in the Field of Informatics in Medicine and Health Care. Controversies Analysis and Scenarios Building, in: VAN GENNIP E.M.S.J. and TALMON J.L. (eds.), Assessment and Evaluation of Information Technologies in Medicine, A Handbook of ATIM Group, IOS Press, Amsterdam, Studies in Health, Technology and Informatics, Nr 17, Jan. 1995, pp. 127-139.

NGUYEN N.T. et al, „Risks and benefits of Computerized Health Cards, a case study", in Facing the challenges of risks and vulnerability in an information society, J. Berleur ed., North Holland, 1993.

NGUYEN N. T., LOBET-MARIS C., BERLEUR J. & KUSTERS B., Methodological Issues in Information Technology Assessment, in: International Journal of Technology Management, Special Issue on Technology Assessment, Inderscience Enterprises Ltd., 1995

NGUYEN N. T., FOUREZ G., DIENG D. (1995), La santé informatisée? La carte-santé et des interrogations ethiques, De Boeck Université, Bruxelles, avril 1995

Michael Möhring

Modellversuche zur Einführung von Patientenchipkarten

Anspruch und Wirklichkeit am Beispiel Koblenz/Neuwied

Seit Ende 1995 läuft in Neuwied bei Koblenz ein Modellversuch zur Einführung von Patientenchipkarten im Gesundheitswesen. Die hierbei eingesetzte Karte soll sowohl medizinische Daten über den Gesundheitszustand seines Inhabers enthalten, orientiert am Datensatz für den europäischen Notfallausweis, als auch über die in Apotheken erhaltenen Medikamente informieren. Den Projektinitiatoren und -betreibern, es handelt sich um die kassenärztliche Vereinigung Koblenz (KVK), das Zentralinstitut für die kassenärztliche Versorgung der BRD (ZI) und die Bundesvereinigung Deutscher Apothekerverbände (ABDA), geht es bei diesem von Chipkarten- und Lesegeräteherstellern unterstützten Modellversuch nach eigenen Aussagen vor allem darum, Erfahrungen beim konkreten Einsatz einer solchen Technik zu sammeln. Hierzu gibt es eine vom ZI durchgeführte wissenschaftliche Begleitforschung, in der nach Abschluß des Modellversuchs, in Anlehnung an die Vorgehensweise bei der Einführung der Krankenversicherungskarte, eine schriftliche Befragung unter den Beteiligten (Ärzte, Apotheker, Patienten) durchgeführt wird.

Auf Initiative von Claus Stark, Medizininformatiker an der Fachhochschule Heilbronn, fand im November 1995 in Koblenz ein Workshop statt, auf dem der Frage nachgegangen wurde, inwieweit die Beteiligung von Bürgern bei der Gestaltung von Patientenchipkarten wünschenswert und machbar ist ([Stark/Schmiede 95]). Als ein Ergebnis dieses Workshops bildete sich eine Arbeitsgruppe mit dem Ziel, Möglichkeiten einer Bürgerbeteiligung zu erarbeiten und im Rahmen des Neuwieder Modellversuchs umzusetzen. Grundlage hierfür war die Aussage des Vertreters der Projektleitung, eine konstruktive Mitarbeit durch Bürger- und Patientengruppen sei grundsätzlich möglich und erwünscht, da es sich um ein rein wissenschaftliches Projekt handele, in dem die Patienteninteressen die wichtigste Rolle spielen.

Betrachtet man die grundsätzlichen Rahmenbedingungen der Einführung von Patientenchipkarten, so scheint für eine wirksame Beteiligung von Betroffenen(gruppen) tatsächlich eine günstige Konstellation vorzuliegen:

- Eine gesetzlich verbindliche Einführung von Patientenchipkarten wird es, so der Bundesgesundheitsminister auf der „Health Card 95", nicht geben. „Durchsetzen werden sich vielmehr diejenigen Lösungen, die dem tatsächlichen Bedarf der Beteiligten im Gesundheitswesen am besten entsprechen" (zitiert aus [a la Card 1995, S. 3]).
- Es gibt noch keine Standards für die einzusetzende Kartenarchitektur (z.B. Prozessor, Speicher), Schreib-/Lesegeräte, Datensatzstrukturen und Sicherheitskonzepte (z.B. Verschlüsselung, Signaturen), ein Spielraum für Gestaltung ist also vorhanden.
- Die Erprobung dieser Technik in einem Modellversuch bietet die Möglichkeit, Erfahrungen direkt Betroffener zu erheben und im Rahmen der installierten wissenschaftlichen Begleitforschung zu analysieren.

Zusätzlich ermöglicht die zweistufige Anlage des Modellversuchs (ab Mitte 1996 soll der Modellversuch von Neuwied auf die Nachbarstadt Andernach ausgedehnt werden) nicht nur eine Untersuchung der Folgen von Patientenchipkarten sondern zusätzlich die Umsetzung der aus der Wirkungsanalyse entwickelten Gestaltungsvorschlägen in dem Folgeprojekt.

Betrachtet man dagegen den Modellversuch und - soweit bekannt - das Konzept der wissenschaftlichen Begleitforschung etwas genauer, so ergeben sich sowohl inhaltlich als auch methodisch eine Reihe von Problemen, die für die Beurteilung der realen Möglichkeiten einer Bürgerbeteiligung von Bedeutung sind.

Modellversuche werden methodisch der Feldforschung zugerechnet, die im Bereich der Technikbewertung [VDI 1991, S. 55] als erfolgversprechend gelten, Erfahrungen direkt Betroffener im alltäglichen Umgang mit einer neuen Technik zu zu sammeln. Sie bilden damit eine Ergänzung zu Methoden (z.B. Szenarios), in denen Erkenntnisse (z.B. prognostizierte Wirkungen, Entwicklung von Gestaltungskriterien) eher theoretisch gewonnen werden [Bizer u.a. 1995, S. 55].

Die Bedingungen für das Sammeln von Erfahrungen im Neuwieder Modellversuch sollen an einigen Beispielen erläutert werden:

Im Zusammenhang mit vermuteten Effekten einer Patientenchipkarte für den einzelnen Patienten stehen vor allem die positiven Auswirkungen auf das Arzt-Patient-Verhältnis (Stichwort: Mündiger Patient) und die Verbesserung medizinischer Leistungen (z.B. bzgl. Betreuungsintensität, Diagnosen, Notfälle, Arztwechsel) durch die bessere Nutzung bereits vorhandener Daten im Vordergrund [BSI 1995, S. 32ff]. Unabhängig davon, welche Veränderungen die Beziehung zwischen Arzt und Patient durch die Verwendung einer Chipkarte wirklich erfährt: Sie werden sich nur sehr langsam und allmählich vollziehen, da Voraussetzung hierfür Routine im Technikumgang ist, besonders in diesem neuen Anwendungszusammenhang. Bei der bisher veranschlag-

ten Laufzeit des Modellversuchs in Neuwied von maximal einem Jahr sind Erfahrungen in diesem Bereich nicht zu erwarten. Ähnliches dürfte auch für die Erfahrungen mit Chipkarten bei Arztwechsel, Kartenverlust oder bei Änderungswünschen im Datensatz gelten.

Wesentliche Voraussetzung für eine bessere Nutzung bereits vorhandener Daten ist die Verläßlichkeit der auf der Chipkarte gespeicherten Daten. Die in diesem Modellversuch getroffenen organisatorischen und technischen Regelungen stellen diese Verläßlichkeit in keiner Weise sicher, d.h. darauf aufbauende Erfahrungen hierzu sind nur beschränkt aussagekräftig:

- Das Fehlen eines Eintrags im Datensatz kann bedeuten, daß entweder der betreffende Befund nicht vorliegt oder aber der Patient den Eintrag nicht gewünscht hat.
- Ein Patient kann sich mehrere Chipkarten mit unterschiedlichen Datensätzen anfertigen lassen.
- Es sind keine Signaturverfahren zur Authentisierung eingetragener Daten vorgesehen.

Schließlich werden im Modellversuch explizit Problembereiche ausgeklammert, zu denen praktische Erfahrungen im Hinblick auf eine Großanwendung notwendig wären. Als Beispiel sei hier die Speicherung der Patientendaten auf die Chipkarten (Personalisierung) genannt, die aus technischen Gründen zentral bei der Kassenärztlichen Vereinigung nach einem vom Datenschutzbeauftragten in Rheinland-Pfalz fest vorgeschriebenen und genehmigten Verfahren erfolgt. Die Erprobung einer Erfassung, Änderung und Löschung von Patientendaten direkt in den Arztpraxen mit all ihren sicherheitstechnischen und datenschutzrechtlichen Problemen ist also nicht möglich. Gleiches gilt für den vorausgesagten Nutzen von Chipkarten bei Notfällen, da es nicht vorgesehen ist, Notfalleinrichtungen (z.B. Rettungsfahrzeuge, Unfallstationen) mit Lesegeräten auszurüsten.

Neben diesen eher inhaltlichen Problemen bleiben auch methodische Fragen offen. So ist zweifelhaft, ob die Erhebung von Patientenerfahrungen allein mittels schriftlicher Befragung ausreicht. Berücksichtigt man, daß ein Schwerpunkt von Feldforschung gerade die detaillierte Untersuchung subjektiven Handelns im Alltag ist [Bizer u.a. 1995, S. 56] und daß mit der Arzt-Patient-Beziehung die individuellen Erfahrungen in einem besonders sensiblen Bereich von Interesse sind, erscheinen eher qualitative Verfahren wie zum Beispiel das offene Interview - zumindestens ergänzend - sinnvoll. Weiterhin wäre es wünschenswert, wenn nach Abschluß des Neuwieder Modellversuchs zur Verifikation der Ergebnisse und als Vorbereitung für die Gestaltung der zweiten Versuchsphase in Andernach Gruppengespräche veranstaltet würden, um die Versuchsteilnehmer mit den Ergebnissen zu konfrontieren und bei denen es zu einem Dialog zwischen Patienten, den Projektbetreibern und Wissenschaftlern kommt.

Als Fazit bleibt festzuhalten, daß erst die Untersuchung des Modellversuchs im Detail Hinweise auf seine realen Möglichkeiten und Grenzen liefert. Günstige Rahmenbedingungen und der Einsatz einer potentiell erfolgversprechenden Methode für eine beteiligungsorientierte Technikbewertung allein reichen für eine Beurteilung nicht aus. Die Projektbetreiber haben sich für einen umfassenden individuellen Freiraum der PatientInnen beim Umgang mit den Chipkarten entschieden. Dies vermindert zweifellos das Konfliktpotential innerhalb des Modellversuchs. Es führt aber auch dazu, daß Erfahrungen zu prognostizierten Wirkungen in Teilbereichen überhaupt nicht gemacht werden können, und somit wichtige Ziele des Modellversuchs, zumindestens aus Sicht von PatientInnen, verfehlt werden. Verstärkt wird dieser Effekt zusätzlich durch einige organisatorische Regelungen (z.B. Zeitrahmen, Personalisierung der Chipkarten). Wohlgemerkt geht es hier nicht darum, den Test potentiell denkbarer, restriktiverer Regelungen zu fordern, die, sofern datenschutzrechtlich bedenklich, auch in einem Modellversuch nicht durchsetzbar wären - hier enden die Möglichkeiten einer Feldstudie -, sondern um die Erprobung von Einsatzbedingungen, wie sie für eine Großanwendung, und nur in diesem Rahmen macht der Einsatz von Chipkarten Sinn, realistisch sind.

Die genannten Schwachstellen des Versuchskonzepts und der Begleitforschung sind von Patienten(gruppen) bei der Beurteilung ihrer realen Beteiligungmöglichkeiten einzubeziehen, um die verbleibenden Möglichkeiten der Einbringung von PatientInneninteressen (z.B. Mitgestaltung des Fragebogens) einschätzen und optimal nutzen zu können. Gleichzeitig sollte auch auf anderen Ebenen der Meinungs- und Erfahrungsaustausch mit PatientInnen gesucht (z.B. durch Informations- und Diskussionsveranstaltungen) und, im Sinne der von den Projektbetreibern proklamierten Offenheit des Modellversuchs, Gestaltungsvorschläge bzgl. der Konzeption des Modellversuchs und der wissenschaftlichen Begleitforschung - zumindestens für das Folgeprojekt - eingebracht werden. ■

Literatur

[a la Card 1995] M. Wolff. Editorial. a la Card Aktuell (1995)33, S. 3.

[Bizer u.a. 1995] Bizer, M.; R. Grimm; V. Hammer (u.a.). Rechtsverbindliche Telekooperation in der elektronischen Vorgangsbearbeitung. Sank Augustin: GMD, 1995. (GMD-Studien, Nr. 261).

[BSI 1995] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.). Chipkarten im Gesundheitswesen: Technikfolgen-Abschätzung zur Sicherheit in der Informationstechnik. Köln: Bundesanzeiger, 1995.

[Stark/Schmiede 1995] Stark, C.; Schmiede, R.: Ist Bürgerbeteiligung bei der Gestaltung einer Patientenchipkarte wünschenswert und machbar?, in: Datow, M. et al (Hrsg.): MultiCard '96 - Die Chipkarte im Alltag, Berlin: intime, 1996.

[VDI 1991] Verein Deutscher Ingenieure (Hrsg.). Technikbewertung: Begriffe und Grundlagen. Berlin: Beuth, 1991. (VDI-RIchtlinie 3780).

Projekt Bürgerbeteiligung in Koblenz

Wer Interesse am Projekt "Patientenchipkarte & Bürgerbeteiligung" hat, kann von Claus Stark (FIFF Heilbronn, siehe Adressen) eine Liste mit verfügbarem Material und Literatur anfordern. Im Internet-WWW sind einige der Artikel verfügbar: http://zeus.stud.fh-heilbronn.de/~stark/chipkarten.html.

Hans-Jürgen Jonas

PatientInnen-Tagebücher statt digitalisierter Krankenakten

Kommentar zu Chipkarten im Gesundheitswesen

Unter der irreführenden Bezeichnung »Patientenchipkarte« werden mittlerweile im Freilandversuch erste Machbarkeitsstudien für eine Digitalisierung von ärztlichen Krankenakten durchgeführt. Irreführend deshalb, weil den PatientInnen bei diesen Planungen wiedermal nur eine Statistenrolle zugedacht wurde. Denn die notleidende heimische Chipindustrie hat das Gesundheitswesen als Absatzmarkt entdeckt .Seither wird sie nicht müde, für jeden nur erdenklichen Bereich ihre »digitalen Wunderkärtchen« als Problemlösung feilzubieten. Motto: Was technisch machbar ist, muß auch gemacht werden.

Aber Chipkarten im Gesundheitswesen bergen nicht nur ein erhebliches Risikopotential, sondern sind auch schlichtweg überflüssig. Für jeden Anwendungsbereich lassen sich sozialverträglichere, umweltfreundlichere und billigere Alternativen benennen. Einfaches Beispiel: Die Bezahlung von ÄrztInnen nach aufgewendeter Arbeitszeit und Anzahl der behandelten PatientInnen, statt nach kostentreibender Einzelleistungsvergütung, entzöge dem gesamten System von Datenerfassung und -austausch den Boden. Die Krankenversicherten-Chipkarten wären mit einem Schlag in die Alben von PlastikkartensammlerInnen verbannt.

Nicht viel anders verhält es sich mit den medizinischen Chipkarten. Zugegeben: Medizin und ärztliches Handeln sind stellenweise schon so weitgehend formalisiert, daß ihre Digitalisierung nur noch als »logische Konsequenz« erscheint. Allerdings ist damit doch noch nichts darüber gesagt, ob diese Entwicklung für eine humane Medizin tatsächlich auch sinnvoll oder gar unverzichtbar ist. Und genau hierüber muß die Diskussion geführt werden. Bezogen auf die Krankenakte lautet die Frage folglich: Welchen Vorteil bietet eine elektronische Krankenakte und - weitaus wichtiger! - inwieweit kann sie zur Verbesserung der Kommunikation zwischen PatientInnen und ÄrztInnen insgesamt beitragen?

Die Einführung medizinischer Chipkarten, so das zentrale Argument der Befürworter, sei vor allem auch für die PatientInnen von Vorteil, denn endlich würden ihnen »ihre Daten in die Hand gegeben«. Das klingt nicht übel, ist aber leider schon im Ansatz falsch: Folgt man der gängigen Rechtssprechung, so gehören die Daten in den Krankenakten gar nicht den PatientInnen, sondern den AktenbesitzerInnen, den ÄrztInnen. Denn Krankheitsdaten von PatientInnen seien - so die Begründung - gewissermaßen transformiert durch ärztliches Denken zu medizinischen Befunden usw. geworden, sozusagen »Produkt der ärztlichen Heilkunst«. Immerhin wird den PatientInnen, da sie ja irgendwie an der Entstehung dieser medizinischen Daten beteiligt sind, das Einsichtsrecht gewährt, zumindestens auf dem Papier. In der alltäglichen Praxis erweist sich die Einsichtnahme in die Krankenakte dagegen immer noch als schwierig, trotz klarer rechtlicher Regeln. Selbst wenn also das Einsichtsrecht auf die elektronische Krankenakte technisch realisierbar ist und auch juristisch eindeutig geregelt würde, wäre fraglich, ob PatientInnen es auch realisieren könnten. Aber selbst dann bliebe das »Urheberrecht« in jedem Fall weiterhin in der Hand der ÄrztInnen.

Will man PatientInnen tatsächlich zum Herr bzw. zur Frau über seine/ihre Daten machen, beläßt man die medizinische Daten am besten gleich in ihren Händen. Ein PatientInnen-Tagebuch ist eine Technik, die nicht erst erfunden werden muß, sondern bereits weit verbreitet ist. Allerdings führen solche Tagebuchaufzeichnungen bisher noch ein Schattendasein, sozusagen als subjektive Ergänzungen oder Anhängsel der »echten« medizinischen Befunde. Dabei sind Patientinnen-Tagebücher in einem produktiven Sinn Kranken-Geschichte, statt der reduzierten Version einer Krankheits-Geschichte in Form einer Sammlung isolierter Daten. In der Kommunikation zwischen PatientInnen und ÄrztInnen könnten PatientInnen-Tagebücher einen Perspektivwechsel einläuten: ÄrztInnen müßten auf die Fragen der PatientInnen eingehen und Antworten in deren Sprache formulieren helfen. PatientInnen wären dann tatsächlich auch UrheberInnen ihrer »Daten«, in die sie auch die »Einsicht« hätten, und zwar nicht mehr nur in einem formaljuristischen Sinn. Und ÄrztInnen wären in erster Linie wieder BegleiterInnen von Gesundheits- bzw, Krankheitsgeschehnissen, statt BeHandlerInnen pathologischer Prozesse.

Aber auch für den Erfahrungsaustausch von PatientInnen untereinander bieten sich Tagebücher an, etwa um Erkenntnisse kommunizierbar zu machen, wie sie aus konkreten Lebenszusammenhängen gewonnen werden können und nicht aus der abstrakten medizinischen Wissenschaft. Medizin ließe sich nicht mehr nur auf biologische Prozesse reduzieren - krankheitsverursachende Arbeits- und Umweltbedingungen wären nicht mehr so einfach zu medikalisieren.

Und weil Technik eben doch nicht neutral ist, stellen PatientInnen-Tagebücher nicht bloß eine Alternative zu medizinischen Chipkarten dar, sondern sind ein Baustein für eine ganz andere Medizin. Und das Gute daran: Jede und Jeder kann heute noch damit anfangen.

Marina Steindor

Patienten-Chipkarte – Zielscheibe für massive Kritik

Ein politischer Kommentar

Blinde Flecken im Datenschutz, ein völlig unzureichender Patientenschutz und mangelnde Mitwirkung der Betroffenen bei den weitreichenden Entscheidungen zur Umstrukturierung des Gesundheitswesens - so lautet 1995 die Bilanz einer verfehlten Gesundheitspolitik der Bundesregierung. Während die Regierung bereits mit dem Gesundheitsstrukturgesetz (GSG) den Rahmen für Entwicklung und Anwendung von Chipkarten geschaffen hat, hat sie ansonsten allein auf das Modell "schlanker Staat" gesetzt und sich bei der Gefahrenvorsorge gänzlich aus der Verantwortung gezogen. Auch im kommenden Jahr will die Bundesregierung nichts dazu beitragen, diese Defizite zu beheben. Dies belegt meine Kleine Anfrage zu den Auswirkungen des Einsatzes von Chipkarten im Gesundheitswesen (BT-Drs. 13/3001), die ich im Herbst dieses Jahr [1995] im Bundestag stellte.

Aus der Antwort der Bundesregierung geht hervor: Studien, wie Patienten-Chipkarten das Arzt-Patient-Verhältnis beeinflussen könnten oder welche Kontrollpotentiale im Einsatz von Chipkarten für Beschäftigte liegen, sind der Bundesregierung nicht bekannt. Forschungsvorhaben über eine patientenorientierte Dokumentation will sie nicht finanzieren; risikoärmere Alternativen zur Verdatung sind für sie kein Thema. Keinerlei Informationen besitzt die Bundesregierung darüber, wie der Datenschutz bei den Krankenkassen gesichert ist. Gesetzliche Regelungen hält sie "derzeit für verfrüht". Dabei hat die Konferenz der Datenschutzbeauftragten aus Bund und Ländern bereits im März 1994 bereichsspezifische Rechtsgrundlagen angemahnt und diese Forderungen 1995 nochmals bekräftigt.

Chipkarten sind Bestandteil einer weltweit einmaligen Infrastruktur zur elektronischen Verarbeitung von Patientendaten nach dem GSG. Der elektronische Datenaustausch führt dazu, daß die Krankenkassen umfassend und detailliert Einblick in das Leistungsgeschehen zwischen Arzt und Patient nehmen können. Um Leistungsdaten auch kassenübergreifend auswerten zu können, werden Millionen sensibler Gesundheitsdaten an ein Privatunternehmen, die Daimler-Tochter debis Systemhaus, übermittelt. Die Krankenkassen erarbeiten bereits "Auswertungsmuster", um diese riesigen Datenmengen zur Kontrolle von ÄrztInnen und PatientInnen zu nutzen. Ein entsprechendes Pilotprojekt der Krankenkassen in Bayern fördert das Bundesgesundheitsministerium mit 1,3 Millionen DM.

Doch 1995 ist deutlich geworden, daß diese tiefgreifenden Veränderungen des Gesundheitswesens bei Patienten wie Ärzte auf massive Kritik stoßen. Sie wehren sich gegen Kontrollen und Eingriffe in die medizinische Behandlung. Dies zeigt deutlich den Protest gegen die computergerechte Verschlüsselung von Dignosen, an der sich sämtliche Patientenstellen und über 30.000 Ärzte beteiligen.

Die Umstrukturierung des Gesundheitswesens kann nicht von Lobbys gegen die Interessen von Patienten und Ärzteschaft durchgesetzt werden. Deshalb muß das kommende Jahr [1996] im Zeichen der Partizipation und der problemorientierten Debatte stehen. Ansonsten ist die Einführung medizinischer Chipkarten von vornherein zum Scheitern verurteilt.

Dieser Artikel ist erschienen in:
à la CARD aktuell, Heft 3, 1996, Mölln. ■

Karl Kollmann

Die »Smartcard«

Eine Facette beim Weg in den Überwachungsstaat?

Vorbemerkung

Die Smartcard[1] als universelles Transaktionsmedium hat zweifellos ihre Reize, und natürlich: ihre Probleme. Da Probleme in unserer Lobby-dominierten und mit Marketingmitteln der Anbieter unterfütterten Medienwelt - und damit der Alltagswirklichkeit - meist nicht so gut auf den Tisch kommen, widmet sich der vorliegende Beitrag in erster Linie diesen Problemen.

Die elektronische Verdinglichung

Um die „elektronische Verdinglichung" in ihren Tiefenschichten zu verstehen, muß man, so glaube ich, ein bißchen ausholen, und die sozusagen klassische Verdinglichung der Bürger unserer modernen Gemeinwesen noch einmal kurz skizzieren. Der Sachverhalt der „Verdinglichung" für die Bewegungsformen und Aktionsmöglichkeiten des Individuums in seinen modernen Umwelten ist ab einem gewissen intellektuellen Niveau in der Auseinandersetzungsfähigkeit mit der Realität eigentlich recht unbestritten.

Die Reduktion individuell möglicher Vielfalt auf Aktenzahlen, Sozialversicherungsnummern, standardisierte Vorkommnisse, Aktivitäten, Handlungen und Denkmuster ist uns allen ja seit vielen Jahren geläufig. Zwar nicht in allen Feinheiten natürlich, aber in groben Typen können wir Menschen heute nicht nur eingeteilt und zugeordnet, sondern auch prognostiziert werden. Die quantitative Sozialforschung, sogar jeder Fragebogen auch eines noch so ambitionierten Forschungsprojekts, belegt das. Auch in den ganz persönlichen privaten Beziehungen „instrumentalisieren" wir bewußt und unbewußt andere Menschen, setzen sie 'politisch' (seien es intime Beziehungen, Vereinsangelegenheiten, Tätigkeiten am Arbeitsplatz oder in Parteien) ein, nutzen und verwenden sie: ihre Gefühle, Meinungen, Stimmungen, Verführbarkeiten. Zum System erhoben ist das „Verdinglichung"[2]; Menschen werden zur Ware. Tatsächlich ist, da eben Menschen heute in vielerlei Hinsicht so miteinander umgehen, der Kern sozialer Aktivitäten und Beziehungen ein ökonomischer - auch dort wo es noch nicht um wirtschaftliche Fragen geht.[3]

Reduktion: Eindimensionalisierung

Zahlen die Menschen nun mit einer Karte, statt wie bisher mit Münzen und Geld, bringen sie jetzt ihre Krankengeschichte nicht mehr in einem Stapel Papier, sondern in einem Chip zum Arzt mit, werden sie nicht mehr von einem menschlichen Portier, sondern vom elektronischen Gerät identifiziert und im Routinefall dann in das Gebäude, wo ihre Erwerbsarbeit stattfindet, eingelassen, dann verändert sich zwar nichts daran, daß Menschen für den Sachbearbeiter, den Arzt, den Vorgesetzten bearbeitbare, handlebare Personen, Sachverhalte, Dinge sind. Nein, das nicht, aber zwischen den routinisierten Vorgang des 'Gegenüber' und den Betroffenen schiebt sich über diese vorhin erwähnte ökonomische Interaktion, quasi als Hülle, ein weiteres Medium: die Elektronik.

Die Interaktions-"Schnittstelle" zum Einzelnen und zwischen diesen Einzelnen, die ich vorhin mit Bedacht als die Betroffenen bezeichnet habe, wird damit auch gänzlich eindimensional. Daten in standardisierter Form werden da übertragen, kein ergänzendes sensorisches Spektrum wird mehr vermittelt, keine zerknitterten oder funkelnagelneuen Geldscheine, keine verschmutzten Aktenblätter, und kein verschnupftes Aussehen runden Menschenbilder ab - nur Bytes nach ISO-Norm. Der Mensch reduziert auf normierte Informationen.

Entmaterialisierung

Das Problem der Smartcard, die Dokumente der verschiedensten Art, Geldbeträge, Berechtigungen, möglicherweise die gesamte persönliche Dokumentenmappe in digitalisierter Form enthält, liegt nicht so sehr in jeweils einer einzelnen Anwendung, sondern darin, daß die Smartcard in ein paar Jahren die umfassende Universallösung für alle diese Anwendungen sein wird.

Werden Dokumente oder auch Geldbeträge[4] durch digitalisierte Information ersetzt, dann werden sie damit auch entstofflicht und sind sie dies, dann verschwinden sie damit aus der Wahrnehmungsfähigkeit von Menschen. Die tun sich ja ohnedies schon mit materiellem Geld in Form von Münzen und Banknoten schwer, etwa bei einem Kauf Preise in Nutzenrelationen umzusetzen, von ihrer persönlichen Ausgabenplanung bspw. ganz zu schweigen.[5] Bleiben wir gleich beim Geld. Eindimensional ist der alltägliche Umgang mit Geld, weil die Banknote, die Währung insgesamt, intermediär ist. Sie tritt im Endeffekt zwischen meinen persönlichen „Wert" (den erzielten Erwerbsarbeitslohn) und meine materiellen „Werte", nämlich die Wünsche und Möglichkeiten (Kosten der Konsumgüter). Immerhin symbolisiert oder visualisiert die Banknote jedoch diese Werteinheiten noch. Pla-

---

1 Der hier benutzte Begriff „Smartcard" folgt dem Verständnis der Smartcard Solutions Group: Smart Card Home Page, What is a Smartcard? Online im Internet, URL: http://burgoyne.com/pages/kjbarnes/scsg.html.

2 Dies ist nun - zugegeben - eine etwas andere Definition als die bspw. der sog. Frankfurter Schule (Adorno, Marcuse, Horkheimer, Habermas usw..) - aber inhaltlich, in der Sache kommt sie auf's selbe hinaus.

3 Die Austauschtheorie für soziale Interaktionen beschreibt diese wohl empirisch am passendsten (Vgl. dazu bspw. als Klassiker John W. Thibaut, Harold H. Kelley: The social psychology of groups, New York 1966.) Während jedoch Homans noch scharf zwischen der Währung „soziale Anerkennung" im sozialen Feld und der Währung Geld im ökonomischen Bereich unterscheiden konnte, gelingt dies heute wohl nicht mehr so gut, da sich soziale Anerkennung vielfach auf Konsumsachverhalte bezieht (vgl. George Caspar Homans: Elementarformen sozialen Verhaltens, Köln 1968, S 30.).

4 Egal welcher Art finanztechnisch die Transaktionen abgewickelt werden, beim Kartengeld bleiben es für den Verbraucher Geldbeträge, die auf- und abgebucht werden.

5 Den kritischen Blick auf diesen Sachverhalt begründet hat David Caplowitz: The Poor Pay More: consumer practices of low-income families, New York 1963.

stikgeld, insbesondere dann, wenn es ein universelles Zahlungsmittel ist und nicht nur im Urlaub oder auf einer Dienstreise eingesetzt wird wie jetzt bspw. die Kreditkarten, hat diese Visualisierungsfähigkeit nicht.

Da einerseits die Visualisierung der monetären 'Werteinheiten' fehlt, andererseits jedoch die Konsumbudgets nahezu aller Menschen mehr oder weniger deutlich beschränkt sind, verleiten derartige Zahlungsformen natürlich zu einem übereilten „Geldausgeben", zu forciertem Konsum. Die Kontrolle entgleitet dem Betroffenen leicht, da die gewohnten Perzeptionsformen nicht greifen - möglich, daß Kinder, die mit Plastikgeld aufwachsen, diese Probleme nicht haben, für viele aber wird das ein Problem: Die technologischen und damit kulturellen Veränderungen sind heute so schnell geworden, daß sie dem biologischen Menschenleben[6] sozusagen davonlaufen.

Verlust der persönlichen Kontrolle

80 Prozent der US-Amerikaner finden heute schon, daß sie die Kontrolle über ihre eigenen persönlichen Informationen verloren haben.[7] Mit Informationssystemen und Transaktionsformen, die auf digitalen Technologien, wie der Smartcard basieren, werden das mehr werden.

Überwachungsformen und Kontrolltechniken werden verstärkt auf der Chipkarte basieren, also Zutrittskontrollen zum Arbeitsplatz usw. In Dänemark, Großbritannien und wer weiß noch wo, wird der persönliche Personalausweis auf Chipkartenbasis diskutiert und von (überwachungs) staatlicher Seite wohl favorisiert. Dies steht auch in Zusammenhang mit den EU-Plänen, für EUROPOL umfassende Datensammlungen über EU-Bürger (im Sinne der Verbrechensbekämpfung) anzulegen.[8] Das von den Befürwortern auf den Tisch gebrachte Argument - bei den deutschen Plänen zum Großen Lauschangriff ebenso wie bei den österreichischen zu Lauschangriff und Rasterfahndung - heißt bekanntlich Schutz des Staates vor Organisierter Kriminalität. Daß es bei Mehrheiten sticht, belegen die Meinungsbefragungen immer wieder: Kampf gegen die Kriminalität steht in der Wunschliste der Bürger ganz oben.

Nicht unverständlich, gehen doch die europäischen Staaten bei der Kriminalitätsbekämpfung eher den Weg, diese - deutlich etwa bei der Eigentumskriminalität - zu privatisieren und zu kommerzialisieren: private Alarmanlagen statt sozialpolitischer Ursachenbekämpfung.[9] Das Argument, das in Hinblick auf eine mögliche persönliche Betroffenheit auch von durchaus nicht unintelligenten Zeitgenossen zu hören ist, nämlich: „Na ja, im Grunde können mir Lauschangriff und Rasterfahndung egal sein, denn ich persönlich habe ja eh' nichts angestellt", erinnert schon an besonders ausgeprägtes Wohlverhalten gegenüber der Autorität Staat; in den dreißiger Jahren mag das ein ähnliches Gefühl gewesen sein.

Aber nicht nur von der staatlichen Seite her wird die menschenrechtliche Freiheit der informationellen Selbstbestimmung des einzelnen Bürgers zerniert, sondern auch von den kommerziellen Unternehmungen. Die Smartcard, in Österreich jetzt, Ende 1995, ganz neu als Elektronische Geldbörse eingeführt, wird es interessierten Firmen ermöglichen, über die Formen eines speziellen Kundenservices oder Bonussysteme (Rabattierung) usw. das Kaufverhalten ihrer Kunden mitzuschreiben. Konform zum geltenden Datenschutzrecht werden sie sich dies vom Kunden unterschreiben lassen und seine Unterschrift wohl auch honorieren, etwa mit 5 Prozent Gutschrift vom Rechnungsbetrag. Die Smartcard ermöglicht das: Herr X.Y. kauft freitags abend stets italienischen Rotwein, am Dienstag folgt ein Großeinkauf mit Pampers-Windeln, Fertiggerichten der Marke A, Donnerstag wird Frischware eingekauft...

Meines Erachtens ist es nur eine Frage der Zeit, bis sich für diese geschäftsspezifischen Kundendaten eine Clearingstelle (etwa ein renommiertes Marktforschungsinstitut) herausbildet, und diese noch firmenbezogenen Kundendaten zu einem Käufergesamtbild zusammenfügt. Das gibt es ja jetzt schon bei den EAN-Daten, also den über das EAN-System codierten Artikeln. Nachvollziehen läßt sich dabei bspw., zu welchem Mehrumsatz eine spezielle Werbemaßnahme der Herstellerfirma geführt hat.

Nun wird auf europäischer Ebene auch ein einheitliches System für die Erfassung der Straßenbenützung normiert: die Chipcard für die Maut (Straßenbenützung) soll nicht national unterschiedlich sein, sondern EU-einheitlich. Ist ja auch sinnvoll: verschiedene Systeme sind teuer, kosten mehr, behindern damit den freien Autoverkehr.

Hier kann sich nun in Zukunft eine riesige Datensammlung von individuellen Verkehrsbewegungen ergeben, die für die Sicherheitsbehörden zweifellos verlockend ist. Keine Frage - hier wären zwar auch Systeme denkbar, bei denen die Verkehrsteilnehmer anonym bleiben, aber gemessen an den heutigen Aktivitäten hin zum Überwachungsstaat, scheint dies auf längere Sicht gesehen, die eher unrealistische Variante.

Ausblick...

Neue Technologien setzen sich vehement durch, dafür sorgen die wirtschaftlichen Interessen dahinter. Dies ist auf nationalen Ebenen so und natürlich auch auf europäischer Ebene. Die EU-Kommission fährt ja einen rasanten Wirtschaftskurs, aktuelles Beispiel etwa Gentechnik. Alle Akteure sind dabei von einer pathologisch-hysterisch wirkenden Angst getrieben, zu kurz, zu spät zu kommen, den Anschluß an die internationale Entwicklung zu versäumen, usw.[10]

Genau das jedoch ist heute das grundsätzliche Problem: die Innovationsgeschwindigkeiten in der Verwertung technischer Neuentwicklungen sind zu schnell. Jeder Softwarebenutzer kennt das ja auch aus eigener Erfahrung. Die Skep-

[6] Nach der Jugendzeit bleiben meist Werte, Einstellungen, Geschmäcker und natürlich die Umgangsmuster des Einzelnen mit seiner Lebenswelt relativ stabil, - nach dieser Sozialisationsphase leben aber die Menschen noch im Schnitt 55 Jahre.

[7] EPIC Alert 2.14, 9. November 1995, [5]; Internet; Mailing List CPSR-Announce, <listserv@cpsr.org>.

[8] Vgl. Wolfgang Gast: Gefangen im Datennetz der Eurocops, in: taz 11.11.1995, S 3.

[9] Vgl. Karl Kollmann: Möglichkeiten für „Schlanken Konsum"? in: Journal für Sozialforschung, 34. Jg. 4/1994, S 317-331.

[10] Nicht nur die Unternehmungen und die wirtschaftspolitisch handelnden Akteure, auch die Administration und die gewerkschaftlich orientierten Institutionen. Ein junger sozialdemokratischer Bürgermeister einer Stadt im Süden von Wien will unbedingt ein berührungsloses Personalinformationssystem für die Bediensteten über eine Smartcard realisieren, mit Zustimmung der Personalvertreter übrigens. Modern sein ist alles, und vor den Sachzwängen kapituliert dann selbst eigenes subjektives Unbehagen.

sis in Hinblick auf Sozialverträglichkeit, Umweltverträglichkeit usw. bei den Neuen Technologien ist nicht in erster Linie auf die konkrete Sachtechnik, sondern auf die Geschwindigkeit zurückzuführen.[11]

Ich denke, daß es - setzt sich bspw. die Smartcard als Transaktionsinstrument breiter durch - nur mehr eine Frage der Zeit ist, berührungslose Anwendungen verstärkt einzuführen. Der nächste Schritt scheint dann - weil dies ja an sich nicht unpraktisch ist - die Implantation des Chips, wie das jetzt schon beim Zuchtvieh der Fall ist. Ist der Chip nur intelligent genug, dann - das scheint mir dabei ein gutes, eingängiges Argument zu sein - kann schon bei den ersten Kreislaufschwierigkeiten eines Menschen der Notarzt punktgenau zur Stelle sein.[12] Praktisch, nicht?

Karl Kollmann,
AK-Wien, Abteilung Konsumentenpolitik,
Universitätsdozent an der Wirtschaftsuniversität Wien,
<kollmann@isis.wu-wien.ac.at> ■

[11] Also nicht das Produkt, sondern die rasche Marktdurchdringung und die damit sehr eindimensionalen, unreflektierten und Probleme schaffenden Verwendungskontexte sind das gesellschaftliche Problem.

[12] Vgl. bspw. Frank Unger: Zukunftsszenario L.A. Kommunikationstechnischer Überwachungsstaat? in: Medien Journal 1/1995, S 37-43.

Chipkarten-Service:

Das WZB-Paper P95-203 von Thomas Elkeles und Rolf Rosenbrock kann (gegen 1,- DM in Briefmarken und einen an sich selbst andressierten Briefaufkleber) bestellt werden bei:

WZB
Presse- und Informationsreferat
Reichpietschufer 50
10785 Berlin (Tiergarten)

Die FIFF-Regionalgruppe Heilbronn pflegt eine Leitseite im Internet-WWW mit Texten und Links zum Thema Chipkarten (im Gesundheitswesen) : http://zeus.stud.fh-heilbronn.de/~stark/Welcome.html. Hinweise auf weitere Chipkartenquellen sind sehr willkommen.

Es gibt zwei Entschließungen der Konferenz der Datenschutzbeauftragten zu „Chipkarten im Gesundheitswesen" (vom 9./10.3.1994 und vom 9./10.11.1995). Sie sind beide im Internet-WWW verfügbar - die Links sind über die Heilbronner Leitseite erreichbar.

1995 gab es eine kleine „grüne" Anfrage im Bundestag mit dem Titel „Wirkungen des Chipkarteneinsatzes im Gesundheitswesen" (BT-Drs. 13/3001). Im rheinland-pfälzischen Landtag gab es 1995 eine große SPD-Anfrage „Chancen und Gefahren bei der Verwendung von Chipkarten" (Drucksache 12/6744). Die Antworten der jeweiligen Regierungen sind z.T. sehr interessant. Es ist beispielsweise erstaunlich zu erfahren, wieviel die Bundesregierung nicht weiß ...

Weiterhin gibt es eine umfangreiche Literaturliste zu (Medizinischen) Chipkarten von der FIFF-Regionalgruppe Heilbronn.

Die genannten Texte (Datenschutz-Entschließungen, Anfragen, Literaturliste) können gegen Kostenerstattung bei der Regionalgruppe Heilbronn angefordert werden (siehe Adressen). ■

Weitere Chipkarten-Informationen:

- *Info der Verbraucher-Initiative und der DVD: **Kreditkarten & Co. - Revolution in der Geldbörse ?**, 1,- DM + Verp. und Porto, Verbraucher-Iniative e.V., Breite Str. 51, 53111 Bonn, Tel.: 0228 / 726 33 93.*
- *Info der BAG PatientInnenstellen: **Chip Chip Hurra? Chipkarten im Gesundheitswesen**, 8,- DM incl. Porto + Verp., Gesundheitsladen Köln, Vondelstraße 28, 50677 Köln, Tel.: 0221 / 32 87 24*
- *Faltblatt der Verbraucherberatung Hamburg: **Die Gesundheitschipkarte - Alles auf eine Karte setzen?**, 2,50 DM in Briefmarken für Porto + Verp., Verbraucherzentrale Hamburg, Patientenberatung, Kirchenallee 22, 20099 Hamburg, Tel.: 040 / 35 00 14 - 85* ■

Projekt »Patientenchipkarte und Bürgerpartizipation«

Texte zum Projekt der TH Darmstadt („Gesellschaftliche Bewertung von Chipkartensystemen im Gesundheitswesen": C. Stark, R. Schmiede) sind erhältlich bei: C. Stark, FIFF Heilbronn (siehe Adressen). ■

Christian Reiser

Die österreichische Chipcard

Vorbereitet für den Überwachungsstaat?

Das österreichische Geldausgabeautomatensystem (Bankomaten und Bankomatkassen) wurde von der Garbe, heute EuroPay, einer Tochterfirma der meisten Banken, aufgebaut und betrieben. In Übereinstimmung mit den Banken wurde nach einem gelungenen Bankomatbetrug beschlossen, ab Anfang 1996 zur Erhöhung der Sicherheit die Scheck- und Bankomatkarten mit einem Chip auszustatten. Dieser Chip soll einerseits die bisherigen Funktionen des Magnetstreifens auf Scheck- und Bankomatkarten ersetzen, der für die Bankomaten und Bankomatkassen verwendet wird, andererseits aber auch die zusätzliche Funktion einer elektronischen Geldbörse ermöglichen. Darüber hinaus ist noch Platz für fünf weitere, noch zu definierende Anwendungen. Bei allen bargeldlosen Zahlungssystemen sind zwei Aspekte im Verhältnis zum Bargeld zu beachten: Die Sicherheit und die Anonymität. Diese Punkte werden in den folgenden Kapiteln für die derzeitige Realisierung und für darauf aufbauende zukünftige Anwendungen betrachtet.

Derzeitige technische Realisierung

Die Umstellung der Bankomat- und Bankomatkassenfunktion von Magnetstreifen auf Chip bringt bezüglich der Sicherheit den Vorteil, daß die Karten mit vertretbarem Aufwand derzeit nicht zu fälschen sind. Allerdings wird bis zu einer Umstellung aller Geräte der Magnetstreifen auch noch funktionieren müssen. Bankomat- und Bankomatkassentransaktionen waren noch nie anonym, und daran wird sich auch mit der Chipkarte nichts ändern. Interessant ist jedoch die Sicherheit und die Anonymität der elektronischen Geldbörse. In der derzeitigen Implementierung werden zur Sicherung und Authentifizierung 3DES und RSA verwendet, Algorithmen, die international als sicher angesehen werden. Es kann daher davon ausgegangen werden, daß die Daten auf der Karte nicht zu ändern sind. Durch die Verwendung eines Challenge-Response-Verfahrens ist auch ein Wiedereinspielen einer Transaktion zwischen Karte und Händlerterminal oder Aufladegerät verhindert. Die Händlerterminals sind nicht online mit der EuroPay verbunden, sondern übertragen nur von Zeit zu Zeit den Saldo der Transaktionen. Sobald der Zentralcomputer diesen Saldo bestätigt, werden die zugehörigen Transaktionen gelöscht. Die einzelnen Transaktionen werden nicht zentral gespeichert oder verarbeitet. Die Transaktionen im Terminal sind von der Karte, mit der sie getätigt wurden, elektronisch signiert. Um eventuell duplizierten Karten auf die Spur zu kommen, werden zu zufälligen Zeitpunkten bei zufälligen Händlern zufällige Transaktionen auf ihre Unterschrift geprüft. So glaubt man, mit statistischen Mitteln Betrügereien zu erkennen. Es wird auch im Moment nicht daran gedacht, die elektronische Geldbörse beim Aufladevorgang mit Personen in Verbindung zu bringen. Diese Daten werden nicht gespeichert. Weiters plant EuroPay, Karten herauszugeben, die ausschließlich die Geldbörsenfunktion erfüllen und somit mit Sicherheit nicht mit dem Karteninhaber in Verbindung gebracht werden können, solange sie nicht von einem Konto aufgefüllt werden.

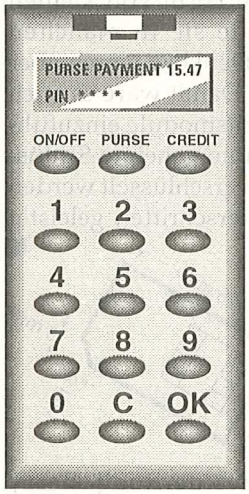
Es gilt noch herauszufinden, welche Möglichkeiten Polizei und Gerichte haben werden, wenn Chipkarten in Zusammenhang mit Straftaten konfisziert werden. Immerhin werden die letzten Bezahlungs- und Aufladevorgänge auch auf der Karte gespeichert. Ob dies als Alibi oder Beweis der Anwesenheit in einer bestimmten Gegend gewertet werden kann, wird sich noch zeigen.

Zukünftige Möglichkeiten

Auch wenn derzeit nur der Saldo der angesammelten Transaktionen aus dem Händlerterminal in den Zentralcomputer übertragen wird, so ist es doch technisch möglich, alle Transaktionen bei der EuroPay zu verarbeiten. Da jede elektronische Geldbörse eine eindeutige Seriennummer hat, wird daraus jede Transaktion verfolgbar. Sobald eine elektronische Geldbörse einmal in Verbindung mit einer Person gebracht werden kann, ließe sich an zentraler Stelle verfolgen, wer zu welcher Zeit wo um welchen Betrag eingekauft hat. Die Karten können einerseits durch einen Aufladevorgang von einem Konto, andererseits aber auch durch gleichzeitiges Auslesen der Bankomat- und Geldbörsenfunktion mit Personen in Verbindung gebracht werden. Es besteht kein technisches Hindernis, alle Bereiche des Chips faktisch zugleich auszulesen. Über die Bankomat- und Geldbörsenfunktionalität hinaus ist vorgesehen, in einer weiteren Ausbaustufe fünf weitere Funktionen zu vermieten. Interessenten könnten zum Beispiel Handelsketten sein, die Kundenkarten auf der Chipkarte unterbringen, um statistische Erhebungen zu Werbezwecken durchzuführen. Was mit diesen Zusatzfunktionen passiert, wird man noch genauer beobachten müssen. Hier sind der Phantasie keine Grenzen gesetzt. ■

Matthias Schunter und Arnd Weber

Sicherheit und Datenschutz für Bankkunden



Das CAFE-Projekt „Conditional Access for Europe" **[BBCM 1_94]**[1] der Europäischen Gemeinschaft hat das Ziel, sowohl ein sicheres portables Benutzergerät „electronic wallet" („elektronische Brieftasche") als auch Chipkarten zu bauen, mit denen anonyme Zahlungen sowie sicherer elektronischer Zugang zu Diensten möglich sind.

Das Institut für Sozialforschung führte verschiedene Befragungen durch **[WCPS_95]**. Hier soll nur auf einige Ergebnisse der Teilbefragung zu den portablen Benutzergeräten und den zur Sicherung dieser Interessen notwendigen Techniken eingegangen werden. Hierbei ging es um kleine elektronische Geräte, die Eingabe und Ausgabe von Daten erlauben. Eingabe erfolgt etwa über Zehnertastatur oder touch screen, Ausgabe über ein LC-Display. Weiterhin kommunizieren diese Geräte per Infrarot mit ihrer Umwelt. Solche Geräte werden oft „electronic wallets" genannt, obwohl sie herkömmliche Brieftaschen nicht vollständig ersetzen können.

Wir beschrieben 123 Kartennutzern in fünf europäischen Ländern die Funktionsweise solcher „electronic wallets" und zeigten diese in einer Simulation. Dabei wurde vorgeführt, daß man mit solchen Geräten sowohl herkömmliche Transaktionen ausführen kann, wie z.B. Kreditkartenzahlungen, als auch mit elektronischem Geld zahlen kann, das wir als ähnlich zu den Guthaben in vorausbezahlten Telefonkarten beschrieben. In den anschließenden Interviews erfuhren wir, daß Kartennutzer folgende Aspekte begrüßen:

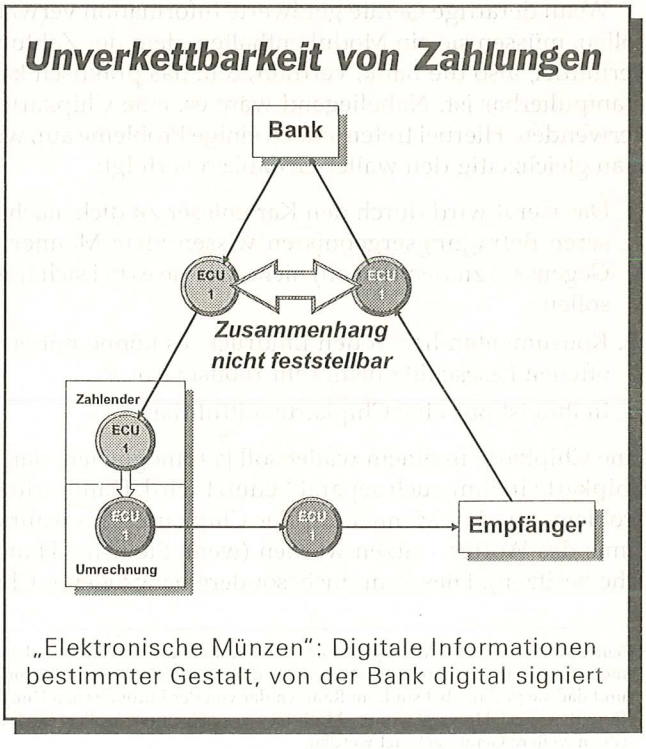
- Sie müssen Zahlungskarten nicht mehr aus der Hand geben.
- Sie können am Display sehen, wieviel Geld sie noch haben bzw. wie hoch der Rechnungsbetrag ist.
- Sie müssen ihre Geheimzahl (PIN) nicht in fremde Geräte eingeben.

Kartennutzer sind sich durchaus der verschiedensten Risiken bewußt, die mit der Kartenbenutzung verbunden sind: Kreditkartenbetrug, Ausspähen der Geheimnummern, Einbehalten von Karten durch Geldausgabeautomaten, etc. Insofern befanden sie, daß sie „ihre elektronische Brieftasche" genausowenig aus der Hand geben möchten, wie ihre herkömmliche.

In anderen Befragungen bestätigte sich, daß Kartennutzer bei Wertkarten vermissen, jederzeit das Guthaben sehen zu können, so wie sie dies beim herkömmlichen Portemonnaie können. Insofern erscheint es sehr attraktiv, solche elektronischen Brieftaschen zu testen.

Im oben erwähnten CAFE-Projekt wurden Chipkarten hergestellt, die unverkettbare Zahlungen im Sinne von Chaum **[Chau_92]** ermöglichen. Mit „unverkettbar" ist hier gemeint, daß Dritte, wie etwa Bank und Händler, nicht feststellen können, wer eine bestimmte Zahlung getätigt hat, und ob mehrere Transaktionen von derselben Person getätigt wurden. Hierbei werden auch keine Kartenidentitäten, Kontonummern oder ähnliches bei der Zahlung weitergegeben, da sonst, selbst bei anonymem Kauf der Karten, sämtliche Aktionen einer Karte verkettbar wären und somit meist auch über eine identifizierende Aktion (z.B. Mietzahlung; Aufladen vom Girokonto) eine Identifikation des Inhabers möglich wäre.

Chaum entwickelte das Konzept für das „blinding" elektronischen Geldes. Hierbei wird das Geld, das der Kunde von der Bank erhält, durch diesen, also durch den Computer des Kunden, verändert. D.h. das Geld, das die Bank an den Kunden gab, ist nicht identisch mit dem, das der Kunde an den Händler gibt und dieser zurück an die Bank. Da dieses elektronische Geld nicht fälschbar sein soll, wird dieses „blinding" mit sogenannten elektronischen Signaturen kombiniert **[Chau_92, DiHe_76, Stal_95]**.



„Elektronische Münzen": Digitale Informationen bestimmter Gestalt, von der Bank digital signiert

[1] Mehr Informationen siehe unter http://www.informatik.uni-hildesheim.de/~sirene. Projektpartner sind Centrum voor Wiskunde en Informatica (NL), Cardware (GB), Gemplus Card International (F), SEPT (F), Royal PTT Nederland N.V. (NL), SINTEF-DELAB (N), DigiCash B.V. (NL), Institut für Sozialforschung Frankfurt (D), Ingenico SA (F), Katholieke Universiteit Leuven Dept. Elektrotechniek E.S.A.T. (B), Mathematisk Institut Aarhus Universitet (DK), Siemens HL AE/IE CC (D), Universität Hildesheim Institut tür Informatik (D).

Im CAFE-Projekt werden nun Chipkarten getestet, die dieses blinde Signieren durchführen. Dieses ist rechenintensiv, da elektronische Unterschriften umgerechnet werden müssen und konkret 150stellige Zahlen potenziert werden müssen. Hierfür hat die Chipkarte einen kryptografischen Coprozessor.[2]

Ein Problem mit diesem Ansatz ist, daß der Kunde ja gar nicht überprüfen kann, was die Chipkarte eigentlich ans Terminal gibt. Hat sie wirklich umgerechnet? Gibt sie nicht zusätzlich die Kontonummer oder eine Kartenidentität weiter? Hat sie sich vielleicht die Geheimnummer des Inhabers gemerkt und gibt sie an einen Insider weiter?

Der individuelle Kunde wird kaum jemals auf Bit-Ebene überprüfen können, was kommuniziert wird. Praktikabel wäre jedoch, wie ebenfalls von Chaum vorgeschlagen **[ChPeI_93]**, daß die Kommunikation der Chipkarte nach außen, also zur Bank und zum Händler, durch ein electronic wallet moderiert wird. Dieses würde das Protokoll mitverfolgen und überprüfen, was kommuniziert wird. Zum Geldabheben würde es die Kontonummer weitergeben, bei Kreditkartenzahlung eine entsprechende Autorisierung, jedoch würde beim Ausgeben von elektronischem Geld jeder unerwünschte Datenfluß unterbunden.

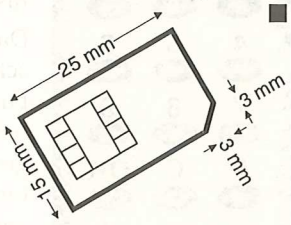
Da die Sicherheit des Benutzers vom wallet abhängt, sollte er diesem Gerät vertrauen. Es sollte also u.a. ein öffentlicher Evaluationsprozeß stattfinden und mehrere potentielle Lieferanten geben **[PPSW_95]**. Es wäre nach diesem Konzept also nicht sinnvoll, daß der Herausgeber der Chipkarte, etwa die Bank, auch das wallet herausgibt und beides vom gleichen Hersteller kommt, womöglich dieselben Chips enthält. Dabei sollte sichergestellt sein, daß das Gerät durch interessierte Verbraucher- oder Datenschützer kontrollierbar ist und daß beliebige Hersteller die Spezifikation zum Nachbau erhalten können (und z. B. Taschenrechner, Laptops, Funktelefone diese Zahlungsfunktionen sozusagen nebenbei ausüben).

Wenn derartige Geräte geldwerte Information verwalten sollen, müssen sie ein Modul enthalten, dem der Zahlungsvermittler, also die Bank, vertraut, d.h. das praktisch kaum manipulierbar ist. Naheliegend wäre es. eine Chipkarte zu verwenden. Hierbei treten jedoch einige Probleme auf, wenn man gleichzeitig den wallet-Gedanken verfolgt:

1. Das Gerät wird durch den Kartenleser zu dick; nach unseren Befragungsergebnissen wissen viele Männer (im Gegensatz zu den Frauen) nicht, wie sie es bei sich tragen sollen.
2. Konsumenten haben den Eindruck, es könne mit einem offenen Leseschlitz nicht sehr robust sein.
3. In ihm ist nur eine Chipkarte mitführbar.

Eine Chipkarte in einem wallet soll ja ermöglichen, daß die Chipkarte in ihm auch separat benutzt wird. Damit tritt das Problem auf, daß Männer auf der Chipkarte - im wahrsten Sinne des Wortes - sitzen werden (wenn Sie keine Handtasche besitzen). Dies kann insbesondere bei größeren Chips, wie sie für Bankkarten erwogen werden, zum Problem werden, da diese dann leicht zerbrechen. Der „Großversuch" in Frankreich mit einer Bank-Chipkarte ist hier nicht unbedingt aussagekräftig, da bei Chipdefekten auf die Magnetstreifenspur umgeschaltet werden kann. Eigene Befragungen von Experten und Konsumenten in Testgebieten elektronischen Chipkarten-Geldes haben die Bedeutung des Problems bestätigt, Statistiken hierzu wurden jedoch nicht veröffentlicht.

Ein Ausweg bestünde in der Einführung kleinerer Sicherheitsmodule. Diese könnten die Form von kleinen Chipkarten (25 x 15 mm) haben, wie sie in manchen GSM-Telephonen verwendet werden. Denkbar wären aber auch andere Formen, Knopfzellen, etc. Damit wäre es auch möglich, in ein wallet mehrere Sicherheitsmodule einzuführen. Ein zweites Sicherheitsmodul könnte geheime Schlüssel enthalten, mit denen Informationen verschlüsselt werden könnten oder sogenannte digitale Unterschriften geleistet werden könnten. ■



[2] Seit Oktober ist das CAFE-System bei der Kommission der Europäischen Gemeinschaften im Test. Insofern ist erwiesen, daß man solche Systeme bauen kann und daß sie praktikabel sind. Im Rahmen der von der Europäischen Union geförderten Special Interest Group „Multi-Currency Electronic Wallet" (SIGMEW) sollen weitere Geräte getestet werden.

Literatur

BBCM 1_94:
Jean-Paul Boly, Antoon Bosselaers, Ronald Cramer, Rolf Michelsen, Stig Mjolsnes, Frank Muller, Torben Pedersen, Birgit Pfitzmann, Peter de Rooij, Berry Schoenmakers, Matthias Schunter, Luc Vallee, Michael Waidner: The ESPRIT Project CAFE - High Security Digital Payment Systems; ESORICS 94 (Third European Symposium on Research in Computer Security), Brighton, LNCS 875, Springer-Verlag, Berlin 1994, 217-230.

Chau_92:
David Chaum: Achieving Electronic Privacy; Scientific American (August 1992) 96-101.

ChPeI_93:
David Chaum, Torben Pryds Pedersen: Wallet Databases with Observers; Crypto '92, LNCS 740, Springer Verlag, Berlin 1993, 89-105.

DiHe_76:
Whitfield Diffie, Martin E. Hellman: New Directions in Cryptography; IEEE Transactions on Information Theory 22/6 (1976) 644-654.

PPSW_95:
Andreas Pfitzmann, Birgit Pfitzmann, Matthias Schunter, Michael Waidner: Vertrauenswürdiger Entwurf portabler Benutzerendgeräte und Sicherheitsmodule; Hans H. Brüggemann, Waltraud Gerhardt-Häckl (ed.): Verläßliche IT- Systeme, Proceedings der GI-Fachtagung VIS '95; DuD Fachbeiträge, Vieweg, Wiesbaden 1995, 329-350.

Stal_95:
William Stallings: Network and Internetwork Security - Principles and Practice; Prentice Hall - IEEE Press, Englewood Cliffs 1995.

WCPS_95:
Arnd Weber, Bob Carter, Birgit Pfitzmann, Matthias Schunter, Chris Stanford, Michael Waidner: Secure International Payment and Information Transfer - Towards a Multi-Currency Electronic Wallet; Project CAFE, Conditional Access for Europe, Frankfurt 1995.

Thilo Weichert

Asyl-Card

Der digitale Flüchtling

1. Das deutsche Projekt

Anfang Januar 1995 schlug der Niedersächsische Landesbeauftragte für den Datenschutz (LfD), Dr. Gerhard Dronsch, Alarm: Er informierte die Öffentlichkeit über die Pläne des Bundesministeriums des Innern (BMI), eine multifunktionale ASYL-CARD zu verwirklichen.

In einem Zwischenbericht der vom BMI koordinierten „Bund/ Länderarbeitsgruppe zur Harmonisierung der Verwaltungsabläufe im Asylverfahren" wurden unterschiedliche informationstechnische Möglichkeiten der Beschleunigung bzw. „Verbesserung" des Asylverfahrens diskutiert. Eindeutig am besten - vor einer noch intensiveren Vernetzung der am Asylverfahren beteiligten Behörden - schnitt dabei die ASYL-CARD ab: Alle Asylsuchenden sollen danach gezwungen werden, eine prozessorgesteuerte Chipkarte mit sich zu führen. Diese soll folgende Funktionen haben: „Identifizierung, Zutrittskontrollfunktionen, Aufenthaltskontrolle, Verfahrensdaten (Antrag, Anhörungen usw.), Empfang von Sachleistungen (z.B. Essensempfang in der Aufenthaltseinrichtung), Empfang von Unterstützungsleistungen, Arbeitserlaubnis, Leistungen von Dritten (z.B. Abrechnung privater Unterkunftsbetreiber). Diese Auflistung ist nicht abschließend". Gespeichert werden sollen auf der Karte auch ein Foto und die „biometrischen Daten eines Fingerabdrucks des Asylbewerbers". Ziel des Chipkarteneinsatzes ist die „Optimierung des Verfahrens durch Minimierung der Verwaltungskosten bei permanenter, bedarfsorientierter Verfügbarkeit von Informationen". Das künftige Verfahren soll sich an folgenden Grundsätzen orientieren: „1. Kein (Asyl-)Antrag ohne ED-Behandlung,[1] 2. ohne ED-Behandlung keine ASYL-CARD, 3. ohne ASYL-CARD keine Leistungen!" Der Mensch wird zum eigenen Datenträger: „Der Karteninhaber sorgt für den Transport der auf dem Chip gespeicherten Daten, indem er die ASYL-CARD, die gleichzeitig als Ausweis dient, bei sich zu führen hat".[2]

2. Die holländische Realität

Inspiriert wurde die im Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl) in Nürnberg geborene deutsche Idee durch den 1992 begonnenen und inzwischen umfassend erfolgenden Einsatz einer ähnlichen Chipkarte in den Niederlanden. Auch dort ist das Ziel ein „effizienteres Asylverfahren". Die Asylsuchenden werden im Anfangsstadium des Verfahrens verpflichtet, sich mehrmals - bis zu viermal täglich - zu vorgegebenen Zeiten an Meldestellen (Meldesäulen) einzufinden und sich durch Einführen der Asyl-Card und Auflegen des Fingers, dessen Abdruck auf der Karte gespeichert ist, zu identifizieren. Unterbleibt die Meldung zweimal unentschuldigt, so wird das Asylverfahren beendet. Der der eindeutigen Identifizierung des Karteninhabers dienende, digitalisierte Fingerabdruck wurde nach kurzer Zeit durch ein digitalisiertes Paßbild ergänzt. Gespeichert sind auch in Holland zunächst die Personalgrunddaten. Da die Karte als offizielles Ausweisdokument gilt, erfolgt die Ausstellung der Karte mit Eintragung der persönlichen Daten sowie Karte und Foto zentral.

Gespeichert werden außerdem: nächste Meldung bei der Meldestelle und bisheriges Meldeverhalten, Verfahrensstand, Angaben zur Arbeitserlaubnis, aktenführende Stelle und Aufenthaltsort, Sozialamt und Sozialleistungen. Bei Verlust der Karte wird eine neue Karte gefertigt. Dazu muß der Asylsuchende bei allen Behörden, die Daten eingespeichert haben, vorsprechen und dafür sorgen, daß die verlorenen Daten wieder aufgeladen werden. Ein mehrfacher Bezug von Leistungen bei derselben Stelle oder bei verschiedenen Stellen an unterschiedlichen Orten soll aufgrund der Datenspeicherung sowohl im Chip der Karte als auch im DV-System der leistungserbringenden Stelle ausgeschlossen werden. Nur ein behördlich gebilligter Ortswechsel ist möglich. Dazu speichert die bisher zuständige Stelle die künftig zuständige Stelle in den Chip ein und gibt die Unterlagen dorthin ab. Damit hat jede neu zuständige Behörde alle erforderlichen Daten für sich verfügbar und kann neue Daten hinzuspeichern. Michel Oude Veldhuis vom holländischen Justizministerium: „Die Smartcard wird auch die Anzahl der Asylsuchenden senken. Außerdem stellen wir sofort fest, wer untergetaucht ist". Mit der Einführung der Karte erfolgte in Holland eine Gesetzesänderung, nach der die Überwachung und Registrierung bestimmter Gruppen von Asylsuchenden verschärft wurde.

Es gibt keine zentrale Datenbank, die über sämtliche auf den ausgegebenen Karten gespeicherten Daten verfügt. Damit, so die Protagonisten dieses Systems, sei die Gefahr des „gläsernen Ausländers" nicht vorhanden. Die in Holland verwendete Karte ist angeblich in hohem Maße fälschungssicher. Die Smartcard hat eine Speicherkapazität von 2 KB. Als Produktionskosten pro Dokument werden ca. 15 DM angeben. Das Resümee des deutschen BMI zum ASYL-CARD-Einsatz in den Niederlanden: „Offensichtlich erfolgreich". Die Asylsuchenden wären zunächst richtig scharf auf die Karten gewesen. Die Verlustquote sei äußerst gering. Dieser „Erfolg" hat einen guten Grund: „Die strengen Regeln des niederländischen Asylverfahrens, denen sich der Asylbewerber unterwerfen muß, werden mit der freien Willensentschließung des einzelnen begründet, in den Niederlanden um Asyl nachzusuchen. Folgerichtig muß ein Asylbewerber mit seiner Abschiebung rechnen, wenn er diese Regeln mißachtet".

Von Anfang an wurden in Holland Überlegungen angestellt, eine Smart-Card auch für alle anderen Ausländerinnen und Ausländer, die sich im Land aufhalten, und letztendlich für alle niederländischen Staatsangehörigen einzuführen. Die übrigen Nicht-Niederländer sind übrigens schon verpflichtet, den Vorläufer dieser Smart-Card - ohne Chip - zu besitzen. Die schöne neue zukunftsträchtige Welt beginnt also heute schon gleich hinter dem Deich.[3]

[1] ED = erkennungsdienstlich

[2] Presseerklärung des LfD Niedersachsen vom 3.1.1995; 17. TB LfD Bremen 1994, S. 60 f; 17. TB LfD Schleswig Holstein 1994/95, S. 37 f.

[3] Bundesmin. des Innern: Bericht über die Erfahrungen mit der Asyl-Card in der niederländ. Asylverwaltung, Stand 24.2.1995; zur ImigrantInnenerfassung in Holland: van der Schans, DANA 6-1994, 18 ff.; vgl. DANA 5-1994, 28.

3. Reaktionen

Da will Deutschland nicht hinter dem Mond bleiben. In Deutschland gibt es Vorläuferversuche mit Magnetstreifenkarten: Seit Ostern 1994 müssen in Baden-Württemberg Flüchtlinge eine Magnetkarte ständig mit sich führen, um in die zentrale Aufnahmestelle und die sechs Bezirksstellen hineinzukommen. Die Karte soll garantieren, daß Flüchtlinge nur das Heim betreten können, in dem sie registriert sind. Im zentralen Aufnahmelager in Eisenhüttenstadt/Brandenburg werden bereits seit 1990 auch die Essensausgabe und die Taschengeldberechtigung über die Magnetkarte kontrolliert. Die Erfahrungen mit der Magnetkarte seien bislang sehr positiv, so die Leiter der betreffenden Heime.

Die Veröffentlichung der Pläne des BMI hatte ein ungewohnt großes Echo: Dem Votum des LfD Niedersachsen schlossen sich viele Kollegen an. Der Bundesbeauftragte für den Datenschutz war über das Vorhaben nicht informiert und bezeichnete es als „unausgegorene Idee". In den Ministerien wurde zunächst abgewiegelt. Das Projekt sei noch nicht ausgereift. Das BMI verwies darauf, es handele sich um „Vorüberlegungen". Nach der heftigen Kritik an der Karte in der Öffentlichkeit meinte das BMI, es bestünde „vorerst keine Chance, die ASYL-CARD wie zunächst projektiert einzuführen". Der Sprecher des bayerischen Sozialministeriums, Anton Haußmann, hielt die ASYL-CARD für ein „durchaus ehrenwertes Vorhaben", mit dem das Asylverfahren vereinfacht und dem „Mißbrauch von Leistungen, wie z.B. wenn einer bei zwei Sozialämtern antanzt und Geld will", begegnet werden könne. Die Karte solle „nicht zum Mißbrauch verwendet werden, sondern ihn verhindern". Ebenso der damalige sächsische Innenminister Eggert: Mit der ASYL-CARD könne die mehrfache Inanspruchnahme von Sozialleistungen durch Asylbewerber verhindert werden. Die BILD-Zeitung assistierte: „Die Chipkarte gehört zum modernen Leben wie unser tägliches Brot. Wer hat sie nicht, die Scheckkarte, die Mitgliedskarte für den Automobilclub oder die Krankenversicherungskarte. Nun wird über die Einführung einer ASYL-CARD diskutiert. Warum eigentlich nicht, wenn Verwaltungsabläufe damit vereinfacht und Leistungsmißbrauch erschwert wird".

Die Innenministerien von Nordrhein-Westfalen, Niedersachsen, Schleswig-Holstein, Baden-Württemberg, Bremen, Rheinland-Pfalz und Brandenburg äußerten Zweifel an der Verfassungsmäßigkeit des Projektes. Der Sprecher des schleswig-holsteinischen Innenministeriums, Thomas Giebeler, meinte, die ASYL-CARD könne den Datenaustausch zwischen den beteiligten Behörden nicht ersetzen.[4] Letztendlich sprachen sich nur sieben Bundesländer für die Durchführung einer Machbarkeitsstudie zur ASYL-CARD aus. Dies hindert aber das BMI nicht, seine Pläne voranzutreiben. Im Rahmen der Machbarkeitstudie sollen nicht nur das BAFl, sondern insbesondere auch Landes- und Kommunaleinrichtungen wie Aufnahmeeinrichtungen, Ausländerämter und Sozialämter einbezogen werden. Einziges Problem scheint die noch ungeklärte Kostenfrage zu sein. Schon im Zwischenbericht der Bund-Länder-Arbeitsgruppe wurden Überlegungen angestellt, die einmal in Deutschland verwirklichte ASYL-CARD europaweit einzusetzen. Die Grundlage hierfür ist schon heute mit dem Dubliner Asylabkommen der EU-Staaten gelegt.

4. Praktische und rechtliche Bedenken

Die Argumente der ASYL-CARD-Befürworter bewegen sich auf einer Ebene, die mit den realen Verhältnissen des Asylverfahrens nichts zu tun hat. Seit der verfassungsrechtlich inakzeptablen ausnahmslosen ED-Behandlung aller Asylsuchenden sowie der Speicherung und dem Datenabgleich im Automatischen Fingerabdruckidentifikationssystem (AFIS) ist das Problem des „Asylmißbrauchs" durch doppelte Antragstellung unter verschiedenen Identitäten mit der informationstechnischen Holzhammermethode gelöst.[5] Das Hauptproblem der Verwaltung, die Feststellung der Identität bei teilweise exotischen Namen und Sprachproblemen ließe sich mit einem einfachen einheitlichen Ausweis lösen. Die vielbeschworene Fälschungssicherheit ist nicht sicherzustellen: Selbst gut gesichert erscheinende Chipkarten lassen sich manipulieren und verfälschen. Dies gilt in jedem Fall bei einem Massensystem, zu dem unterschiedlichste Stellen Zugang haben sollen. Und selbst der Fingerabdruck ist kopierbar. Automatische Lesegeräte können nicht verläßlich zwischen echter Haut und dem Abziehbild eines Gummihandschuhs unterscheiden.[6] Solange der Speicherchip nicht implantiert ist oder, wie bei der elektronischen Häftlingsüberwachung im Hausarrest, mit dem Menschen unlösbar verbunden wird, bleiben die ASYL-CARDs übertragbar.

Die Problemanalyse, die dem Zwischenbericht mit dem SmartCard-Vorschlag voranging, zeigte, daß sowohl bei den Bundesländern wie auch bei den beteiligten Stellen kein Bedürfnis für eine verbesserte Kommunikation über Asylsuchende besteht. Mit der ASYL-CARD wird offensichtlich ein anderes politisches Ziel verfolgt: Es geht um Kontrolle und Ausgrenzung. Außerdem geht es um das Austesten eines neuen technischen Überwachungsinstruments an einer Personengruppe, von der wenig Widerstand erwartet wird. Die für die ASYL-CARD vorgesehenen Funktionen sind für die praktische Durchführung des Asylverfahrens nicht nötig; sie sind bequem. Ob sie billig und wirksam sind, darf in Frage gestellt werden. Aus rechtlicher Sicht spricht alles gegen die ASYL-CARD: Das Grundrecht auf informationelle Selbstbestimmung gilt auch für ausländische Flüchtlinge. Eingriffe in das Grundrecht sind nur im überwiegenden Allgemeininteresse zulässig.[7] Derartige überwiegende Gemeinwohlbelange sind nicht erkennbar. Der Umstand, daß die Meldungen an das Ausländerzentralregister (AZR) durch die Ausländerbehörden unbefriedigend und daher der dortige Datenbestand oft inaktuell ist, kann ein Grund sein, die AZR-Konzeption zu überdenken, kann aber nicht die Einführung neuer Überwachungsmechanismen rechtfertigen. In der Wertordnung des Grundgesetzes (GG) gilt die Menschenwürde als oberster Wert, der es verbietet, den Menschen zum bloßen Objekt zu machen. Mit dem GG nicht zu vereinbaren ist es, wenn der Staat für sich das Recht in Anspruch nehmen würde, Menschen zwangsweise in ihrer ganzen Persönlich-

[4] Junge Welt, 5.1. 1995 S. 1; Göttinger Tageblatt 5.1.1995; Bild 5.1.1995; FAZ 7.1.1995, S. 4; Focus 2/1995, 15.

[5] DSB-Konferenz, abgedruckt in: XI. TB LfD Niedersachsen, Anlage 7; DANA 5-1994, 9; entsprechendes ist für Bürgerkriegsflüchtlinge geplant, vgl. XII. TB LfD Niedersachsen S. 110 f.

[6] Dazu DANA 6-1994, 29.

[7] Volkszählungsurteil: BVerfG, NJW 1984, 419 ff.

keit zu registrieren und zu katalogisieren.[8] Diesen verfassungsrechtlichen Vorgaben widerspricht die geplante ASYL-CARD: Auf ihr sollen nicht nur Identifizierungsdaten, sondern Angaben aus allen Lebensbereichen gespeichert werden, insbesondere auch aus den Bereichen der Fürsorge (Leistungen) und der Repression (ausländerrechtliche Verfahrensdaten). Damit besteht die Tendenz, auf der ASYL-CARD Daten in einem Umfang zu speichern, der die Erstellung unzulässiger Persönlichkeitsprofile ermöglicht. Es werden dabei unterschiedliche Zwecke verfolgt, die tendenziell nicht miteinander vereinbar sind. Auch dies hat das Bundesverfassungsgericht als Verstoß gegen das informationelle Selbstbestimmungsrecht erkannt.[9] Außerdem würde die ASYL-CARD die Gefahr der sozialen Abstempelung hervorrufen. Derartig massive Eingriffe sind weder erforderlich noch angemessen.

Um zu vermeiden, daß bei Verlust der ASYL-CARD die darauf gespeicherten Daten verloren gehen, ist nach den deutschen Plänen - anders als in Holland - als Back-Up eine Sicherungsdatei vorgesehen, in der die relevanten Daten hinterlegt sind. Ein derartiges zentrales oder zentralisiertes System mit Verfahrens- und Leistungsdaten würde trotz ASYLON, AFIS und AZR eine neue Dimension bei der Erfassung zur Folge haben, da bei den bisherigen Systemen Sozialdaten regelmäßig keine Rolle spielten.[10]

Mit der Einführung einer umfassenden Smart-Card für Flüchtlinge würde ein wesentlicher Grundrechtseingriff erfolgen, der, wenn überhaupt, nur per Gesetz möglich wäre. Da mit der ASYL-CARD das Verwaltungsverfahren, für das die Länder zuständig sind, tangiert werden würde, bedürfte es bei einer bundesweiten Einführung der derzeit projektierten Karte zudem einer gesetzlichen Regelung, die der Zustimmung der Bundesrates bedürfte. Die aktuellen Äußerungen einiger SPD-regierter Länder zeigten, daß für die ASYL-CARD im Bundesrat derzeit keine Mehrheit zu erreichen wäre. Das BMI versucht zu verhindern, daß das Asylverfahrensgesetz aufgeschnürt wird, weil damit SPD, Grüne und FDP eine Gelegenheit hätten, Lokkerungen des Asylrechts durchzudrücken. Die Durchführung einer Machbarkeitsstudie auch ohne gesetzliche Grundlage ist aber allemal nicht verboten. So sollen darüber Fakten geschaffen werden, mit denen den Flüchtlingen ihre Würde und ihre Persönlichkeit genommen wird, während die guten Deutschen wieder einmal die trügerische Hoffnung haben können, mit ihrem Überwachungswesen alles in den Griff zu bekommen. ■

[8] BVerfG, NJW 1969, 1707.

[9] BVerfG, NJW 1984, 422, 426 f.

[10] Vgl. dazu DANA 5-1994, 8 ff.

Rainer W. Gerling

Internet: juristische Probleme und kein Ende?

Wer heute ein Rechenzentrum (dabei ist es egal, ob es sich um ein Hochschulrechenzentrum oder um ein Minirechenzentrum eines Lehrstuhles handelt) betreibt, sieht sich unverhofft einer Vielzahl von rechtlichen Problemen aus nahezu allen Rechtsbereichen gegenüber. Dazu kommt als besondere juristische Delikatesse die Problematik des Internets, das sich aufgrund seiner teilweise nahezu chaotischen internationalen Strukturen einer Beurteilung nach nationalem Recht fast schon entzieht. Wenn der Staatsanwalt an der Tür steht oder die Abmahnung ins Haus flattert, dann ist es meistens schon zu spät.

Im folgenden soll nicht das Internet verteufelt werden, sondern der Verantwortliche soll auf potentielle Probleme hingewiesen werden. Der vorliegende Beitrag soll deshalb exemplarisch einige Rechtsfragen beim Betrieb von Rechenzentren mit Zugang zu öffentlichen Datennetzen behandeln. Die Auswahl der Themen orientiert sich dabei an einem typischen Hochschulrechenzentrum. Es geht hier mehr um das Bewußtmachen möglicher Problemfelder, als um die umfassende Darstellung rechtlicher Lösungen. Wir befinden uns erst in der Anfangsphase der einschlägigen Rechtsprechung. Bis zur endgültigen Klärung der Rechtsfragen wird es noch etlicher Gerichtsentscheidungen bedürfen. Trotzdem muß man die Fragen aufwerfen und diskutieren. Es darf nicht dazu kommen, daß die internationalen Kommunikationsmöglichkeiten, die gerade aus der Wissenschaft nicht mehr wegzudenken sind, durch Rechtsmißbrauch einzelner eingeschränkt werden.

Lizenzrecht

Am 24.6.1993 ist das zweite Gesetz zur Änderung des Urheberrechtsgesetzes (UrhG) vom 9.6.1993 in Kraft getreten. Das Gesetz dient der Umsetzung der Richtlinie 91/250/EWG des Rats der Europäischen Gemeinschaft vom 14.5.1991 über den Rechtsschutz von Computerprogrammen (Abl. EG Nr. L 122 S. 42). Diese Gesetzesänderung hat weitreichende Konsequenzen für jemanden, der nicht lizensierte Software (Raubkopien) wissentlich oder unwissentlich einsetzt.

Nach der neuen Rechtslage genießt Software auch dann schon urheberrechtlichen Schutz, wenn sie nur einen geringen Grad an Originalität (sog. „Kleine Münze") aufweist. Das war bisher nicht der Fall. Deshalb standen aufgrund der alten Rechtslage der Softwareindustrie nur sehr geringe Möglichkeiten zur Verfügung, um sich effektiv gegenüber Raubkopierern zur Wehr zu setzen.

Das neue Gesetz erlaubt es jetzt, ohne langwierige Prozesse Unterlassungsverfügungen, Schadensersatzforderungen und Strafanträge durchzusetzen. Der Verband der deutschen Softwareindustrie droht aufgrund der neuen Rechtslage mit Aktionen gegen Firmen und Organisationen, die weiterhin Raubkopien einsetzen. Das neue Gesetz gilt nicht nur für Software, die ab dem 24.06.1993 verkauft wurde, sondern rückwirkend für alle Software, die zur Zeit genutzt wird. Es gibt auch keine Übergangsregelungen.

Es ist deswegen unbedingt erforderlich, den Umfang bestehender Softwarenutzung und deren Rechtmäßigkeit zu überprüfen. Nicht lizensierte Software ist entweder zu löschen oder durch Nachkauf der Lizenz zu legalisieren. Wer eine großen Zahl PCs einsetzt, muß dabei unter Umständen erhebliche finanzielle Mittel einsetzen.

Es wird empfohlen, eine Liste aller installierten Software zu erstellen. Dieses Softwareregister ist dann mit der Liste der tatsächlich lizensierten Software zu vergleichen. Um den ordnungsgemäßen Softwareeinsatz jederzeit demonstrieren zu können, ist es auf Dauer erforderlich, ein solches Softwareregister ständig fortzuschreiben. Die Mitarbeiter sind darauf hinzuweisen, daß die Installation von Software auf Rechnern der Einrichtung nur durch dafür speziell autorisierte Mitarbeiter erfolgt, die dann auch das Softwareregister fortschreiben.

Alle Nutzer müssen vertraglich verpflichtet werden, keine Software auf Rechnern der Einrichtung zu installieren. Die Einhaltung dieser Regelung ist stichprobenartig zu überprüfen. Wenn es technisch und organisatorisch möglich ist, das Einspielen von Software zu verhindern (z.B.: Ausbau oder Sperrung von Disketten-Laufwerken), sollte das gemacht werden.

Die beste Lösung sind aber Campus-Lizenzverträge, die eine unbegrenzte Anzahl von Kopien einer Software auf Rechnern der Einrichtung erlauben. Hier müssen gerade auch Hochschulrechenzentren gemeinsam aktiv werden und Druck auf Software-Firmen ausüben.

Eine Überprüfung aller Softwareverträge ist zweckmäßig. Insbesondere Software, die speziell für eine Einrichtung als Auftragsarbeit (Arbeits-, Dienst- oder Werkvertrag) erstellt wurde, sollte auf vorhandenes Nutzungsrecht überprüft werden. Es kann davon ausgegangen werden, daß in der Vergangenheit diese Fragen nicht immer eindeutig geregelt worden sind.

Was ein Arbeitgeber von festangestellten oder freien Mitarbeitern an Software schreiben läßt, unterliegt seiner ausschließlichen Nutzung (§ 69b UrhG), sofern nichts anderes vereinbart ist. Auch wenn sich der Autor von Software als ausschließlicher Copyright-Inhaber sieht, so ist die neue Rechtslage eindeutig anders. Wer als Arbeitgeber Software im Auftrag von seinen Mitarbeitern schreiben läßt, hat alle Nutzungsrechte an dieser Software.

Datenschutzgesetze

Es steht außer Frage, daß bei Informationsangeboten eines Rechenzentrums (z.B. WWW-Seiten), die personenbezogene Daten enthalten, das Bundesdatenschutzgesetz (BDSG; Bundesdatenschutzgesetz vom 20.12.1990, Bundesgesetzblatt, Jahrgang 1990, I, Seite 2954) bzw. das entsprechende Landesdatenschutzgesetz anzuwenden ist. Sobald auf diese Daten auch außerhalb der Einrichtung zugegriffen werden kann, ist der Tatbestand einer Übermittlung an Dritte erfüllt. Da es sich hier nicht um die gezielte Weitergabe an einen genau bezeichneten Dritten handelt, sondern die Daten jedem zugänglich gemacht werden, sind besonders strenge Maßstäbe anzulegen. Zur Zeit kann davon ausgegangen werden, daß die schriftliche Einwilligung der Betroffenen erforderlich ist.

Der Gesetzgeber hat im BDSG geregelt, daß die Übermittlung und Verarbeitung personenbezogener Daten erlaubt ist, wenn sie „aus allgemein zugänglichen Quellen entnommen werden können". Ein WWW-Server stellt definitiv eine „allgemein zugängliche Quelle" dar, und schafft damit den Erlaubnistatbestand für eine freie Nutzung der Daten. Deshalb muß hier besonders sorgfältig überlegt werden, welche Daten wie angeboten werden. Gerade auch vor dem Hintergrund einer Kommerzialisierung des Internets ist momentan nicht zu übersehen, wozu die personenbezogenen Daten aus solchen WWW-Servern in Zukunft benutzt werden. Eines Tages werden sich auch Adreßhändler im Internet „bedienen".

Auf Grund des weltweit (!) freien Zugriffs ist auch bei auf den ersten Blick relativ „harmlosen" Daten eine Einwilligung des Betroffenen erforderlich.

Bei Dateien mit personenbezogenen oder beziehbaren Angaben Dritter ist nach den Datenschutzgesetzen eine schriftliche Einwilligung der Betroffen (§ 4 Abs. 2 BDSG) einzuholen. Bei minder sensiblen Daten (z.B. Name, Vorname, Dienstanschrift, E-Mail-Adresse) kann eventuell auch eine Einwilligung per E-Mail eingeholt werden. Keinesfalls ist eine Widerspruchsregelung ausreichend. Bei extensiven Daten (Bild, beruflicher Werdegang, Ausbildung etc.) ist eine schriftliche Einwilligung auf jeden Fall erforderlich. Wenn die Zuordnung der Person zu der Einrichtung kritisch ist (z.B. weil die Einrichtung Tierversuche oder gentechnische Versuche macht), dann ist eine besonders sorgfältige Abwägung zu machen. Hier ist unter Umständen schon die Aufnahme in ein X.500 Verzeichnis kritisch.

Auf keinen Fall ist es zulässig, daß personenbezogene oder beziehbare Daten ohne Wissen der Betroffenen in irgendeiner Weise irgendwo uneingeschränkt „angeboten" werden

Das Einholen der erforderlichen Einwilligungen ist aufwendig. Es bietet sich deshalb an, die Einwilligung in das Formular für die Beantragung einer Benutzerkennung aufzunehmen. Damit entsteht jetzt nur der Aufwand für das Einholen der Einwilligung der bereits vorhandenen Benutzer.

Die Informationen eines Bibliothekskatalogs (Daten über Bücher wie Autor, Titel, Verlag etc. aber nicht Ausleiher oder Beschaffer) können allgemein zugänglich gemacht werden, da sie aus allgemein zugänglichen Quellen (Verlagskataloge etc.) stammen.

Bei der Beurteilung der Frage ob eine Einrichtung einen Datenschutzbeauftragten benötigt, sind bei der Bestimmung der Anzahl der Personen, die „personenbezogene Daten automatisiert verarbeiten" (§ 36 Abs. 1 BDSG), die Personen, die einen WWW-Server oder ähnliche Server mit personenbezogenen Angaben betreuen, mitzuzählen.

Eine weitere umstrittene Frage ist, inwieweit man die Namen und dienstlichen Anschriften von Mitarbeitern, die aufgrund ihrer Tätigkeit eine Außenwirkung haben, auch gegen ihren Willen im Netz auf WWW-Seiten angeben kann. Dies betrifft z.B. Außendienstmitarbeiter, Kundendienstmitarbeiter aber auch Mitarbeiter in Technologietransferzentren, Pressestellen und ähnlichem. Insbesondere wenn die Mitarbeiter dieser Art von Datenweitergabe explizit widersprechen, gibt es ein Problem. Hier kann man dann nur auf eine Funktionsbeschreibung ausweichen. So ist es z.B. möglich, in einem Technologietransferzentrum nur die Sachgebiete und Zuständigkeiten mit der Telefonnummer anzugeben und auf Namen zu verzichten. Dies hätte auch den Vorteil, daß im Falle eines Personalwechsels keine Änderungen nötig sind. Es ist auch denkbar, die Einwilligung des Mitarbeiters bereits im Arbeitsvertrag einzuholen.

Daten in Computernetzen

Die Datendienste eines Rechenzentrums können im wesentlichen in drei klassische Bereiche eingeteilt werden:

1. **Individualkommunikation**

   Hierunter versteht man die Versendung von Einzelmitteilungen, z.B. E-Mail, an einzelne oder mehrere vom Absender festgelegte Empfänger.

2. **Öffentliche Kommunikation**

   Hierunter versteht man die Versendung von öffentlichen Mitteilungen. Der Absender legt nicht fest, wer die Mitteilung lesen darf. Hierunter fallen vor allem auch die Usenet News oder schwarze Bretter.

3. **Dateidienste**

   Hierunter versteht man das Anbieten von Public-Domain- oder Shareware-Programmen sowie von Daten (z.B. Text, Grafik oder Sound Dateien). Anonymous-ftp-Server sind ein typischer Vertreter dieser Gruppe.

E-Mail

Artikel 10 des Grundgesetzes schützt neben dem Briefgeheimnis auch das Post- und Fernmeldegeheimnis. Details dazu sind im Fernmeldeanlagengesetz (FAG) geregelt. Ein E-Mail-System eines Rechenzentrums gilt als Fernmeldeanlage im Sinne des § 354 Abs. 3 Strafgesetzbuch (StGB), wenn es an ein öffentliches Netz angeschlossen ist. Nahezu alle Rechenzentren sind über Telefonleitungen, Datex-P- oder WIN-Anschlüsse an öffentliche Netze angeschlossen. Damit greift der Schutz des FAG und der Teledienstunternehmen-Datenschutzverordnung (UDSV; Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen, vom 18.12.1991, Bundesgesetzblatt, Jahrgang 1991, Teil 1, Seite 2337). Die UDSV regelt im wesentlichen die Verarbeitung der bei der Kommunikation anfallenden Verbindungsdaten. Alle Verbindungsdaten, die Aufschlüsse über das Kommunikationsverhalten der Teilneh-

mer zu lassen, unterliegen der Geheimhaltung und einer strikten Zweckbindung.

§ 14a FAG und § 354 StGB regeln die Vertraulichkeit der Kommunikationsinhalte. Danach ist es nicht erlaubt, daß der Betreiber des E-Mail-Systems die Inhalte der E-Mails kontrolliert. Eine entsprechende Regelung in einer Benutzungsordnung oder Betriebsvereinbarung wäre rechtlich nicht wirksam, da sie gegen geltendes Recht verstößt. In die E-Mail eines Benutzers darf nur mit Zustimmung des Benutzers Einsicht genommen werden.

Usenet News

Ein besonderes Problem, das auch durch die Medien hochgespielt wird, stellen die Usenet News dar. So ist es in der Vergangenheit vorgekommen, daß hier Hehlerwaren angeboten, rassistisches Gedankengut verbreitet, pornographische Bilder angeboten oder sogar öffentlich zu Straftaten aufgefordert wurde (F. W. Hülsmann, DuD 18, 11/1994, Seite 621). Es ist unmöglich, bei dem gewaltigen Datenaufkommen der Usenet News (es gibt derzeit etwa 12 000 verschiedene Diskussionsgruppen mit einem täglichen Datenaufkommen von ca. 260 Megabyte) die Inhalte zu kontrollieren (H. Hassemüller und B. Reder, Gateway - Zeitschrift für Daten- und Telekommunikation, 6/1995, Seite 100). Es kann also passieren, daß strafrechtlich relevante öffentliche E-Mail ohne Wissen der Systembetreuung in die öffentlichen Angebote eines Rechenzentrums gelangt. Die Justizpressestelle des Oberlandesgerichts Nürnberg (Gz.1270-49/93-5. Januar 1994) hat im Zusammenhang mit einem konkreten Verfahren dazu erklärt:

„Konkrete Anhaltspunkte dafür, daß der Betreiber der ... Mailbox von der Zuspielung wußte und die Datei wissentlich auf seiner Mailbox duldete, hat die Staatsanwaltschaft nicht, infolgedessen kann ihm auch kein Vorsatz nachgewiesen werden. Das aber wäre Voraussetzung für eine Straftat gemäß § 130a Strafgesetzbuch".

Man kann den Betreiber nur dann zur Verantwortung ziehen, wenn wissentlich Dateien mit strafrechtlich relevantem Inhalt verbreitet werden. Diese Rechtsauffassung hat sich allerdings noch nicht allgemein durchgesetzt.

Bei Newsgruppen, wo der Inhalt von vorne herein bekannt ist, ist die Situation anders. Wenn z.B. in den Newsgruppen des alt.sex Baumes Dateien mit pornographischem Inhalt verbreitet werden, so ist das vorhersehbar. Hier bleibt bei einer stringenten Auslegung wohl nur das Abschalten der entsprechenden Newsgruppen. Da nur in den wenigsten Rechenzentren alle Newsgruppen angeboten werden, ist dies vertretbar. Bei einer großen Zahl von Newsgruppen gibt es sicherlich eine Diskussion, ob sie angeboten werden sollen oder nicht. Der objektive Maßstab kann hier nur das Strafgesetz sein. Der Vorwurf der Zensur ist in einem solchen Fall nicht gerechtfertigt, da nicht willkürlich unerwünschte Information unterdrückt wird, sondern dem deutschen Strafrecht Rechnung getragen wird.

Nicht gerechtfertigt ist es jedoch, den Zugriff auf Usenet News komplett zu unterbinden. Kritisch ist es jedoch, den eigenen Mitarbeitern (oder z.B. in einer Universität den Studenten) zu untersagen, auf externe News-Server zuzugreifen. Dies wäre ein Eingriff in die Informationsfreiheit. Die Daten, die sich ein Benutzer selber von einem externen Server holt, unterliegen auch voll der Verantwortung des Benutzers. Den Zugriff auf den eigenen News Server kann man für Externe ganz oder teilweise sperren.

Anonymous-ftp-Server

Beim Anbieten von Daten (Anonymous-ftp-Server) muß man die angebotenen Dateien einzeln kontrollieren. Es ist nicht möglich, einen Dateibereich einzurichten, in den Dritte Dateien einstellen (upload) können, und der von allen gelesen (download) werden kann.

Als ein praktikables Verfahren gilt das folgende: Es gibt einen Upload-Bereich, in den nur geschrieben werden kann. Hier kann jeder Dateien ablegen, aber nur autorisierte Mitarbeiter des Rechenzentrums können den Bereich auch lesen. Diese Mitarbeiter prüfen die Dateien und kopieren sie anschließend in den allgemein zugänglichen Bereich. Alle Dateien, deren Inhalt zu beanstanden ist, werden bei diesem Verfahren ausgesondert. Sicherlich verlangt dieses Verfahren einiges an personellen Ressourcen, aber es stellt auch sicher, daß das Rechenzentrum seiner rechtlichen Verantwortung gerecht wird. Bei diesem Verfahren ist folgendes zu prüfen:

- Das Programm/der Inhalt der Dateien ist nur im Ausland Freeware, Shareware oder Public Domain, aber in der BRD kommerziell. Oder das Programm ist kommerziell oder kommerziell geworden. Stellt ein Software-Autor sein Programmpaket als Freeware, Shareware oder Public Domain zur Verfügung, so gibt es in der Dokumentation meistens Angaben des Autors zur Verbreitung des Programms, die im allgemeinen die erforderliche Erlaubnis beinhalten. Der entsprechende Text ist genau zu lesen und zu beachten. In allen Zweifelsfällen muß der Autor kontaktiert werden.
- Aufgrund der lizenzrechtlichen oder patentrechtlichen Lage ist das Programm oder die Datei nirgendwo oder nur außerhalb der BRD frei von Rechten Dritter.
- Das Programm oder die Datei hat einen Inhalt (z.B. Pornographie, Gewaltverherrlichung), der in der BRD strafrechtlich relevant ist.
- Das Programm fällt unter Exportbeschränkungen der BRD und kann deshalb von der BRD aus nicht weltweit angeboten werden. In diesem Fall müssen Vorkehrungen getroffen werden, die einem Benutzer außerhalb der BRD den Zugriff unmöglich machen. •Das Programm hätte nach den Exportvorschriften des Landes, in dem es entstanden ist, nicht exportiert werden dürfen. Nach der derzeitigen Rechtslage macht sich nur der strafbar (und zwar in dem Drittland), der die Exportvorschriften des Drittlandes nicht beachtet. Dieser Punkt betrifft vor allem Crypto-Software aus den USA.

Spiegelt ein Rechenzentrum einen oder mehrere andere Server, so halte ich es für erforderlich, daß man mit dem Betreiber des Ursprung-Servers einen Vertrag über dieses Spiegeln schließt. Einerseits ist es wegen des Copyrights der Zusammenstellung der Dateien (Compilation Copyright) sowieso unerläßlich, sich die Erlaubnis zum Spiegeln zu holen, andererseits kann man sich hierdurch rechtlich absichern, daß von diesem Server nur „saubere" Software kommt. Dessen ungeachtet ist es natürlich erforderlich, daß der Betreiber des deutschen Rechenzentrums stichprobenartig den Inhalt seines Anonymous-ftp-Servers überprüft.

Anwendung des Presserechts

In allen Landespressegesetzen (LPG) gibt es das Konzept des verantwortlichen Redakteurs. So regelt § 5 Abs. 1 des Bayerischen LPG: „Bei jeder Zeitung muß mindestens ein verantwortlicher Redakteure bestellt werden." Der § 11 Abs. 2 des Bayerischen LPG regelt dann weiter: „Zu Lasten des verantwortlichen Redakteurs eines periodischen Druckwerkes wird vermutet, daß er den Inhalt eines unter seiner Verantwortung erschienen Textes gekannt und den Abdruck gebilligt hat." Aufgrund dieser Regelung ist klar, daß die Landespressegesetze klare Verantwortungsregeln kennen. Gibt es keinen verantwortlichen Redakteur ist der Verleger, Drucker oder Verbreiter verantwortlich, wenn er nicht entsprechende Sorgfalt nachweist. Die Sorgfalt kann nachgewiesen werden, in dem einerseits klare Vereinbarungen, die regeln, was erlaubt ist, vorliegen und andererseits die Einhaltung dieser Vereinbarungen angemessen überprüft wird.

Bleibt die Frage, inwieweit das Presserecht anzuwenden ist. Die LPGs gelten für Druckwerke, Zeitungen und Zeitschriften. Im Bayerischen LPG werden Druckwerke in § 6 definiert. Es stellt sich die Frage ob z.B. eine WWW-Seite die Voraussetzungen für die Anwendung des Presserechts erfüllt. Sie ist sicherlich „zur Verbreitung in der Öffentlichkeit bestimmt". Auch erfüllt sie das Kriterium „Schrift, bildliche Darstellung mit und ohne Schrift". Alle Daten in einer EDV Anlage sind aber nicht „mittels der Buchdruckerpresse" erstellt. Man kann die elektronische Verteilung aber sicherlich als ein „sonstiges Vervielfältigungsverfahren" ansehen. Hinzu kommt, daß einige LPGs zumindest bei „presseredaktionellen Hilfsunternehmen" ein Druckwerk „ohne Rücksicht auf die technische Form" der Zulieferung definieren.

Die Beurteilung, insbesondere von WWW-Servern, nach dem Presserecht ist wegen der Analogie zu einer Zeitung oder Zeitschrift vertretbar. Damit ist die strafrechtliche Verantwortung des Betreibers (Leiter des Rechenzentrums) zu vermuten. Dies macht detaillierte interne Vorschriften über den zulässigen Inhalt der WWW-Seiten erforderlich. Im Sinne von Corporate Identity und der Selbstdarstellung der betreffenden Einrichtung ist auch die äußere Gestaltung sehr wichtig. Die Tatsache, daß insbesondere in Hochschulen jeder Betreuer einer UNIX-Workstation in eigener Regie unkoordiniert WWW-Seiten anbietet, ist sorgfältig zu überdenken. Ein klares Konzept ist für eine Einrichtung wichtig. Gerade bei der zunehmenden Verbreitung von WWW wird dieses Medium auf Dauer wichtiger als die mit viel Aufwand produzierte Hauszeitschrift.

Vorsicht ist auch bei Äußerungen in internen oder öffentlichen schwarzen Brettern über Firmen oder dgl. geboten. So können z.B. negative Aussagen über eine Firma (schlechter Support, fehlende Kulanz) zivilrechtliche Forderungen nach sich ziehen.

Manche Einrichtungen gehen dazu über, ihren Mitarbeitern private WWW-Seiten einzuräumen. Auf dieser privaten Seite können Mitarbeiter sich privat mit Hobbys, Interessen und dgl. vorstellen. Dieses Vorgehen schafft eine Menge rechtlicher Probleme. Es ist sicherlich nicht wünschenswert, daß Mitarbeiter ihre privaten Interessen völlig ohne Kontrolle des Arbeitgebers hier darstellen können. Wenn es aber Kontrolle gibt, muß es genaue Richtlinien geben, was erlaubt ist und was nicht. Das Aufstellen dieser Richtlinien ist sehr kompliziert, da hier viele Aspekte einfließen, die sich einer objektiven Beurteilung entziehen. Es ist einfacher, dieses Angebot an die Mitarbeiter gar nicht erst zu machen.

Urheberrechtliche Fragen

Wer auf einem Server Dateien anbietet, an denen er nicht das Urheberrecht hat, bzw. für die er nicht die Erlaubnis des Urhebers für das Anbieten hat, läuft in rechtliche Probleme. Die urheberrechtlichen Verwertungs- und Verbreitungsrechte von Bildern, Musikstücken, Videos, Texten usw. müssen geprüft werden und eine Verbreitung wie im WWW mit einem kaum einsschätzbaren Teilnehmerkreis bedarf auf jeden Fall der Zustimmung des Inhabers der Rechte. Die Tatsache, daß die Angebote im WWW kostenlos sind, ist unerheblich.

In Deutschland sind alle Werke bis 70 Jahre nach dem Tod des Urhebers geschützt. Danach können die Werke frei verwendet werden. Es ist aber trotzdem Vorsicht geboten. Bei Texten, Musikstücken usw. kann der Schutz durch Bearbeiten neu entstehen. So sind z.B. die Originaltexte längst verstorbener Dichter frei, Bearbeitungen in neuen Ausgaben aber nicht, auch wenn sich die beiden Versionen auf den ersten Blick nur wenig unterscheiden.

Es kann nicht davon ausgegangen werden, daß der Inhalt von Tageszeitungen, Zeitschriften, Büchern usw. frei von solchen Verwertungsrechten ist. Häufig ist sogar das Speichern in EDV-Anlagen (hierunter fällt auch das Einscannen von Comics, Karrikaturen, Texten und ähnlichem aus allgemein zugänglichen Medien) im Impressum untersagt. Vor diesem Hintergrund sind auch Aktivitäten wie das Web-Museum zu sehen. Die bildliche Darstellung der Kunstwerke ist bei modernen Malern nur mit Zustimmung der jeweiligen Rechteinhaber möglich. Da es hier im allgemeinen um eine Kollision des Anbieters im WWW mit den kommerziellen Interessen des Rechteinhabers geht, muß hier mit entsprechenden rechtlichen Schritten gerechnet werden.

So ist es schon vorgekommen, daß der Inhaber der Verwertungsrechte dem WWW-Anbieter eine Unterlassungsverpflichtung abverlangt hat. Der Inhalt dieser Verpflichtung ist üblicherweise die, daß man die Verbreitungen in Zukunft bei Androhung einer Vertragsstrafe von etlichen 10 TDM für jeden Verstoß unterläßt. Die anwaltlichen Gebühren für dieses Verfahren werden von dem Anbieter im WWW entrichtet. Dies könne leicht über 1000 DM sein.

Zugriff auf Dateien

Ein Benutzer darf seine Dateien oder Teile davon weltweit zugänglich machen (z.B. unter UNIX-Leserechte für alle), wenn er alle Rechte an dem Inhalt der Dateien hat und diese Dateien keine personenbezogenen oder beziehbare Angaben Dritter enthalten. Außerdem muß der Benutzer natürlich die Vorschriften über den Umgang mit vertraulichen Daten seiner Einrichtung befolgen.

Bei nicht selbsterstellten Programmen oder Daten kann im allgemeinen nicht davon ausgegangen werden, daß der Benutzer die Rechte daran hat. Er muß deshalb die Erlaubnis der Rechteinhaber für die Verbreitung einholen. Auch die Regelungen des Urheberrechts (Lizenzrecht) sind einzuhalten. Gerade auch bei Daten, die aus Druckwerken abgetippt oder eingescannt werden (Listings oder Bilder aus Zeitschriften und Büchern), liegen die Rechte an den Daten fast im-

mer bei anderen. Entsprechende Hinweise im Impressum sind zu beachten.

Der Betreiber des Rechenzentrums muß die Zugriffsrechte so einstellen, daß der freie Zugriff auf die Dateien eines Benutzers nicht die Voreinstellung ist. Die Dateien dürfen nicht auf Grund der Voreinstellungen ohne zutun des Benutzers frei zugreifbar sein. So sollten zum Beispiel in einem UNIX System die Dateiattribute auf (rw- — —) voreingestellt sein, damit nur der Benutzer selber auf die Dateien zugreifen kann. Jeder Benutzer kann dann im eigenen Ermessen und in eigener Verantwortung diese Attribute ändern.

Der § 202a des StGB regelt den Tatbestand des „Ausspähens von Computer Daten". Danach wird bestraft, wer sich Daten unbefugt verschafft, „die nicht für ihn bestimmt und die gegen unberechtigten Zugriff besonders gesichert sind". Daten, auf die man nur nach Eingabe einer Benutzerkennung und eines Paßwortes zugreifen kann, gelten als besonders gesichert. Für den besonderen Schutz ist es nicht erforderlich, die Daten zu verschlüsseln. Daten, die sich dagegen auf allgemein ohne Paßwort zugänglichen Rechnern befinden, gelten nicht als besonders geschützt. Enthalten die Dateien personenbezogene Daten, so wird der unbefugte Zugriff auch durch § 43 Abs. 1 Nr. 3 BDSG unter Strafe gestellt.

Die Daten, die ein Benutzer auf einem Rechner des Rechenzentrums in seinem Dateibereich hält, sind im allgemeinen nicht für den Betreiber des Rechenzentrums bestimmt. Die Leitung eines Rechenzentrums darf also nicht anordnen, daß alle Benutzer-Dateien überprüft werden, ob der Inhalt strafrechtlich relevant ist. Hat man den begründeten Verdacht, daß ein Benutzer die Infrastruktur des Rechenzentrum für Straftaten benutzt, so sind die Strafverfolgungsbehörden einzuschalten. Auf keinen Fall darf man versuchen, durch Einsichtnahme in die Dateien des Benutzers den Verdacht zu erhärten.

Patentrecht

Eine besondere rechtliche Situation wird durch das Patentrecht geschaffen. Die Situation sei beispielhaft für den IDEA Algorithmus beschrieben. Es gibt viele gute Programme (Shareware, Freeware usw.), die den Verschlüsselungsalgorithmus IDEA verwenden. Eines der bekanntesten Programme ist sicherlich Pretty Good Privacy (P. Zimmermann, Pretty Good Privacy, verfügbar über anonymous ftp für DOS, UNIX und Macintosh Rechner). Aber der IDEA-Algorithmus ist in der EU patentiert (Patent Nr. EP 0 482 154 B1, erteilt am 30 Juni 1993). Die Schweizer Firma Ascom-Sysec AG vertritt die Rechte (Ascom Systec AG, Gewerbepark, CH - 5506 Mägenwil, Schweiz; E-Mail: IDEA@ascom.ch). Für private Anwendungen kann der IDEA-Algorithmus kostenlos verwendet werden. Für die Verwendung in einer Universität, Behörde oder Firma sind jedoch Lizenzgebühren fällig. Die Lizensierung des Algorithmus hat dabei nichts mit dem Status des Anwendungsprogramms zu tun. Auch wenn der Autor des Anwendungsprogrammes erklärt, daß sein Programm für beliebige Anwendungen kostenlos benutzt werden kann, entbindet dieses den kommerziellen Anwender nicht von der Zahlung der Lizenzgebühr an Ascom-Tech. Dieses schafft Probleme, wenn ein Mitarbeiter eines Rechenzentrums in Eigeninitiative ein Freeware Programm mit diesem Algorithmus einsetzt. Die Grenzen zwischen privater und nicht-privater Nutzung sind hier nur schwer zu ziehen.

Es wird häufig argumentiert, daß nach deutschem Recht Algorithmen nicht patentierbar sind und das IDEA-Patent deshalb ungültig sei. Das EU-Patent ist erteilt und damit auch in Deutschland gültig. Solange niemand dieses Patent anficht und ein Gericht es für ungültig erklärt, ist es gültig. Da EU-Recht deutsches Recht bricht, ist der Ausgang einer Anfechtung offen.

Ein anderes prominentes Beispiel sind Programme, die Grafikdateien im GIF-Format handhaben. Der verwendete Komprimierungsalgorithmus (Lemple-Zev-Welch) ist von Unisys patentiert (US-Patent 4 558 302) (c't, 3/1995, Seite 29) und Compuserve/Unisys verlangen Lizenzgebühren von allen Autoren solcher Programme.

Zusammenfassung

- Das Software-Copyright-Problem ist insbesondere in Universitäten und Forschungseinrichtungen letztendlich nur durch Campus-Lizenzen lösbar. Solange installierte Softwarepakete gezählt werden müssen, gibt es unvermeidlich im akademischen Bereich Raubkopien.
- Die Regelungen des BDSG müssen beachtet werden. Eine effiziente Handhabung auf Dauer ist nur möglich, wenn die erforderlichen Einwilligungen bereits auf dem Benutzerantrag eingeholt werden.
- Usenet News stellen ein rechtlich kompliziertes Medium dar. Strafrechtliche Vorschriften müssen beachtet werden. Die einzige Möglichkeit stellt die Zensur dar, indem einzelne Newsgruppen abgeschaltet werden. Dies ist sicherlich keine schöne Lösung, zumal die Meinungen, was abgeschaltet werden muß und was nicht, auseinander gehen. Hier fehlen eindeutige und handhabbare rechtliche Regelungen.
- Anonymous-ftp-Server können nur mit umfangreicher Kontrolle der angebotenen Daten betrieben werden. Beim Mirroring eines Servers ist ein Vertrag mit dem Betreiber des Ursprung-Servers erforderlich.
- Das WWW wird auf Dauer ein sehr wichtiges, wenn nicht das wichtigste Medium für die Außenwirkung eines Rechenzentrums oder des Rechenzentrumbetreibers. Im Sinne von Coporate Identity muß die Selbstdarstellung im WWW reglementiert und kontrolliert werden.
- Alle Voreinstellungen des Rechenzentrumsbetreibers müssen restriktiv gewählt werden. Der einzelne Benutzer kann dann die Restriktionen durch gezielte Maßnahmen, die er dann auch verantworten muß, verändern.
- Zur Vermeidung von Anwaltskosten sollte man vor dem Anbieten im WWW prüfen, wer die Rechte an den Werken hat, und gegebenenfalls eine Einwilligung einholen.
- Der Betreiber eines Rechenzentrums darf in Benutzerdateien ohne Zustimmung des Benutzers nicht hineinschauen. Besteht der Verdacht auf Mißbrauch, so muß entweder die Zustimmung eingeholt werden oder es müssen die Strafverfolgungsbehörden eingeschaltet werden.

Ich danke J. Bizer für anregende Diskussionen. Der Beitrag ist die erweiterte Fassung eines Vortrags auf der 11. GI Fachtagung über Rechenzentren, Göttingen, 1995.

Rainer W. Gerling, Max-Planck-Gesellschaft, München
E-Mail: gerling@mpg-gv.mpg.de ■

FIfF e.V.

Satzung

Errichtet am 2. Juni 1984. — Änderungen vom 29. Juni 1985, 17. Oktober 1987 und 18. November 1995 eingearbeitet. Vereinsregister beim Amtsgericht Bonn, Nr. VR 5102.

§1 Name und Sitz

(1) Der Verein trägt den Namen „Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V.". Er hat seinen Sitz in Bonn.

(2) Als Geschäftsjahr gilt das Kalenderjahr.

§2 Zweck

(1) Zweck des Vereins ist es, zu Wechselwirkungen zwischen Informations- und Kommunikationstechnologie einerseits und Gesellschaft und Umwelt andererseits, insbesondere über den Zusammenhang von Informationstechnik und Rüstung,

- eigene wissenschaftliche Beiträge und Forschungen zu leisten, und sich an derartigen Projekten zu beteiligen,
- die Öffentlichkeit und Fachwelt zu informieren.

Der Verein wirkt darauf hin, daß Informations- und Kommunikationstechnologie als Mittel der Völkerverständigung entwickelt und genutzt wird.

(2) Ein Schwerpunkt des Vereins liegt in der Friedensarbeit und -forschung im Sinne der Förderung der Völkerverständigung; seine vordringlichen Aufgaben sind:

a) die Bedeutung der Informationstechnik und der Arbeit der DV-Fachleute für militärtechnische Zwecke aufzuzeigen,

b) den militärischen Einfluß auf die Entwicklung der Informationstechnik und auf die Fachgebiete der Informations- und Kommunikationstechnik zu untersuchen,

c) die prinzipielle Fehlerhaftigkeit informationstechnischer Systeme, insbesondere komplexer Systeme im militärischen Bereich, und deren Implikationen aufzudecken,

d) die eigenen Fachkollegen, die politischen Entscheidungsträger und die Öffentlichkeit zu informieren und zur Diskussion zu ermuntern,

e) das Verantwortungsbewußtsein der im Bereich der Informationstechnik Tätigen zu schärfen,

f) gesellschaftlich verantwortbare und die internationale Zusammenarbeit fördernde Alternativen zur militärisch orientierten Forschung und Entwicklung im Bereich der Informationstechnik zu erarbeiten.

(3) Zu den weiteren Zielen des Vereins gehört es:

a) die Bedeutung der Informationstechnik und die Arbeit der DV-Fachleute für die Schaffung von Rationalisierungs- und Kontrolltechnologien aufzuzeigen,

b) die Verantwortung für die gesellschaftlichen Auswirkungen von Informationstechnologie mit der Verantwortung für die Forschung und Entwicklung von Informationstechnologien zu koppeln.

(4) Der Vereinszweck soll insbesondere verwirklicht werden durch:

a) fachliche und wissenschaftliche Unterstützung von regionalen Gruppen und Initiativen, die dieselben Zwecke verfolgen,

b) Durchführung von und Beteiligung an wissenschaftlichen Tagungen und Kongressen, Verbreitung der Erkenntnisse in öffentlichen Veranstaltungen,

c) Durchführung, Beteiligung, Vergabe und Veröffentlichungen von wissenschaftlichen Untersuchungen, Forschungsvorhaben und Projekten,

d) wissenschaftlichen Dienstleistungen und Bildungsangebote,

e) Zusammenarbeit mit nationalen und internationalen Organisationen, die ähnliche Zwecke verfolgen,

f) Einrichtung und Unterhaltung einer Geschäftsstelle, die organisatorische Arbeiten erledigt und dem Vorstand sowie den Arbeitsgruppen zuarbeitet.

(5) Der Verein ist parteipolitisch und weltanschaulich unabhängig.

§3 Gemeinnützigkeit

(1) Der Verein verfolgt ausschließlich und unmittelbar gemeinnützige Zwecke im Sinne des Abschnitts „Steuerbegünstigte Zwecke" der Abgabeordnung.

(2) Der Verein ist selbstlos tätig. Er verfolgt nicht in erster Linie eigenwirtschaftliche Zwecke.

(3) Mittel des Vereins dürfen nur für die satzungsgemäßen Zwecke verwendet werden. Die Mitglieder des Vereins erhalten in ihrer Eigenschaft als Mitglieder keine Zuwendungen aus Mitteln des Vereins.

(4) Es darf keine Person durch Ausgaben, die dem Zweck des Vereins fremd sind, oder durch unverhältnismäßig hohe Vergütungen begünstigt werden.

§4 Mitgliedschaft

(1) Jede natürliche Person aus Wissenschaft oder Praxis, die sich mit der Informationstechnik befaßt, kann Mitglied des Vereins werden, wenn sie die Zwecke des Vereins anerkennt und fördern will.

(2) Jede natürliche Person, Organisation oder Vereinigung, die den Verein und seine Ziele finanziell unterstützen will, kann dies durch Spenden oder durch eine kontinuierliche Fördermitgliedschaft tun.

(3) Der Antrag auf Mitgliedschaft muß schriftlich an den Vorstand gerichtet werden. Über die Aufnahme entscheidet der Vorstand. Ablehnungen müssen schriftlich begründet werden. Gegen die Ablehnung kann die nächste Mitgliederversammlung angerufen werden, die endgültig entscheidet.

(4) Die Mitgliedschaft beginnt mit dem Tag der Aufnahmebestätigung. Die Mitgliedschaft endet durch Austritt, Ausschluß oder Tod.

(5) Der Austritt ist dem Vorstand gegenüber schriftlich zu erklären. Er ist fristlos wirksam.

(6) Mitglieder, die gegen die Ziele des Vereins verstoßen oder das Ansehen des Vereins schädigen, können durch Beschluß des Vorstandes ausgeschlossen werden. Gegen den Beschluß kann das Mitglied mit aufschiebender Wirkung die nächste Mitgliederversammlung anrufen, die dann endgültig entscheidet. Auf Wunsch hat persönliche Anhörung zu erfolgen.

§5 Rechte und Pflichten der Mitglieder

(1) Mitglieder haben das persönliche Stimmrecht in der Mitgliederversammlung. Eine Übertragung des Stimmrechts ist nicht möglich.

(2) Alle Mitglieder haben das Recht, dem Vorstand und der Mitgliederversammlung gegenüber Anträge zu unterbreiten. Sie sind berechtigt, an allen Veranstaltungen des Vereins teilzunehmen.

(3) Die Mitglieder erhalten außer der Erstattung von Auslagen keinerlei Zuwendungen aus dem Verein.

(4) Der Verein erhebt einen jährlichen Mitgliederbeitrag. Über die Höhe des Beitrags entscheidet die Mitgliederversammlung.

(5) Für die Verbindlichkeiten des Vereins haften die Mitglieder nur mit ihren etwaigen rückständigen Beiträgen. Jede weitergehende Haftung ist ausgeschlossen.

(6) Fördernde Mitglieder erhalten die Rundbriefe des Vereins, haben ansonsten weder vereinsbezogene Rechte noch Pflichten.

§6 Organe des Vereins

Die Organe des Vereins sind:

(1) die Mitgliederversammlung,

(2) der Vorstand.

§7 Mitgliederversammlung

(1) Die Mitgliederversammlung ist das höchste Organ des Vereins.

(2) Der Vorstand beruft die Mitgliederversammlung mindestens einmal jährlich ein. Er kann jederzeit eine außerordentliche Mitgliederversammlung einberufen. Er muß eine außerordentliche Mitgliederversammlung einberufen, wenn mindestens 10% der Mitglieder dies verlangen.

(3) Die schriftliche Einladung zur Mitgliederversammlung ist unter Beifügung der Tagesordnung spätestens vier Wochen vor deren Termin abzusenden oder in der entsprechend rechtzeitig verschickten Mitgliederzeitung zu veröffentlichen.

(4) Die Mitgliederversammlung ist beschlußfähig, wenn sie ordnungsgemäß einberufen wurde, unabhängig von der Zahl der erschienenen Mitglieder.

(5) Die Mitgliederversammlung hat folgende Aufgaben:

a) sie wählt den Vorstand,

b) sie nimmt den Kassenbericht und den Rechenschaftsbericht des Vorstands entgegen und erteilt dem Vorstand Entlastung,

c) sie entscheidet über die Aufgaben des Vereins, die Richtlinien der künftigen Arbeit und die Verwendung der finanziellen Mittel,

d) sie entscheidet über die Höhe der Mitgliedsbeiträge,

e) sie beschließt über Satzungsänderungen und über die Auflösung des Vereins.

§8 Vorstand

(1) Der Vorstand besteht aus einem/r Vorsitzenden, einem/r stellvertretenden Vorsitzenden und mindestens drei weiteren Personen.

(2) Der Vorstand führt die laufenden Geschäfte des Vereins und erledigt die ihm von der Mitgliederversammlung übertragenen Aufgaben.

(3) Die Vorstandsmitglieder sind je einzeln zur Vertretung des Vereins berechtigt.

(4) Der Vorstand wird auf die Dauer von 2 Jahren gewählt und bleibt bis zur Wahl eines neuen Vorstands im Amt. Wiederwahl oder vorzeitige Abwahl ist möglich.

(5) Der Vorstand ist beschlußfähig, wenn in der Vorstandssitzung mindestens die Hälfte der Vorstandsmitglieder anwesend ist. Der Vorstand entscheidet mit einfacher Mehrheit der abgegebenen Stimmen.

§9 Regionalrat

(1) Der Verein kann einen Regionalrat bilden. Dieser setzt sich aus Vertretern der regionalen Gruppen und Initiativen sowie aus weiteren, von der Mitgliederversammlung gewählten Personen zusammen.

(2) Die Amtszeit von Mitgliedern des Regionalrats kann von der Mitgliederversammlung begrenzt werden.

(3) Der Regionalrat unterstützt den Vorstand bei dessen Aufgaben.

(4) Aus der Mitgliedschaft ergeben sich darüberhinaus keinerlei besondere Rechte oder Pflichten gegenüber dem Verein.

§10 Beirat

(1) Der Verein kann einen Beirat bilden. Der Beirat berät den Vorstand bei wissenschaftlichen und satzungsmäßigen Angelegenheiten.

(2) Der Vorstand bestimmt über die Mitgliedschaft im Beirat.

(3) Aus der Mitgliedschaft im Beirat ergeben sich darüberhinaus keinerlei besondere Rechte oder Pflichten gegenüber dem Verein.

§11 Auflösung des Vereins

Bei Auflösung des Vereins oder bei Wegfall seines bisherigen Zwecks fällt das Vermögen des Vereins an eine von der Mitgliederversammlung im Zusammenhang mit dem Auflösungsbeschluß zu bestimmende Körperschaft, die es unmittelbar und ausschließlich für gemeinnützige Zwecke im Sinne dieser Satzung verwenden muß.

§12 Schlußbestimmung

Die Satzung tritt mit der Annahme durch die Mitgliederversammlung am 2. Juni 1984 in Kraft. ■

Werner Langenheder

4. 10. 1938 — 26. 12. 1995

Werner Langenheder ist tot. Er starb völlig überraschend und ohne die leiseste Vorwarnung in der Nacht zum zweiten Weihnachtstag, am 26. Dezember 1995. Es erscheint uns, die es noch immer nicht wahrhaben wollen, wie ein heimtückischer Überfall. Ein Herzinfarkt. Wir können es kaum glauben.

Werner Langenheders wissenschaftliche Leidenschaft richtete sich auf eine sozialorientierte Technikgestaltung und die damit verbundenen Aktivitäten interdisziplinärer Technikforschung. Dies ist das Feld, auf dem er bis zuletzt aktiv war. Nach einer vielbeachteten Habilitation über soziologische Handlungstheorie und anschließenden Arbeiten über die Anwendung informationstechnischer Werkzeuge in den Sozialwissenschaften übernahm er 1980 - als die GMD sich zum Aufbau einer TA-Forschungsgruppe entschloß - die Leitung der "Gruppe Wirkungsforschung" im damaligen Institut für Planungs- und Entscheidungssysteme. Diese Tätigkeit erschien ihm attraktiver und größere Wirkungsmöglichkeiten eröffnend als eine Lehrtätigkeit an einer Universität. Einen Ruf auf eine Soziologie-Professur lehnte er zugunsten der GMD ab.

Die fortdauernde Kontroverse um eine angemessene Konzeption einer TA-Gruppe innerhalb der GMD machte allerdings deutlich, wie schwer es war, eine solche Aufgabe innerhalb des organisatorischen Rahmens derjenigen Institution zu übernehmen, deren Wirken zum Gegenstand der Beobachtung gemacht werden sollte. In der Frage, ob TA eine eigenständige Aufgabe in einer Großforschungseinrichtung sein sollte oder als eine eher integrierte, in den verschiedenen Technikentwicklungsgruppen (mit mäeutischer Hilfe von in diesen Gruppen integrierten Sozialwissenschaftlern) selbst durchzuführende Aktivität verstanden werden müsse, setzte sich letztlich die zweite Position durch und führte 1983 zur Auflösung einer eigenständigen TA-Gruppe in der GMD.

In der Folgezeit richteten sich Werner Langenheders Aktivitäten auf den Aufbau eines interdisziplinären Netzwerks zum Thema „Informatik und Gesellschaft". Sein Ziel war es, eine bessere Koordinierung der verschiedenen TA-Aktivitäten sowohl innerhalb als auch außerhalb der GMD zu erreichen. Ihm schwebte die Etablierung eines Netzwerkes vor, in dem die verschiedensten Aktivitäten in Forschung und wissenschaftlicher Politikberatung nicht nur ein Informations- sondern auch ein lebendiges Diskursforum zur Gestaltung der Informationsgesellschaft finden konnten.

Dieser Netzwerkidee entsprach sein Engagement im Fachbereich 8 der Gesellschaft für Informatik (GI). Hier war er Mitglied des Leitungsgremiums und lange Zeit Sprecher der Fachgruppe „Informatik und Gesellschaft". Sein Einsatz für eine verantwortungsvolle, an sozialen und ökologischen Zielen orientierte Entwicklung der Informationstechnik äußerte sich auch in seinen Aktivitäten im Rahmen der Friedensbewegung der 80er Jahre. Er war ein aktives Mitglied der Friedensinitiative in der GMD und einer der Gründungsväter des FIFF, der bundesweiten Vereinigung kritischer InformatikerInnen. Er hat dem FIFF-Vorstand in der Anfangsphase zur Seite gestanden und mehrere Jahre die Regionalgruppe Bonn geleitet. Im Rahmen eines Kooperationsvertrages zwischen der GMD und der Universität Freiburg wirkte er seit 1991 beim Aufbau des Instituts für Informatik und Gesellschaft (IIG) der Universität Freiburg mit.

Werner Langenheder hat, wo immer er konnte, radikal gefragt, oft auch radikal in Frage gestellt, was andere für selbstverständlich gehalten haben oder für selbstverständlich gehalten wissen wollten. Die Frage nach der Eigentlichkeit, nach den „eigentlichen" Interessen von Akteuren, den „eigentlichen" Gründen für Handeln, den „eigentlichen" Bestimmungsgrößen von Umständen, hat ihn oft vor Grenzen der Beantwortbarkeit gestellt. Dies hat ihn geschmerzt, aber nicht davon abgehalten, weiter radikal zu fragen. Er hat lieber Fragen unbeantwortet gelassen, als einfacher zu fragen.

Werner Langenheder konnte in systemischen Zusammenhängen denken, verlor jedoch niemals die Rolle des Individuums innerhalb dieser Prozesse aus dem Auge. In dieser Hinsicht war er hartnäckig. Komplexe sozio-technische Entwicklungsprozesse so zu gestalten, daß sie nicht in einer Subordination des Individuums unter die systemischen Prozesse führen, das war seine große Vision. Pluralität, Demokratie und Partizipation waren die Leitbilder, an denen er nicht rütteln ließ. Daß er sich damit nicht nur Freunde schuf, sondern auch Gegner, die derartige Ideen eher als Bremsbacken denn als Schmiermittel für einen glatten Weg in die Informationsgesellschaft ansahen, mußte er hinnehmen.

Diejenigen, die mit ihm näher zusammenarbeiteten, seine ehemaligen Kolleginnen und Kollegen in der GMD-Wifo-Gruppe, im GI-Fachbereich 8 und im FIFF, am Institut für Informatik und Gesellschaft in Freiburg, aber auch viele andere, haben mit Werner Langenheder einen Kollegen verloren, der seine gesellschaftpolitischen Ansprüche an diskursive und auf gegenseitiger Anerkennung basierende Entscheidungen auch selbst lebte, privat und beruflich. Diese - auch unter fortschrittlich denkenden Menschen - seltene Eigenschaft machte Werner Langenheder angreifbar. Er wollte nicht herrschen, aber auch nicht beherrscht werden. Organisationen können mit einer solchen Haltung oft nur sehr schwer umgehen.

Werner Langenheder hat niemandem, selbst denjenigen, die ihn angriffen, die Geltungsansprüche ihres Handelns aberkannt. Für uns Jüngere, die oft geneigt waren, unsere Positionen kompromißloser durchzufechten, war das manchmal kaum zu fassen, irgendwie aber bewundernswert. Seine menschliche Art, Konflikte auszutragen und die Hilfslosigkeit seiner Umwelt, darauf angemessen zu reagieren, muß Werner oft irritiert und wohl auch verletzt haben.

Wir vermissen ihn.

Michael Paetau

Sankt Augustin im Januar 1996. ■

»Arbeit und Informationstechnologie – Wie verändert sich unsere Lebenswelt?«

Aufruf zur Teilnahme an der 13. Jahrestagung des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) in Tübingen, voraussichtlich vom 8. bis 10. November 1996.

In der derzeitigen Diskussion um den Übergang von der Industrie- zur Informationsgesellschaft dominieren Umsatz- und Gewinnerwartungen. Mit neuen Möglichkeiten der Informationstechnik aber wird sich die Art und Weise, wie Menschen arbeiten (und ihre Freizeit verbringen) wesentlich ändern. Das Ausmaß der dadurch hervorgerufenen sozialen Umwälzungen wird nur unzureichend reflektiert.

Mit diesem ersten Aufruf möchten wir, die FIFF-Gruppe in Tübingen, alle interessierten InformatikerInnen, FIFFerlinge und sonstige Interessierte zur nächsten Jahrestagung in Tübingen einladen.

Wie üblich werden wir am Freitag mit einem Plenumsvortrag beginnen. Am Samstag greifen wir in Arbeitsgruppen einzelne Aspekte des Schwerpunkthemas auf. Wir haben in einer ersten Sammlung folgende Arbeitsgruppen ins Auge gefaßt, wünschen uns aber noch weitere Ideen:

- Veränderung von betrieblichen Arbeistplätzen durch Einsatz von Informationstechnolgie: zur Debatte um Lean Production, Job Enlargement, Job Enrichment
- Telearbeit
- Rationalisierungseffekte
- Arbeitsplatzanalyse, -gestaltung
- Workflowmanagement
- projektbezogene Leiharbeit
- AnwendungsentwicklerInnen nach Indien - Wo sind in Zukunft unsere Arbeitsplätze und wie sehen sie aus?
- Internationalisierung des Datenverkehrs und ArbeitnehmerInnen-Datenschutz
- Datenschutz-Probleme bei betrieblicher Internet-Nutzung
- Städtische Online-Pilotprojekte: Erfahrungen, Handlungsmöglichkeiten, Perspektiven
- Arbeitsteilung: Möglichkeiten der Verantwortungswahrnehmung und -zuschreibung
- Einsatz von Multimedia in der Aus- und Weiterbildung
- Informatik und Schule

Wir hoffen, möglichst viele Arbeitsgruppen realisieren zu können und suchen hiermit nach ModeratorInnen, die bereit sind, die Vorbereitung einer der aufgeführten oder einer weiteren Arbeitsgruppe zu übernehmen. Eure bzw. Ihre Mitarbeit und Engagement werden maßgeblich den Erfolg der Tagung bestimmen.

Am Samstag findet auch die Mitgliederversammlung statt. Am Sonntag treffen wir uns wieder im Plenum, um die Ergebnisse aus den Arbeitsgruppen vorzutragen und mit weiteren Vorträgen die Tagung zu beschließen.

Anfragen, Vorschläge und Mitteilungen bezüglich der Jahrestagung bitten wir an die Email-Adresse

fiff@ informatik. uni-tuebingen.de

oder folgende Anschrift zu senden:

Elisabeth Meinhardt
Sekretariat
Lehrstuhl Programmierung
Kennwort: FIFF-Tagung
Universität Tübingen
Sand 13
D-72076 Tübingen
Tel. 07071/29-5754
Fax 07071/29-5958

Für telefonische Rückfragen stehen

Jochen Krämer
Tel. 07071/29-5957

Detmar Meurers
Tel. 07071/29-7314

zur Verfügung.

Die Jahrestagung wird inhaltlich

- *vom Zentrum für Ethik in den Wissenschaften an der Universität Tübingen (ZEW),*
- *von der Deutschen Vereinigung für Datenschutz e.V. (DVD),*
- *vom Institut für Kommunikationsökologie e.V. (IKÖ) und*
- *vom Kreis Netzwerk - Arbeitswelt - Informatik (NAI)*

mitgetragen und -gestaltet.

Auf unserer WWW-Seite

http://www-fiff.informatik. uni-tuebingen.de

wird es die aktuellen Informationen zur Jahrestagung geben.

Lesen

Neues für den Bücherwurm – kurz belichtet

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.):

Patienten und ihre computergerechten Gesundheitsdaten.

1995, SecuMedia, 29,- DM; ISBN: 3-922746-26-8

Kein demokratisches Land hat in solchem Maße die technische Infrastruktur zur kostendämpfenden Durchlöcherung, womöglich gar Abschaffung des Arztgeheimnisses eingeführt, wie die Bundesrepublik. Die weltweit einmalige Vollversorgung mit der Krankenversicherten-Karte (KVK) - eine Chipkarte als Berechtigungsausweis für die KassenpatientInnen - ist die Basis für das Anlegen eines abrechnungsfreundlichen Datensatzes bei jedem Arztbesuch. Für die Kassen war dies schon ein Schritt zur Kostensenkung, da der Datenaustausch ihre Verwaltungskosten senkt - ein Ergebnis von Kostendämpfungsprojekten durch Computer, die bei den Krankenkassen ab 1972 versucht wurden. DV-Firmen und Chipkartenhersteller haben sich gleichzeitig einen lukrativen Absatzmarkt aufgetan - fast ein Dutzend verschiedene weitere Chipkarten-Projekte sind geplant.

Als zweiter Schritt füllt die Abrechnung ärztlicher Leistungen nach der ICD 10-Tabelle diese Datensätze nun mit computergerecht aufbereiteten höchst sensiblen PatientInnen-Daten. An Kassenärztliche Verrechnungsstellen und Krankenkassen gehen Arzt- und PatientInnen-bezogene Daten, die im Gegensatz zu früher nicht länger von Hand, sondern maschinell auswertbar sind. Damit ist eine gründliche Rationalisierung der Verwaltungsarbeit möglich. Dieses Idealbild rationeller Verwaltung macht allerdings - sofern der Arzt nicht auf die Vergütung seiner Leistung verzichtet - das Arztgeheimnis zur Makulatur.

Vor diesem Hintergrund hatte die Gruppe Technikfolgen-Abschätzung des Bundesamts für Sicherheit in der Informationstechnik (BSI) im Herbst 1994 zu einer Veranstaltung zu „Patienten und ihre computergerechten Gesundheitsdaten" eingeladen. Vertreter von Krankenkassen, Ärzten und Patienten einerseits und Computerexperten, Ministerial-Beamte und Politiker andererseits sollten Ansichten und Befürchtungen in einem interdisziplinären Diskurs austauschen. Als Ergebnis dieser Veranstaltung liegt nun ein Buch vor, in dem viele Beiträge allerdings auf den Stand von Sommer 1995 gebracht wurden.

In einem einleitenden Beitrag begründet Anja Hartmann vom BSI ihre Akteursorientierung damit, daß bei der Sicherheit der Chipkarten-Technologie weder technische noch gesetzliche Regelungen ausreichen. Notwendig sei, die Beteiligten an den sicheren Umgang mit dieser neuen Technik zu gewöhnen und eine kulturell verankerte Basis für diese Technik - eine IT-Sicherheitskultur - zu schaffen. Zwar ist der Gedanke richtig, daß neue Technik im Alltagsleben auch kulturell adaptiert werden muß, jedoch bleibt die Ausbildung einer IT-Sicherheitskultur als „hochwertiger Kommunikationsprozeß" ebenso unscharf, wie die Frage nach deren Grenzen.

Daß Vorhersagen über die kulturelle Aneignung von Technik nicht einfach sind, zeigt Hans-Jürgen Weißbach, der die unterschiedlichen ärztlichen Kulturen im Umgang mit Daten betrachtet. Ihm gelingt es zu zeigen, welche Unwägbarkeiten und Brüche heute schon bei diesem Umgang zu finden sind. Trotzdem er die unmittelbaren Wirkungen der KVK für gering hält, legt er die Frage nahe, wie die absehbaren Formen des Umgangs mit den so erzeugten Patienten-Daten regulativ jemals gefaßt werden könnten.

Aufschlußreich ist oft ein Blick über den Tellerrand, den Leo van Romunde über die Nutzung von Computern im niederländischen Gesundheitswesen gibt. Dort nutzen 80% der Allgemeinmediziner Computer, ein Großteil auch den elektronischen Austausch von Dokumenten. Auf der Basis dieser Vernetzung werden auch dort Chipkartenlösungen debattiert - ein Teil, der ruhig hätte ausführlicher sein können.

Eines der zugänglichsten Projekte einer erweiterten Chipkartennutzung ist das Koblenzer Modell, bei dem auf einer Chipkarte sensible Daten zum Gesundheitszustand des Patienten zur Kommunikation zwischen Ärzten und Apothekern gespeichert werden. Interessant neben Projekt-Darstellungen von Beteiligten ist hier ein Beitrag eines Mediziners. Wolfgang Streit schildert die skeptischen Reaktionen seiner Patienten und warnt zugleich davor, daß diese im Zwiespalt zwischen ihrer oft ehrfürchtigen Haltung gegenüber dem Arzt und der Angst vor Verdatung ausweichen in Bereiche der Alternativ-Medizin, in denen sie keine Verdatung befürchten. Streit nennt Vertrauensverlust zwischen Arzt und Patient, der sich unter anderem in verschriebenen, aber weggeworfenen Medikamenten im Umfang von Milliarden ausdrückt und der durch die Chipkarte forciert wird, als ein Grund, warum Chipkarten für ihn das Gesundheitswesen verteuern.

Im technischen Teil werden verschiedene Ansätze und Projekte dargestellt. In einem Beitrag aus der Sicht der Forschung offenbart Gisela Meister ein grundlegendes Problem der Technikfolgen-Abschätzung: Wenn wie sie Entwicklerinnen und Entwickler es in technikzentrierter Sicht für ausreichend erachten, rechtliche Normen in System-Funktionen abzubilden, die gesellschaftlichen Einsatzbedingungen aber außen vor lassen, sind Probleme unausweichlich. Helfen könnte hier die möglichst frühzeitige Rückkopplung von TA-Arbeiten auf die Forschung - daran aber hapert es.

Nach der Lektüre des Buches läßt sich resumieren, daß darin bei der Abwägung zwischen Medizin-Cards und Arztgeheimnis kein überzeugendes Argument für die Kartentechnik zu finden ist. Im Gegenteil: Wenn die IT-Sicherheitsfachleute erklären, die Sicherheit der Technik sei nicht in den Griff zu bekommen, sollte dies eindringliche Warnung sein. Diese Warnung bleibt jedoch verhalten. Deutlich schimmert das Interesse an der Herausforderung für die IT-Sicherheit durch. Auch die Frage nach Alternativen wurde zwar gestellt, aber nicht ernsthaft auf sie eingegangen.

Das verweist auf drei Defizite des Projekts. Als erstes fehlt schlicht ein kurzer juristischer Problemaufriß, der über den Datenschutz hinausgeht. Vertragsverhältnisse im Gesundheitswesen, Schweigepflicht und Freiheit ärztlicher Berufsausübung sind Fragen, die die juristische Verträglichkeit einer technischen Lösung klären könnten.

Nur ansatzweise, oft aber gar nicht, wurde zum zweiten auf die Interessen der die Technikentwicklung und -nutzung betreibenden Akteure eingegangen. Sowohl, wenn man es als TA-Projekt zur Politikberatung versteht und den selbst postulierten Akteursansatz ernst nimmt, als auch zur Abschätzung der Sicherheitsgefährdung wäre eine eingehende Darstellung der grundlegenden Einsatzmotive nötig gewesen. Sie hätte auf Gestaltungsspielräume und -grenzen verwiesen.

Defizitär war zum dritten, mangels technischer Lösungen den kulturellen gesellschaftlichen Hintergrund als Lösungsausweg ins Spiel zu bringen, nicht jedoch danach zu fragen, wo kulturell die Grenzen akzeptierbaren Technikeinsatzes im Gesundheitswesen liegen. Wenn auch in der Bundesrepublik die Reaktion auf den technischen Abbau des Arztgeheimnisses im internationalen Vergleich schwach ist, zeigen die Reaktionen bei Ärzten wie PatientInnen, daß es Grenzen des als zumutbar empfundenen gibt. Auch die Karten-Promotoren wissen das und - Beispiel Koblenz - werben durch Offenheit für ihre Projekte. TA-Forschung, die diesen Konflikt nicht genügend berücksichtigt, liefert keine Antwort auf die wichtigste Frage.

Dennoch ist das Buch eine interessante Lektüre und empfehlenswert gleichermaßen für Interessierte sowohl an medizinischen ChipCards als auch TA. Bedenkt man, daß kein anderes Bundesamt Aufgaben im Bereich TA hat, so ist das Buch noch bemerkenswerter.

(Ingo Ruhmann)

Bertrand, Ute; Kuhlmann, Jan; Stark, Claus:

Der Gesundheitschip – Vom Arztgeheimnis zum Gläsernen Patienten.

1995, Campus, 29,80 DM; ISBN: 3-593-35353-9

Seit 1995 ist in Deutschland die Chipkarte bundesweit als „Ausweis" der ordnungsgemäß Krankenversicherten eingeführt, in Österreich hat es dazu Feldversuche gegeben. Diese Chipkarte ist ein recht passender Anlaß für ein Buch wie dieses: es geht hier gar nicht so sehr um das hübsche kleine Kärtchen selbst, sondern um die Hintergründe eines neuen und bei genauer Hinsicht, zunehmend totalitäre Züge annehmenden Systems.

War der Krankenschein das Symbol für die Bürokratisierung des Gesundheitswesens im deutschen (und ebenso österreichischen) Verwaltungsstaat, so ist die Chipkarte nunmehr das Symbol für die weit weitergehende Informatisierung dieses Gesundheitswesens, und für die „Ver-Ordnung" auf einer neuen Stufe. Um diese Sachen geht es in diesem Buch:

- zuerst um eine kleine und hochinteressante Geschichte medizinischer Leitbilder,
- dann um einen knappen Rückblick auf die Beziehung von Medizin und Sozialversicherung,
- schließlich um die Funktion und Rolle der Ärzte, der praktischen Medizin in unserer Gesellschaft,
- dann - wie auch in der alltäglichen Lebenswelt zuletzt - um den sogenannten „Patienten", den üblicherweise oder auch hoffentlich sozialversicherten Menschen.
- Zentrales Thema bleibt dabei die Vernetzung von medizinischer Information, die Verwaltung dieser Information und schließlich die weitere Rationalisierung von Informationsverwaltung.

Es ist eine enorme und hoch ausdifferenzierte Macht, die im Verlauf der letzten rd. 200 Jahre den Gesundheitsberufen zugeschoben wurde. Wo immer es um Krankheit, um Persönliches, oft um Allzupersönliches geht, bestimmen mittlerweile Ärzte, Krankenschwestern, sonstige allgemein Heilungsbefugte, gelegentlich auch Psychotherapeuten, den Weg der individuellen Gesundung und Heilung: der Einordnung zuerst (Diagnose), dann den der Rückführung (Therapie); oft über die Intentionen, Motive und natürlich die eigentlichen Verursacher des persönlichen Krankheitsbildes hinweg. Zentrale Perspektive bei dieser medizintechnischen Verwaltung von Versorgungsleistungen ist ein altes, und vergleichsweise totalitäres Modell: Die Sicht des individuellen Menschen als kleine Bio-Maschine, die handwerklich (bis wissenschaftlich) bearbeitbar ist. Dabei sind die Versicherten mittlerweile von der direkten Kontrolle weitgehend ausgeschlossen (vgl. S 48); so etwas würde die pseudobürokratische Objektivität des Medizinapparates bedrohen (vgl. S 62).

Aus der Perspektive dieser (heute mittlerweile dominanten) gesellschaftlichen Logik der Verwaltung von individueller Gesundheit besehen, ist es nur zu verständlich, mit den technologischen Fortschritten auch die Informationsseite besser und regelgerechter verwalten zu können. Statt Papier eben Elektronik, statt persönlicher „Behandlung" (Begegnung, Zugang, Verantwortung, Einschätzung usw.) nunmehr sog. 'objektive' Information, und: alle (egal ob der Betroffene die Zusammenhänge kennt oder nicht) wissen über Alles Bescheid. Letztlich sollen objektive Maschinen (egal wie subjektiv deren Programme sind - [das ist die Ebene dahinter, die interessiert ja niemanden wirklich]) statt individuelle, mit leider immer noch zuviel Skrupeln ausgestattete Menschen entscheiden. Und es sollen allgemeine Regeln gelten, egal ob zur simplen ärztlichen Meldung über einen Behandlungsfall zur Versicherungsnummer xxx, oder zur Vorausinformation, oder zur Administration, oder zur Anweisung, was das Abschalten lebenserhaltender Maschinen oder das Auswaiden von verwertbaren Organen anlangt.

Eines wird aus der im Buch so nicht angesprochenen Schärfe, aber in der Meinungsbildung des skeptischen Lesers dann schon irgendwie deutlich absehbar: Die kommende Verdatung der individuellen Menschen (denen wir uns bislang nur mit ihrem mitunter recht still ausgesprochenen und vorsichtig erlaubten Einverständnis nähern können, - das Begreifen von individuellen Biographien kostet ja dem Gegenüber manchmal sehr viel an eigener Zeit) macht das Ordnungsprinzip gesellschaftlicher Administration umfassend. In Wahrheit ist ja das die unausgesprochene Zielsetzung in der Informatisierung der Alltagswelt: das Durchsetzen von Ordnungsprinzipien, oder - wenn man so will: der optimierten Verwaltung der einzelnen Individuen (vgl. William Bogard: The Simulation of Surveillance: Hypercontrol in Telematic Societies. Cambridge (Cambridge University Press) 1995).

Und, eines wird aus den Analysen in diesem Buch doch recht deutlich, auch wenn das nicht in dieser Form so explizit angesprochen wird: der totale Gesundheitschip, auf dem sich alles und jedes irgendwie gesundheitlich Relevante über die betroffene Person findet, kommt über kurz oder lang unweigerlich auf uns zu. Am sinnvollsten wird es, fortgedacht, in sagen wir 15 Jahren sein, wir implantieren ihn gleich nach der Geburt. Die informationelle Logik der Struktur unseres gegenwärtigen Gesundheitsverwaltungssystems legt das ja auch nahe. Dazu kommt noch: „Eine Gesellschaft, die Politiker und Wissenschaftler zur „Informationsgesellschaft" erkoren haben, verkauft diesen Wandel als Befreiung, Information gilt als Schlüssel zu Freiheit, Gleichheit und Demokratie." (vgl. S 25).

Alle, die sich - ohne die Geschichte der gegenwärtigen Medizin aus den Augen zu verlieren -

aus einer gewissen, gebotenen Distanz mit der Gegenwart und künftigen Entwicklung von Gesundheitsdienstleistungen unter dem Gesichtspunkt der Verdatung und der informationstechnologischen Entwicklung auseinandersetzen wollen, kann dieses Buch nur empfohlen werden. Einen Kritikpunkt allerdings gibt es: die für die einzelnen Abschnitte Verantwortlichen erscheinen etwas zu unkenntlich, - ein bißchen zu sehr ist das die Autoren vereinende Gemeinsame, das zweifellos vorhanden ist, betont. Weniger sanfte Übergänge hätten hier auch nicht geschadet.

(Karl Kollmann)

Datow, M. et al (Hrsg.):

MultiCard Berlin – Die Kongreß-dokumentation (1994, 1995, 1996).

inTime, Berlin, jeweils ca. 50,- bis 70,- DM.

Alljährlich im Januar trifft sich die Crème der deutschen Chipkartenelite in Berlin zum Fachdisput auf der MultiCard. Dabei handelt es sich leider nicht um eine wissenschaftliche Veranstaltung - das ganze wird von den großen Kartenfirmen wie Giesecke&Devrient und Siemens gesponsort und die Referenten sind stets handverlesen. Kritische Töne kommen nur langsam und zögerlich auf der MultiCard zu Wort - Die Kongresse widmen sich vorrangig den großen Anwendungsfeldern (z.B. Banken, Gesundheitswesen, Verkehr) und den grundsätzlichen Aspekten der Verkartung (Sicherheit, Multifunktionalität, Technologien), miesepetrige Kritik ist nicht gefragt. Der vorliegende dritte Band von 1996 „Die Chipkarte im Alltag. Anwendungskonzepte und Verbraucherschutz" erweitert den Focus aber langsam auch auf kritische (Verbraucher-)Belange - wird man sich langsam klar, daß auch das schönste Kartenhaus ohne zufriedene Endbenutzer schnell in sich zusammenfällt? Vielleicht gibt es auf der MultiCard 97 sogar endlich einen FIFF-Referenten, der den Finger tief in die Wunden legen darf? Nötig wäre es, denn bisher wurden Themen wie AsylCard, Sicherheitsstaat und Gläserner Bürger elegant ausgespart.

Nichtsdestotrotz sind die Beiträge in den bisher vorliegenden drei Tagungsbänden für Chipkarteninteressierte sehr aufschlußreich - sei es, um zu erfahren, was Industrie und Ministerien planen; sei es, um sich einfach über die vielfältigen Einsatzmöglichkeiten und Probleme von Karten zu informieren. Im aktuellen Band beispielsweise wird die Verkartung im Hochschulbereich aus Industrie- und Verwaltungssicht intensiv diskutiert - für Kritiker sicherlich hochinteressante Lektüre. Aber auch der Verbraucherschutz kommt in diesem Band zu Wort: Kritische Referenten versuchen, die Anforderungen an eine akzeptable und sozialverträgliche Karte zu entwickeln. Diese Kriterien sollten innerhalb des FIFF diskutiert werden. Interessant und wichtig sind auch die finanzpolitischen Überlegungen zum Plastikgeld.

Die MultiCard-Tagungsbände gehören für chipkarteninteressierte FIFFerlinge zur Pflichtlektüre.

(Claus Stark)

Die Kongreßbände können direkt bestellt werden bei: inTime berlin, Seesener Straße 53, 10711 Berlin, Tel.: 030 / 8929763 (M. Datow)

Friedrich, J.; Herrmann, Th.; Peschek, M.; Rolf, A. (Hrsg.):

Informatik und Gesellschaft.

1995, Spektrum Akademischer Verlag, 38,- DM; ISBN: 3-86025-521-5

Mit „Informatik und Gesellschaft" erwirbt man zu einem durchaus attraktiven Preis eine Mischung aus kurzgefaßtem Lehrbuch und Nachschlagewerk der kritischen Informatik, in dem fast alle AutorInnen aus dem deutschsprachigen Raum versammelt sind, die in dieser community Rang und Namen und etwas zu sagen haben. (Man hätte sich allerdings gewünscht, die VerfasserInnen der einzelnen Kapitel schon im Inhaltsverzeichnis genannt zu bekommen, statt sie sich erst im Buch selbst erschließen zu müssen.) Das Buch läßt die Akzente und Unterbelichtungen, Stärken und Schwächen der gegenwärtigen Debatte gut erkennen. Sein Schwergewicht liegt auf einer - im Sinne der Steinmüllerschen Definition - „angewandten Informatik"[1], also auf der Darstellung einzelner Einsatzbereiche der Informatik (Tl. 2 des Buches), verschiedener Dimensionen von Wirkungen und Handlungsanforderungen (Tl. 3) und einzelner Perspektiven für eine sozialorientierte Gestaltung der Informatik (Tl. 4). Demgegenüber sind die einleitenden Reflexionen über Informatik und Gesellschaft: Grundlagen einer neuen Orientierung der Informatik (Tl. 1) mit 28 S. und die abschließende Erörterung der Verortung der Informatik zwischen Theorie und Praxis (Tl. 5) mit 40 S. eher knapp geraten. Die Thematisierung von Problemen und Theorieansätzen zum Verständnis der „Informationsgesellschaft", die in der angelsächsischen und französischen Diskussion einigen Stellenwert besitzen, fehlt ganz - auch hierin ist das Buch ein getreues Abbild der deutschen Debatte. Antworten auf Fragen wie die, was Information eigentlich ist und wodurch sie sich etwa von Wissen oder Erkenntnis unterscheidet, oder was die Informatisierung für die Qualität und Struktur der gesellschaftlichen Arbeit bedeutet, oder ob die „Informationsgesellschaft" im Sinne ihrer Propagandisten informierte Gesellschaft ist, oder schließlich, wie sich die Informatisierung auf die Stellung des Individuums in der Gesellschaft auswirkt (erhält der Einzelne neue Chancen der Individualisierung im Sinne der Becks oder wird er - wie Holling und Kempin argumentieren - zum „peripheren Individuum" am Rande eines gesellschaftsprägenden Informationssystems?[2]), sucht man vergeblich.

Nun soll diese Mängelanzeige keineswegs den Wert des vorgelegten Bandes schmälern; er faßt in i.d.R. gut geschriebener und komprimierter Form das zusammen, was die kritische Informatik in Deutschland heute zu bieten hat. Der skeptische Blick auf Selbstverständnis und Sichtweisen der Informatik wird ergänzt um eine Skizze der Sozialgeschichte der Datenverarbeitung (Rolf und Berger in Tl. 1 des Buches). Der Einsatz der IuK-Techniken ist Gegenstand von Tl. 2; er wird in der Arbeitswelt - und zwar in der Produktion (Brödner), der Material- und Güterlogistik (Char und Danckwerts), den Dienstleistungen (Becker-Töpfer und Richter), in Büro und Verwaltung sowie zur computergestützten Überwachung in der Arbeitswelt (Friedrich) - und im staatlichen Bereich - und zwar bei Planung, Verwaltung und öffentlichen Diensten (Brinckmann), zur inneren Sicherheit (Brozio und Wilhelm), im militärischen Kontext (Bernhardt und Ruhmann), im Gesundheitssystem und Sozialbereich (Dimitz und Wagner) sowie im Bildungssektor (Schulz-Zander) - dargestellt. Während auf der einen Seite zu optimistische Perspektiven (z.B. Brödners Vorstellung von „menschenzentrierten Produktionskonzepten") eher kritisch zu hinterfragen sind, werden auf der anderen Seite auch brisante Themen wie „Überwachungsstaat" (Brozio und Wilhelm) oder der militärische Ursprung vieler Komponenten der IuK-Techniken (Bernhardt und Ruhmann) nicht ausgespart. Als wichtige Dimensionen von Wirkungen und Handlungsanforderungen werden in Tl. 3 die Arbeitsmarkt- und Berufsstruktur (Dostal), vernetzte Organisation (Wagner), Produktqualität (Nake), Informatik und Ökologie (Rolf und Page), Frauen und Informationstechnologie (Schelhowe), die Gesichtspunkte Belastungsoptimierung und Persönlichkeitsförderlichkeit (Herrmann) sowie Denk- und Kommunikationsstrukturen (Erb und Herrmann) behandelt. In dem umfangreichsten Tl. 4 geht es, als Ausfüllung des Themas Perspektiven für eine sozialorientierte Informatik, um die Gerätetechnik (Coy), die Programmiersprachenentwicklung (Pflüger), Arbeitsanalyse und Softwareentwicklung (Rödiger), die Software-Ergonomie (Maaß und Oberquelle), das Software Engineering (Floyd und Falck), um rechtliche Bedingungen der Systemgestaltung (Meyer-Degenhardt), um Datenschutzfragen (Peschek und Steinmüller), ferner um künstliche Intelligenz und Expertensysteme (Bonsiepen bzw. Busch), schließlich um Netze und verteilte Systeme (Höller und Kubicek). In jedem Abschnitt wird am Schluß der Versuch unternommen, praktische Konsequenzen und Leitlinien zu formulieren. In der abschließenden Diskussion von Informatik zwischen Theorie und Praxis (Tl. 5) behandeln Langenheder die Technikfolgenabschätzung, Domeyer, Grusdat, Kuhnt, Schmithals und Wildt die Didaktik von „Informatik und Gesellschaft", Peschek ethische Probleme, Roloff den Zusammenhang von Professionalisierung und Zugangschancen von Frauen und schließlich Friedrich Probleme der Berufspraxis von InformatikerInnen. Als kompetente und anregende Darstellung mit den genannten Begrenzungen ist der Band sehr zu empfehlen; er stellt Denkansätze und Stand einer wissenschaftlichen community sehr gut dar. Besonders hervorzuheben ist das mit 22 S. umfangreiche, gegliederte und für weiterführende Lektüre sehr nützliche Literaturverzeichnis am Schluß des Buches.

(Rudi Schmiede)

Der Rat für Forschung, Technologie und Innovation

Informationsgesellschaft – Chancen, Innovationen und Herausforderungen. Feststellungen und Empfehlungen.

1995, BMBF, kostenlos.

Neu sind die Empfehlungen, die der Technologierat zum Thema „Chancen, Innovationen und Herausforderungen" der Informationsgesellschaft in Bonn präsentiert hat, nicht. Und wenn es gar heißt, mit diesem Bericht der Experten aus Wissenschaft, Wirtschaft, Gewerkschaften und Politik eröffne sich für die Gesellschaft erstmals die Chance, aktiv statt reaktiv auf Folgen neuer Technik zu handeln, ist das schlicht Schönfärberei. Denn alles, was der Technologierat jetzt festgestellt hat, war bereits im Kanzleramt der sozialliberalen Koalition angedacht. Nach der Wende 1982 wurde es nur unter den Teppich gekehrt. Hätte man statt dessen schon damals agiert, brauchte man jetzt nicht zu reagieren - im Hinblick auf Datenschutz, Medienrecht, Bildungswesen, Arbeitsleben oder auf Wettbewerb und die Herausbildung neuer Monopole in der schönen neuen Multimediawelt. Schließlich befinden wir uns längst mitten in der Informationsgesellschaft, ohne die Folgen - etwa der Telearbeit - auf Arbeitswelt und Arbeitsrecht auch nur halbwegs abgeschätzt zu haben.

(Wolfgang Hoffmann, aus: Die Zeit vom 29.12.1995)

Der Report kann kostenlos angefordert werden beim Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie (BMBF), Broschürenstelle, 53170 Bonn, Tel.: 0228 / 573917. Oder via Internet: http://www.dlr.de/bmbf

Eine weitere Broschüre der Bundesregierung mit dem Titel „Die Informationsgesellschaft - Fakten, Analysen, Trends" ist über das Wirtschaftsministerium zu beziehen: Bundesministerium für Wirtschaft, Ref. Öffentlichkeitsarbeit, Kennwort: BMWi-Report, 53107 Bonn, WWW: http://www.dlr.de/BMWi/

Bundesamt für Sicherheit in der Informationstechnik (Hrsg.):

Chipkarten im Gesundheitswesen – Abschlußbericht. Band 5 der Schriftenreihe zur IT-Sicherheit.

1995, Bundesanzeiger, 44,- DM; ISSN: 0947-093X

Dieser Band faßt die Ergebnisse des vom BSI initiierten Diskursprozesses zum Thema „Chipkarten im Gesundheitswesen" zusammen. Ziele waren, die „Folgen fehlender Sicherheitsvorkehrungen im definierten Anwendungsfeld aufzuzeigen, Konzepte zur Verhinderung von Verletzlichkeiten und Abhängigkeiten zu entwickeln und die Grundlagen für die Beratung von Herstellern, Vertreibern und Anwendern in Fragen der IT-Sicherheit bereitzustellen". Zwei dieser drei Ziele wurden teilweise erreicht: Risiken wurden offen dargestellt und Chipkarteninteressierte können sich ganz gut über die gesellschaftliche Brisanz unbedachter Technikeinführung schlaumachen. Nur Konzepte, die Verletzlichkeiten verhindern sollen, sind halt nicht so einfach zu entwickeln. Zugute halten muß man den Autoren, daß Sie IT-Sicherheit nicht nur technisch, sondern auch organisatorisch, rechtlich, ökonomisch, ökologisch und gesellschaftlich verstehen. Der rote Faden durch diese Studie ist folgerichtig die Forderung nach einer angemessenen Sicherheitskultur.

Neben der technischen Bestandsaufnahme und der ganzen Diskussion um „Chancen und Risiken des Einsatzes von Patientenkarten" machten die Verfasser Handlungsfelder aus, in denen die IT-Sicherheit erhöht werden sollte. Die Studie geht dabei auf die Diskussion „Freiheit vs. Sicherheit in einer Informationsgesellschaft" ein und fordert eindeutig die Vermeidung von Kontrollpotentialen (Kein „Gläserner Patient!") ein - so erhält FIFF unverhoffte Rückendeckung durch das BSI.

[1] Vgl. Wilhelm Steinmüller: Informationstechnologie und Gesellschaft. Einführung in die Angewandte Informatik, Darmstadt: Wiss. Buchgesellschaft 1993

[2] Vgl. Ulrick Beck; Elisabeth Beck-Gernsheim (Hrsg.): Riskante Freiheiten, Frankfurt a.M.: edition suhrkamp 1994; Eggert Holling; Peter Kempin: Identität, Geist und Maschine. Auf dem Weg zur technologischen Zivilisation, Reinbek bei Hamburg: Rowohlt TB-Verlag 1989

Es ist wohl dem Initiator Otto Ulrich zu verdanken, daß bei der Durchführung der Studie keine Scheuklappen in Bezug auf potentielle gesellschaftliche Chancen und Risiken getragen wurden: Die schärfsten Kritiker und die euphorischsten „Macher" wurden eingeladen - nichtsdestotrotz war man meilenweit von einem herrschaftsfreien Diskurs à la Habermas entfernt. Unverständlich ist auch, warum die Verfasser in das Horn der „Wertneutralität der Chipkarte" blasen - mit dieser These lockt man doch nur noch die Chipkartenprotagonisten hinter dem Ofen hervor - und das auch nur, weil denen das gut in ihr Konzept paßt. Die Studie ist insgesamt sehr lesenswert und kann zur Aufweichung starrer Fronten beitragen - deshalb sollten die Chipkarteneuphoriker und -kritiker auch mal einen Blick hineinwerfen.

(Claus Stark)

Rankl, W.; Effing, W.:

Handbuch der Chipkarten. Aufbau - Funktionsweise - Einsatz.

1995, Hanser, 68,- DM; ISBN: 3-446-17993-3

Wer sich für die Hard- und Software von Chipkarten interessiert, dem sei dieses Buch empfohlen - zumal es zur Zeit auch kein anderes deutschsprachiges Werk dazu gibt. Es ist in einem ingenieur-typischen Stil geschrieben - für Techniklaien ohne Vorkenntnisse in Mathematik und Datenübertragung wird es nur schwer verständlich sein. Inhaltlich findet man im Buch alle relevanten Themen: Von der Kartenherstellung über die informationstechnischen Grundlagen der Datenübertragung bis hin zum Aufbau der Betriebssysteme (am Beispiel von STARCOS) und von ganzen Anwendungen ist alles drin. Wer allerdings Details über konkrete Chipkarten(anwendungen) sucht, blättert vergeblich. Diese werden nicht verraten, es werden nur Prinzipien dargestellt - da hätte man von den beiden Mitarbeitern der Firma Giesecke&Devrient schon etwas mehr Nähkästchenplauderei erwartet. Um sich einen groben Überblick über die Technik von Chipkarten zu verschaffen, ist das Buch sicherlich geeignet - mehr Literaturhinweise auf grundlegende Lehrtexte („Was ist nochmal ein Generatorpolynom?") wären nützlich gewesen. Als technisches Nachschlagewerk oder als eigenständiger Lehrtext für Chipkarteninteressierte ist es leider nicht zu gebrauchen - es ist ein Fachbuch für den technisch Versierten. Deshalb fehlt sicherlich auch ein Hinweis auf die kontroverse gesellschaftliche Auseinandersetzung um Chipkartenanwendungen in Deutschland.

(Claus Stark)

Bundesministerium für Forschung und Technologie

Chipkarten - Werkzeuge der Innovation. Dokumentation.

1994, BMBF, kostenlos.

Das BMFT (heute BMBF) hat zusammen mit der GMD der Chipkarte eine eigene Veranstaltung im Rahmen ihrer Reihe „Innovationen für die Informationsgesellschaft" gewidmet. Sie fand am 8.12.1994 in Bonn statt und sollte klären helfen, wie der Chipkarte als „Schlüsseltechnologie der Innovation zu breiterer Anwendung zu verhelfen" ist. Es wurde erörtert, welche Bedingungen im Politischen, im Industriellen und im Infrastrukturellen verbessert werden müßten, um das Potential der Chipkarte besser als bisher zu nutzen.

Wirtschaft, Industrie, und Verwaltung und Regierung sollten in den Dialog eintreten. So kommen auch die Protagonisten der großen Anwendungsfelder (Electronic Money, Gesundheit, Road Pricing) zu Wort und die von ihnen als unerläßlich erachteten Infrastrukturanforderungen (Trusted Third Parties, Evaluierung) wurden erörtert. Die Wirtschaft würde mit der Chipkarte und den diversen Dienstleistungen in den nächsten Jahren gerne zweistellige Zuwachsraten erreichen - das sei aber nur erreichbar, wenn Schlüsselanwendungen öffentlich vom Staat unterstützt würden!

Die Dokumentation ist nicht „state of the art", aber als erster (technokratischer) Überblick über die grundsätzlichen Fragen und Anwendungen sicherlich nützlich. Technikkritik darf man in dieser Dokumentation allerdings nicht erwarten.

(Claus Stark)

Die Dokumentation kann kostenlos angefordert werden beim Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie, Ref. 526, Heinemannstraße, 53175 Bonn, Tel.: 0228 / 59 32 26

Ellsässer, K.-H.; Kunath, H.; Leitgeb, U.; Lochmann, H.

Patient und Medizinische Informatik.

1995, ecomed, 78.-DM.; ISBN: 3-609-63500-2

Das Buch ist dem Medizininformatiker Claus O. Köhler zum 60. Geburtstag gewidmet: Alle Reden des Festaktes 1995 in Heidelberg sind enthalten. Eine kurze berufliche Autobiographie Köhlers gibt Aufschluß über sein wissenschaftliches und praktisches Wirken an der von ihm geleiteten Abteilung „Medizinische und Biologische Informatik" am Deutschen Krebsforschungszentrum Heidelberg. Der Leser erfährt z. B. einiges über die Lochkartenzeit und den ersten Dialog-Rechner am DKFZ. Den Hauptteil machen ausgewählte Texte aus dem wissenschaftlichen Wirken Köhlers aus.

Wer das Buch wegen seines ansprechenden Titels „Patient und Medizinische Informatik" gekauft hat, wird wahrscheinlich enttäuscht sein: Der Leser erfährt wenig darüber, wie Köhler sich in seinem wissenschaftlichen Werk speziell für die Patienteninteressen stark gemacht hat - da wäre sicher einiges mehr zu berichten gewesen. In den aufgenommenen Texten geht es nicht explizit um Patienten, sondern u.a. um die Zeitschriftenausstattung in einer Bibliothek und um KRATZTUR, einen Generator für medizinische Dokumentations- und Informationssysteme. Zwei Texte behandeln die Themen Shared Care und Patientenchipkarte - beides wird auch auf dem Titelbild des Buches eindrucksvoll visualisiert. Symptomatisch ist nur, daß in den Texten gesellschaftliche Risiken der Medizinischen Informatik nur unzureichend thematisiert werden. Beispielsweise hat es den Anschein, als protagiere Köhler die Chipkarte über alle Kritik. Warum greift Köhler keines der zahlreichen Argumente der Kritiker ernsthaft auf und warum ist er nicht bereit, sie öffentlich zu diskutieren?

(Inge Allinger, Claus Stark) ■

FIFF e.V.

FIFF-Vorstand

- **Prof. Dr. Reinhard Keil-Slawik (Vors.)**
  Uni-GH Paderborn ZIT,
  Postfach 16 21,
  33098 Paderborn
- **Ute Bernhardt (stv. Vorsitzende)**
  Paulstraße 15, 53111 Bonn
- **Prof. Dr. Hans-Jörg Kreowski**
  Uni Bremen, FB 3,
  Postfach 33 04 40,
  28334 Bremen
- **Werner Moritz**
  Uhlandstraße 17,
  27576 Bremerhaven
- **Ingo Ruhmann**
  Paulstraße 15,
  53111 Bonn
- **Dr. Cornelia Teller**
  Kittlerstraße 27,
  64289 Darmstadt
- **Jürgen Ditz Schroer**
  Graf-Schenck-Str. 4a,
  82299 Türkenfeld
- **Peter Bittner**
  Aschbacherhof 3,
  67661 Kaiserslautern
- **Prof. Dr. Friedrich-Lothar Holl**
  Hektorstraße 7,
  10711 Berlin
- **Johannes Busse**
  Derendingerstraße 106,
  72072 Tübingen

Beirat

Prof. Dr. Wolfgang Coy (Bremen); **Prof. Dr. Leonie Dreschler-Fischer** (Hamburg); **Prof. Dr. Christiane Floyd** (Hamburg); **Prof. Dr. Klaus Fuchs-Kittowski** (Berlin); **Prof. Dr. Thomas Herrmann** (Dortmund); **Prof. Dr. Wolfgang Hesse** (Marburg); **Prof. Dr. Michael Grütz** (Konstanz); **Dr. Rolf Günther** (München); **Ulrich Klotz** (Frankfurt); **Prof. Dr. Hans-Jörg Kreowski** (Bremen); **Prof. Dr. Herbert Kubicek** (Bremen); **Prof. Dr. Hans-Peter Löhr** (Berlin); **Dipl.-Ing. Werber Mühlmann** (Oppung); **Prof. Dr. Frieder Nake** (Bremen); **Prof. Dr. Rolf Oberliesen** (Hamburg); **Dr. Hermann Rampacher** (Bonn); **Prof. Dr. Arno Rolf** (Hamburg); **Prof. Dr. Alexander Roßnagel** (Kassel); **Prof. Dr. Gerhard Sagerer** (Bielefeld); **Dr. Gabriele Schade** (Ilmenau); **Prof. Dr. Britta Schinzel** (Freiburg); **Prof. Dr. Dirk Siefkes** (Berlin); **Prof. Dr. Marie-Theres Tinnefeld** (München); **Prof. Dr. Dirk Siefkes** (Berlin); **Prof. Dr. Josef Weizenbaum** (Freibg./Cambridge); **Dr. Gerhard Wohland** (Wankheim)

FIFF-Beirat: Dr. Rolf Günther

Diplom in Elektrotechnik, Promotion in Wirtschaftswissenschaften, Berufstätigkeit zunächst in der Dieselmotoren-Fabrikation, dann ab 1961 in Programmierung, Systems-Engineering, Marketing, Öffentlichkeitsarbeit und Unternehmensführung bei Siemens in Europa und Übersee; in den 80er Jahren Mitglied der Gesellschaft für Informatik (und im FIFF) – Fachbereich „Computer und Gesellschaft", zum Schluß dort Fachbereichssprecher; seit 1990 im beruflichen Ruhestand.

Arbeits- und Interessen-Schwerpunkte als Mitglied der Synode der Ev.-Luth.-Kirche in Bayern: Entwicklungspolitik, Anti-Arbeitslosigkeitspolitik, Sozial- und Gesellschaftspolitik, und in der Informatik: benutzerorientierte Arbeitsteilung Mensch/Maschine.

FIFF Bibliothek

Hans-Jörg Kreowski, Thomas Risse, Andreas Spillner, Ralf E. Streibl, Karin Vosseberg (Hg.): Realität und Utopien der Informatik

Der Sammelband faßt die Ergebnisse der 10. Jahrestagung des Forums InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIFF) zusammen, die im Oktober 1994 in Bremen stattgefunden hat. Die Beiträge setzen sich aus verschiedenen Blickrichtungen und zu unterschiedlichen Anwendungsfeldern mit dem Spannungsverhältnis von Informatik und Gesellschaft auseinander. Im Mittelpunkt steht dabei die Frage: Welche Utopien und Visionen in den Bereichen Arbeit und Alltag, Staat und Umwelt haben in der Vergangenheit bei der Entwicklung der Informatik eine entscheidende Rolle gespielt, welche bestimmen Gegenwart und Zukunft?
agenda-Verlag, Bonn 1995, 28,- DM

Ute Bernhardt: Informatik und Gesellschaft. Eine Auswahlbibliographie
Ein thematisch gegliederter Einstieg in die Literatur zu Informatik und Gesellschaft
26 Seiten, Bonn 1990, 3,- DM

Ulrike Joos, Michael Kempf, Thomas Leuthold, Angelika Reiser, Bernd Rendenbach, Jürgen D. Schroer, Daniela Zelger: Das Datendschungelbuch. Ein pF!FFiger Wegweiser
... wenn Sie sich wundern wollen, wer Ihre Daten schon hat!
30 Seiten, Bonn 1991, 10,- DM

Ralf Klischewski, Simone Pribbenow (Hg.): ComputerArbeit. Täter, Opfer – Perspektiven
Das demokratische Potential der Neuen Fabrik · Maschinelle Intelligenz – Industrielle Arbeit · Arbeitnehmer und Betriebsräte zur Informatik im Betrieb
190 Seiten, Berlin 1989, 19,80 DM

Ute Bernhardt, Ingo Ruhmann (Hg.): Computer, Macht und Gegenwehr – InformatikerInnen für eine andere Informatik
Protected Mode · Computersicherheit: militärisch oder zivil · Computer und Umwelt · Technologiepolitik und Technikfolgenforschung · Partizipative Entwicklung von Systemen · EU: Grundrechte als Handelshemmnis? · u.v.a.
216 Seiten, Bonn 1991, 12,80 DM

Jutta Schaaf (Hg.): Die Würde des Menschen ist unverNETZbar
Netzknoten Frankfurt · Automatisierung des Zahlungsverkehrs · Rüstungshaushalt und Informationstechnik · Verfassungsverträglichkeit als Kriterium der Technikbewertung · Ethik und Technik · Theorie der Informatik · u.v.a.
300 Seiten, Bonn 1990, 12,80 DM

Ute Bernhardt, Ingo Ruhmann (Hg.): Ein sauberer Tod: Informatik und Krieg.
Informations- und Kommunikationstechnik – seit ihren Anfängen politisch geformt · Computer auf dem Schlachtfeld · Dual-Use: zivil geforscht – militärisch genutzt? · «Wehrtechnik und Landesverteidigung« – Zur Forschung in der Bundesrepublik · Weiter so oder umsteuern? · u.v.a.
320 Seiten, Marburg 1991, 20,- DM

Rudolf Kitzing, Ursula Linder-Kostka, Fritz Obermaier (Hg.): Schöne neue Computerwelt – Zur gesellschaftlichen Verantwortung der Informatiker
Beherrschbarkeit von Systemen, ihre Verletzlichkeit und die Verantwortung von Informatikern · Neue Wege in der Informatik · Psychosoziale Folgen des Computereinsatzes
256 Seiten, Berlin 1988, 19,80 DM

Heiko Dörr (Hg.): Herausforderungen an die Informatik? – Science and Peace in a Rapidly Changing Environment
Wissenschaft und Ethik · Computergestützte und Elektronische Kriegsführung · Curricula und Forschungs- & Entwicklungs- Ansätze in der Informatik – den Anforderungen des 21. Jahrhunderts gerecht werden · Computertechnologie – ein angemessenes Mittel gegen die Armut der 3. Welt? · (Kredit-) Kartenzahlung im Licht von Daten- und Verbraucherschutz · Vernetzung von Friedensgruppen · Texte in englisch und deutsch, 126 Seiten, Bonn 1992, 12,80 DM

Michael Löwe, Gerhard Schmidt, Rudolf Wilhelm (Hg.): Umdenken in der Informatik
231 Seiten, Marburg 1987, 19,80 DM

Alle Bücher zzgl. Porto zu beziehen bei: FIFF-Geschäftsstelle, Reuterstr. 44, 53113 Bonn.

Vielzweck-Schnipsel

Kopieren, ausfüllen und einsenden an: FIFF e.V., Reuterstr. 44, 53113 Bonn

FIFF

Das möchte ich:

❒ **Ich möchte ❒ aktives / ❒ förderndes Mitglied des FIFF werden** (Mindestjahresbeitrag ist für Verdienende **100,– DM**, für Studierende und Menschen in vergleichbarer Situation **25,– DM** pro Jahr. Mitglieder in den neuen Bundesländern zahlen **60%** des Beitrags.)

❒ **Ich möchte die FIFF-Kommunikation zum Preis von 25,– DM jährlich frei Haus abonnieren.**

❒ **Ich überweise den Mitglieds- bzw. Abobeitrag auf das Konto 480 00 798 bei der SPK BONN, BLZ 380 500 00.**

❒ **Der Mitglieds- bzw. Abobeitrag soll per Lastschriftverfahren von meinem Konto abgebucht werden** (siehe unten).

❒ **Ich möchte meine neue/korrigierte Anschrift mitteilen** (siehen unten). **Meine alte/falsche Anschrift:**

Straße: _____ Wohnort: _____

❒ **Ich möchte dem FIFF etwas spenden:**

❒ Verrechnungsscheck über _____ DM liegt bei ❒ Spendenquittung am Ende des Kalenderjahres erbeten

❒ **Ich möchte mehr über das FIFF wissen, bitte schickt mir:** _____

❒ **Ich möchte gegen Rechnung, zuzügl. Portokosten, bestellen:** _____

❒ **Ich möchte das FIFF über einen Artikel/ein Buch informieren:** ❒ **Zitat** (siehe unten) ❒ **Kopie liegt bei**

❒ **Ich möchte zur FIFF-Kommunikation beitragen mit:** ❒ **einem Manuskript zur Veröffentlichung** (liegt bei)
❒ **einer Anregung** (siehe unten)

Bemerkungen / Ergänzungen: _____

_____

_____

❒ **Ich möchte einen richtigen Brief schreiben. Der Vielzweck-Schnipsel ist nichts für mich.**

Die/der bin ich:

Name: _____ Straße: _____

Wohnort: _____ ggfs. Mitgliedsnummer: _____

Telefon (privat): _____ (Arbeit): _____ E-Mail: _____

Einzugsermächtigung

Hiermit ermächtige ich das FIFF e.V. widerruflich, meinen Mitgliedsbeitrag durch Lastschrift einzuziehen.
Wenn das Konto keine Deckung aufweist, besteht keine Verpflichtung des Geldinstituts, die Lastschrift auszuführen.

Name: _____ Jahresbeitrag: _____ DM, erstmals _____

Konto-Nr.: _____ BLZ: _____ Geldinstitut: _____

Straße: _____ Wohnort: _____

Datum: Unterschrift:

(Wir werden Ihre Daten nach §28 BDSG nur für eigene Zwecke verarbeiten und keinem Dritten zugänglich machen.)

Was will das FIFF?

Im Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V. haben sich InformatikerInnen zusammengeschlossen, die sich nicht nur für die technischen Aspekte, sondern auch für die gesellschaftlichen Auswirkungen ihres Fachgebiets verantwortlich fühlen und entsprechende Arbeit leisten wollen:

- *Kritik üben, denn wir haben das Know-How dazu*
- *uns für eine Abrüstung der Informatik engagieren*
- *uns am Diskurs über Technik und Wissenschaft beteiligen*
- *die Öffentlichkeit warnen, wenn wir Entwicklungen in unserem Fachgebiet für schädlich halten*
- *möglichen Gefahren eigene Vorstellungen entgegensetzen*
- *die Informations- und Kommunikationstechnik nicht gegen, sondern für den Menschen gestalten*
- *uns für eine zivile und gerechte Welt einsetzen; eine Welt, in der die Grundrechte aller Menschen gewahrt werden, eine Welt, die menschenwürdig ist*
- *last not least nicht alles machen, was machbar ist.*

Geplante Themenschwerpunkte für die FIFF-Kommunikation für das Jahr 1996:

2/96 »Computer & Schule«
zuständig: *Harald Selke*

3/96 »Computer & Krieg«
zuständig: *Peter Ansorge, Ralf E. Streibl*

4/96 »Computer & Demokratie«
zuständig: *Eva Jelden, Ingo Ruhmann, Ralf E. Streibl*

Die FIFF-Kommunikation bittet um Beiträge!

Die FIFF-Kommunikation lebt von der aktiven Mitarbeit ihrer LeserInnen!

Interessante Artikel, am besten zusammen mit geeigneten Fotos, Zeichnungen oder Comics zur Illustration (mit Quellenangabe) sind immer herzlich willkommen. Die Bearbeitung wird erleichtert, wenn Beiträge elektronisch und zusätzlich auf Papier der Redaktion zugehen. Die Redaktion behält sich Kürzungen und Titeländerungen vor.

Impressum

Die FIFF-Kommunikation ist das Mitteilungsblatt des »Forum InformatikerInnen für Frieden und Gesellschaftliche Verantwortung e.V.« (FIFF). Die Beiträge sollen die Diskussion unter Fachleuten anregen und die interessierte Öffentlichkeit informieren. Namentlich gekennzeichnete Artikel geben die jeweilige AutorInnen-Meinung wieder. Nachdruckgenehmigung wird nach Rücksprache mit der Redaktion in der Regel gerne erteilt. Voraussetzung hierfür ist die Quellenangabe und die Zusendung von zwei Belegexemplaren. Für unverlangt eingesandte Artikel übernimmt die Redaktion keine Haftung.

Heftpreis: 6 DM. Der Bezugspreis für die FIFF-Kommunikation ist für FIFF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die FIFF-Kommunikation für 25 DM/Jahr (inkl. Versand) abonnieren.

Erscheinungsweise: einmal vierteljährlich

Erscheinungsort: Bonn

Auflage: 2000

Herausgeber: Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIFF)

Verlagsadresse: FIFF-Geschäftsstelle, Reuterstr. 44, 53113 Bonn, Tel. (0228) 21 95 48

ISSN 0938 – 3476

Druck: Printwerkstatt Rambow, Auguststr. 10, 53229 Bonn

Layout: Markus Fleck

Redaktionsadresse: FIFF-Kommunikation, Reuterstr. 44, 53113 Bonn, Tel. (0228) 21 95 48, Fax (0228) 21 49 24, E-Mail: fiff-ko@informatik.uni-bonn.de

FIFF-Überall: In dieser Rubrik der FIFF-Kommunikation ist jederzeit Platz für Beiträge aus den Regionalgruppen und den überregionalen AKs. Aktuelle Informationen bitte per E-Mail an: Hubert.Biskup@sdm.de.

Lesen, Schluß-PFIFF: Beiträge für diese Rubriken bitte per Post an Claus Stark (Heilbronn) oder per E-Mail an: stark@fh-heilbronn.de

Redaktionsschluß für die Ausgabe 2/96: 31.4.1996.

Redaktions-Team FIFF-Kommunikation 1/96: Ute Bernhardt, Hubert Biskup, Markus Fleck, Hagen Kliemann, Ingo Ruhmann, Claus Stark, Harald Selke (verantwortlich)

Postvertriebsstücke werden von der Post auch auf Antrag nicht nachgesandt, daher bitten wir alle Mitglieder und Abonnenten, uns jede ***Adreßänderung*** rechtzeitig bekanntzugeben!

Hinweis: Entsprechend der seit 1. Juli 1992 gültigen Postdienst-Datenschutzverordnung teilt die Bundespost dem Herausgeber die neue Adresse eines Abonnenten mit, auch wenn kein Nachsendeantrag gestellt wurde. Wer damit nicht einverstanden ist, kann diesem Verfahren innerhalb von 6 Wochen widersprechen. ■

Adressen

Berlin

Irina Piens
Schmidtstraße 3
10179 Berlin
piens@prz.tu-berlin.de

Bonn

Manfred Domke
Am Wildpfad 12
53639 Königswinter
manfred.domke@gmd.de

Braunschweig

TU Braunschweig
Fachschaft Informatik
AStA – Fach
Katharinenstr. 1
38106 Braunschweig

Bremen

Prof.Dr. Hans-Jörg Kreowski
Uni Bremen
FB Informatik/Mathematik
Postfach 330440
28334 Bremen
Tel.: (0421) 218-2956
kreo@informatik.uni-bremen.de

Darmstadt

Dr. Cornelia Teller
Kittlerstr. 27
64289 Darmstadt
Tel.: (06151) 712926
CTE@software-ag.de

Erlangen/Fürth/Nürnberg

Klaus Thielking-Riechert
Herrnstr. 9
90763 Fürth
Tel.: 0911 / 775821
k.thielking@link-n.cl.sub.de

Frankfurt

Ingo Fischer
Dahlmannstr.31
60385 Frankfurt am Main

Hamburg

Simone Pribbenow
Hein-Köllisch-Platz 5
20359 Hamburg
Tel.: (040) 54715-366
pribbeno@informatik.uni-hamburg.de

Heilbronn

Claus Stark
Fachhochschule Heilbronn
FB Medizinische Informatik
Max-Planck-Straße 39
74081 Heilbronn
Tel.: (07131) 504-354
(07135) 7625
stark@fh-heilbronn.de

Kaiserslautern

Frank Leidermann
Moltkestr. 58
67655 Kaiserslautern
f_leider@informatik.uni-kl.de

Karlsruhe

Dietmar Seifert
Gartenstr. 7
76344 Eggenstein-
Leopoldshafen
Tel.: (0721) 9831387 (d)
bzw. 707897 (p)

Kiel

Hans-Otto Kühl
Alte Kieler Landstr. 118
24768 Rendsburg
Tel.: (04331) 201-2187

Koblenz

Dr. Michael Möhring
Uni Koblenz-Landau
FB Informatik
Rheinau 3-4
56075 Koblenz
Tel.: (0261) 9119477
Fax: (0261) 37524
moeh@infko.uni-koblenz.de

Köln

Manfred Keul
Landsbergstr. 16
50678 Köln
Tel.: (0221) 317911
100031.12@compuserve.com

Konstanz

Thomas Freytag
Irisweg 2
78467 Konstanz
Tel.: (07531) 50367
freytag@fh-konstanz.de

Lübeck

Lukas Faulstich
Inst. f. prakt. Informatik
Uni Lübeck
Wallstr. 40
23560 Lübeck
Tel.: (0451) 7030-420
faulstic@informatik.mu-luebeck.de

München

Bernd Rendenbach
Leerbichlallee 19
82031 Grünwald
Tel.: (089) 6410547

Münster

Werner Ahrens
Hohe Geest 120
48165 Münster
Tel.: (02051) 3054 (p)
bzw. (0251) 491-429 (d)

Oldenburg

Universität Oldenburg
Fachschaft Informatik
Ammerländer Heerstraße
26129 Oldenburg
Fachschaft.Informatik@informatik.uni-oldenburg.de

Paderborn

Harald Selke
Heinz Nixdorf Institut
Universität Paderborn
Fürstenallee 11
33102 Paderborn
Tel.: (05251) 606518
hase@uni-paderborn.de

Regensburg

Paul Hilmer
Zollerstraße 13
93053 Regensburg
Tel.: (0941) 706542
Fax: (0941) 706540
P.Hilmer@LINK-R.de

Stuttgart

Wolfgang Schneider
Sudetenstr. 21
71032 Böblingen

Tübingen

AK Informatik & Gesellschaft
Jochen Krämer
Sand 13
72076 Tübingen
Tel.: (07071) 29 – 5957
iug@informatik.uni-tuebingen.de
http://www-iug.informatik.uni-tuebingen.de/:8080

Ulm

Universität Ulm
Fachschaft Informatik
Bernhard C. Witt
Oberer Eselsberg
89081 Ulm
wittbe@pcpool1.informatik.uni-ulm.de

Überregionale Arbeitskreise

AK »RUIN» (Rüstung und Informatik)

Ingo Ruhmann
Paulstr. 15
53111 Bonn
Tel.: (0228) 634816
fiff@fiff.gun.de

AK »FIFF in Europa»

Dagmar Boedicker
Daiserstr. 45
81371 München
Tel.: (089) 7256547

AK »Informationstechnik für eine lebenswerte Welt»

Ralf Klischewski
Universität Hamburg,
FB Informatik
Vogt-Kölln-Str. 30
22527 Hamburg
Tel.: (040) 54715-367
Fax: (040) 54715-311
klischew@informatik.uni-hamburg.de

FIFF-Mailingliste

Beiträge an:
fiff-l@dia.informatik.uni-stuttgart.de
An- und Abbestellungen an:
fiff-l-request@dia.informatik.uni-stuttgart.de

FIFF-WWW-Seiten

http://www.uni-paderborn.de/arbeitsgruppen/fiff/fiff.html

FIFF-Kommunikation

fiff-ko@informatik.uni-bonn.de

FIFF-Geschäftsstelle

Reuterstr. 44
53113 Bonn
Tel.: (0228) 219548
Fax: (0228) 214924
E-Mail: fiff@fiff.gun.de
Dienstag und Donnerstag
jeweils 9 bis 15 Uhr
Kontoverbindung: 48000798
Sparkasse Bonn BLZ 380 500 00

Pure Alchemie

von Sönke Jahn

Der technische Fortschritt auf dem Gebiet der Chipkarten beeilt sich, als hätte man ihm in den Hintern getreten. Und obwohl an dieser Stelle im März (im MacMagazin) schon einmal Ansichten zu diesen Karten präsentiert wurden, kommen wir nicht umhin, noch einmal darauf zurückzukommen. So ist zu vermelden, daß sich bereits der erste Kleinunternehmer eine goldene Nase verdient mit einer Geschäftsidee, welche die persönlichen Daten auf unser aller Krankenkassenkarte pfiffig mißbraucht. Wie die Berliner Zeitung "Die Wirtschaft" berichtete, programmierte ein aufgeweckter Westfale eine Software, mit der aus der Versicherten- eine Stechkarte wird. So wird aus dem Lesegerät, wie es bereits in den Arztpraxen in Gebrauch ist, eine Stechuhr. Dieser Pfiffikus hat die digitalisierten Krankenscheindaten, so wie sie sind, in ein nahezu perfektes Identifikationssystem umgemodelt. Seine Kunden gehören vor allem zur Kaste der Privatversicherten, die uns gesetzlich Versicherte unter ihre Fuchtel bringen will. Die Krankenkassen fuchst es nach Ansicht des Wirtschaftsblattes nicht nur, daß hier ein Mißbrauch intimster Daten vorliegt. Es stört vor allem die Tatsache, daß so ein Mißbrauch überhaupt öffentlich ruchbar wird. Meldungen darüber kommen bei den Versicherten nicht gut an, graust es die Kassen. Denn die machen sich gerade daran, eine Patientenkarte einzuführen, auf der sensible Daten über den genauen Gesundheitszustand des Versicherten enthalten sein sollen. Die Kassen fürchten zu Recht unliebsame Fragen. Wenn schon mit den derzeitigen, vergleichsweise harmlosen Personaldaten Schindluder getrieben werden kann - was passiert dann erst, wenn demnächst Typhus, Tage und Tumor auch auf der Chipkarte verewigt werden?

Auch über die sogenannte elektronische Geldbörse gibt es Neuigkeiten. Diese Bargeldkarte ähnelt der Telefonkarte - nur daß auf ihrem Chip jederzeit ein neuer Geldbetrag abgespeichert werden kann. Diese und auch die Kreditkarten, die demnächst mit Computerchips bestückt werden, soll man nicht mehr zücken müssen, um damit zu bezahlen. Groß im Kommen ist nämlich die sogenannte kontaktlose Chipkarte, mit der man Handel und Wandel nur nahe genug (etwa zwei Meter) kommen muß, um im Vorübergehen um seine sauer verdienten Groschen erleichtert zu werden. Gedacht wird beispielsweise an die automatische Belastung des Kontos mit Eintrittsgeldern und Ticketgebühren. Wer mit einer Bargeldkarte in einen Bus der Lüneburger oder Oldenburger Verkehrsbetriebe einsteigt, dem wird dort versuchsweise bereits fleißig das Geld aus den Taschen gebeamt. Man muß um nicht allzu viele Ecken denken, um sich vorzustellen, wie begehrt diese Geldpump-Technologie auch bei Lumpen und Panzerknackern sein wird, sobald alle Welt kontaktlosen Cash mit sich herumträgt. Der Handtaschenklau funktioniert dann per Fernbedienung.

Unter uns Kassenpatienten: Wären wir nicht eine Herde frommer Schäfchen, wenn uns da nicht bange würde um unser Haushaltsgeld, wenn wir das sauer Verdiente künftig nur noch in Bytes (eventuell auch nur in Bits?) verwandelt mit uns herumtragen? Heißt es dann: "Ich hatte einen Systemabsturz" statt schlicht "Ich bin blank"? Romantiker erinnern sich gerne daran, wie sie sinnlich wie Hans im Glück selber die Geldstücke in ihrer Hosentasche klimpern lassen konnten. Und das beste daran war, daß man niemandem dafür irgendwelche Gebühren zu zahlen hatte. Warum eigentlich meint man, daß wir darauf vertrauen, daß uns nicht das Fell über die Ohren gezogen wird? Uns traut doch auch keiner, weshalb man uns ja mit Stechuhren und ähnlichem Teufelszeug plagt. Und richtig: Betreffs des Plastegeldes haben Banken kürzlich angekündigt, pro Barzahlung 0,3 Prozent des jeweiligen Betrages - mindestens aber fünf Pfennige - abhaben zu wollen. Somit ist die Ausgabe von elektronischen Zahlkarten mehr noch als die Kontrolle von Krankenkassenchip die wirkliche Geschäftsidee des Jahres. Früher nannte man sowas Wegelagerei, dann etwas feiner Steuern und heute halt euphemistisch Gebühr. Deshalb ist jedem, der noch nicht Bankbesitzer ist, anzuraten, schleunigst einer zu werden. Nicht nur, daß die Menschen einem dann ihr ganzes Geld vorbeibringen, sie sollen danach ohne Murren dafür bezahlen, daß sie es zwar nicht wiederbekommen, es ihnen aber auf ein Stück Plastik geschrieben wird.Und dann als Bankdirektor sogar noch vom Gemüsemann Gebühren zu verlangen, wenn der aus seinen digitalen Tageseinnahmen analoge Scheinchen machen will, ist das finanzpolitische Perpetuum mobile. Das ist wahre Goldmacherkunst und pure Alchemie: aus Scheiße Geld machen.

Erschienen in: Mac Magazin, November 1995.